swipe25

Privacy Policy

Operator	StaceLabs Ltd
Registered office	71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, United Kingdom

swipe25 Privacy Policy

Effective date: 1st April, 2026

This Privacy Policy explains how StaceLabs Ltd ("StaceLabs", "we", "us", or "our") collects, uses, shares, stores, and protects personal data when you use the swipe25 website, mobile application, and related services.

1. Who we are

Controller: StaceLabs Ltd

Registered office: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, UK

Email: admin@stacelabs.com

Privacy contact:+44 7393060439

Phone: +44 7393060439

For the purposes of UK data protection law, StaceLabs will usually act as a data controller for personal data processed through swipe25 where we decide why and how that personal data is used.

In some cases, third parties such as payment providers, analytics providers, cloud hosting vendors, customer support providers, identity verification providers, or fraud tools may act as our processors or as independent controllers, depending on the circumstances.

2. Scope of this Policy

This Privacy Policy applies to personal data we process about customers, prospective customers, service providers and prospective service providers, users of our website and app, people who contact us,

newsletter subscribers, complainants and other support contacts, and people whose information is included in booking or compliance records.

3. Personal data we collect

3.1 Identity and profile data

We may collect full name, username or account identifier, date of birth or age confirmation, profile photo, business or trading name, service category and profile bio, and identity verification data where required.

3.2 Contact data

We may collect email address, telephone number, billing address, service address, and correspondence address.

3.3 Account and authentication data

We may collect login credentials, password hashes, account settings, device or session authentication information, and security-related logs.

3.4 Booking and transaction data

We may collect booking requests, service descriptions, date, time, and location of bookings, pricing, cancellation information, payout status, refunds, dispute history, receipts, and invoices.

3.5 Payment-related data

Payments are processed through Stripe. We may receive limited payment-related information such as payment status, card type or last four digits, transaction identifiers, payout account status, connected account status, and fraud or risk indicators.

We do not ordinarily store full card numbers or full security codes on our own systems where Stripe handles the payment method collection.

3.6 Verification and compliance data

For providers especially, we may collect identity documents, bank account or payout details, proof of address, insurance details, licence or certification information, tax information, onboarding questionnaire responses, and sanctions, fraud, or compliance screening results where applicable.

3.7 Communications data

We may collect messages sent through the Platform, customer support queries, complaint records, call notes, email and in-app communications, and attachments and evidence submitted in disputes.

3.8 User content

We may collect reviews, ratings, photos, listing images, feedback, and responses to surveys or forms.

3.9 Device and technical data

We may collect IP address, device identifiers, browser or app version, operating system, crash data, diagnostics, log files, cookie and similar technology data, and approximate location derived from IP or device settings where enabled.

3.10 Usage data

We may collect pages viewed, screens visited, clicks or taps, interactions with listings, search terms, referral source, feature usage, and session durations.

3.11 Marketing and preferences data

We may collect email subscription preferences, consent records, campaign engagement data, and notification settings.

3.12 Special category or sensitive data

We do not intend to collect special category personal data unless this becomes genuinely necessary for a lawful purpose, such as handling an accessibility request, safety incident, or legal dispute. If we do need such data, we will process it only where we have a valid legal basis and, where required, an additional condition for processing.

4. How we collect personal data

We collect personal data directly from you when you register, book, apply as a provider, contact support, or use the Platform, automatically through your use of the website or app, from payment and onboarding partners such as Stripe, from verification, fraud, analytics, communications, and hosting vendors, from reviews, complaints, and dispute evidence, from cookies and similar technologies, from social sign-in or third-party account connections if you use them, and occasionally from public sources or third parties where required for trust, safety, legal, or fraud prevention purposes.

5. How we use personal data

We use personal data to create and manage user accounts, enable discovery of local services, facilitate bookings between customers and providers, process payments, refunds, reserves, and payouts, onboard and verify providers, communicate about bookings and account issues, provide customer support, investigate disputes, complaints, and safety concerns, prevent fraud, abuse, and unauthorised activity, improve the Platform, product design, and user experience, personalise content and search results, send service notices and operational communications, send marketing communications where permitted, enforce our Terms and platform rules, comply with legal, regulatory, tax, accounting, and payment obligations, and establish, exercise, or defend legal claims.

6. Lawful bases for processing

We generally rely on the following lawful bases under UK GDPR.

6.1 Contract

We process personal data where necessary to create and maintain your account, provide the Platform, administer bookings, process payments and payouts, provide support, and perform our contractual obligations.

6.2 Legitimate interests

We may process personal data where necessary for our legitimate interests, including operating and improving the Platform, marketplace administration, fraud prevention and platform security, trust and safety operations, dispute handling, business analytics, product development, enforcing our Terms, and limited direct marketing to existing users where permitted by law.

Where we rely on legitimate interests, we consider the impact on individuals and their rights.

6.3 Legal obligation

We process personal data where necessary to comply with legal obligations, including obligations relating to financial records, tax, anti-fraud requirements, consumer complaints, court orders, regulatory requests, law enforcement cooperation, sanctions screening, and data protection compliance.

6.4 Consent

Where required, we rely on consent for certain marketing communications, optional cookies or similar technologies, and any processing that clearly requires consent under applicable law.

You may withdraw consent at any time, but this does not affect the lawfulness of processing before withdrawal.

6.5 Vital interests or legal claims

In limited circumstances, we may process data to protect someone's vital interests or to establish, exercise, or defend legal claims.

7. Cookies and similar technologies

We may use cookies, SDKs, pixels, local storage, and similar technologies for authentication, remembering settings, fraud prevention, analytics, performance monitoring, app functionality, and marketing, where permitted.

You should also publish a separate Cookie Notice if you are using non-essential cookies or tracking tools on the site or app.

8. Sharing of personal data

We may share personal data with the following categories of recipients where necessary.

8.1 Other users

Customers see relevant provider listing information. Providers receive booking details needed to deliver the service. Users may see ratings, reviews, profile names, and related public profile information.

8.2 Payment providers

We share personal data with Stripe and associated services to process payments, onboard providers, verify payout eligibility, and manage refunds, disputes, and fraud controls. Stripe also has its own privacy terms and may act as a controller for certain processing.

8.3 Service providers and processors

We may share data with cloud hosting, analytics, customer support platforms, email, SMS, or push messaging providers, identity verification vendors, fraud detection vendors, CRM tools, document storage providers, and bug or crash monitoring tools.

8.4 Professional advisers and corporate recipients

We may share data with lawyers, accountants, auditors, insurers, banks, investors, acquirers, and advisors, where appropriate and lawful.

8.5 Authorities and law enforcement

We may disclose personal data where required by law or where reasonably necessary to comply with legal process, respond to regulatory requests, prevent fraud or crime, protect rights, safety, and property, or enforce our legal rights.

8.6 Business transfer

If StaceLabs undergoes a merger, acquisition, reorganisation, financing, or asset transfer, personal data may be disclosed as part of that transaction subject to confidentiality and applicable law.

9. International transfers

Some of our service providers may process personal data outside the UK. Where we transfer personal data internationally, we will take steps to ensure appropriate safeguards are in place, which may include adequacy regulations, the UK International Data Transfer Agreement, international data transfer addenda, or other lawful transfer mechanisms.

10. Data retention

We keep personal data only for as long as reasonably necessary for the purposes described in this Policy, including for account administration, booking history, customer support, dispute handling, legal and tax obligations, fraud prevention, and defending claims.

Retention periods may vary by data type. For example, account data may be held while the account remains active and for a reasonable period afterwards, transaction and payout records as needed for accounting, tax, and compliance purposes, support and dispute records for a reasonable period based on

legal and operational need, and marketing consent records while relevant and as needed to demonstrate compliance.

You should map exact retention periods in an internal retention schedule.

11. Data security

We use technical and organisational security measures designed to protect personal data, including measures such as access controls, authentication safeguards, encryption in transit where appropriate, role-based permissions, logging and monitoring, vendor due diligence, backups, and incident response processes.

No system is completely secure, and we cannot guarantee absolute security.

12. Children

swipe25 is not intended for children. Users must be at least 18 years old. We do not knowingly collect personal data from children in connection with the Platform. If you believe a child has provided personal data, contact us so we can investigate and take appropriate action.

13. Your data protection rights

Depending on the circumstances, you may have the right to be informed about how your data is used, access your personal data, request correction of inaccurate data, request deletion of your data, request restriction of processing, object to certain processing, request transfer of your data in portable form where applicable, withdraw consent where processing is based on consent, and complain to the UK Information Commissioner’s Office.

These rights are not absolute and may depend on the lawful basis for processing.

To exercise your rights, contact us at: admin@stacelabs.com

We may need to verify your identity before acting on a request.

14. Marketing communications

We may send you marketing communications where allowed by law and based on your preferences. You can opt out at any time by clicking the unsubscribe link in an email, updating notification preferences in the app, or contacting us directly.

Even if you opt out of marketing, we may still send service-related communications necessary for your account or bookings.

15. App analytics, diagnostics, and privacy disclosures

If swipe25 uses analytics, crash reporting, attribution, advertising SDKs, support SDKs, fraud tools, or other third-party technologies, the data they collect must be reflected accurately in this Privacy Policy, your App Store privacy questionnaire, and any in-app privacy controls or consent flows where required.

16. User-generated content and moderation data

Because swipe25 allows ratings, reviews, listings, and other user content, we may process content and metadata for moderation, trust and safety, fraud prevention, abuse detection, complaint handling, and enforcement of platform rules.

17. Provider onboarding and compliance data

Providers may be asked to submit additional information needed to assess suitability for listing, verify identity, comply with payment provider requirements, confirm payout eligibility, reduce fraud and platform abuse, validate service category restrictions, and manage legal or insurance risk.

Failure to provide required information may mean we cannot onboard or continue to list a provider.

18. Complaints

If you have concerns about our privacy practices, please contact us first.

Privacy contact: admin@stacelabs.com

Postal address: StaceLabs Ltd, 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ, UK

You also have the right to complain to the Information Commissioner's Office (ICO) in the UK.

19. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in law, regulation, payment or provider requirements, app functionality, business practices, or service providers.

If changes are material, we will take reasonable steps to notify users, such as via the app, website, or email.

Your continued use of the Platform after the effective date of the updated Policy may indicate acceptance of the updated Policy where permitted by law.