

BASSWALA PRIVACY POLICY

BASSWALA PRIVACY POLICY

Effective date: 8 September 2025

Last updated: 8 September 2025

Introduction

This Privacy Policy governs how Basswala ("we", "us", "our"), a platform that connects clients seeking DJ rental services with DJ operators ("DJ Operators"), collects, uses, discloses, and protects personal data. Basswala is committed to protecting the privacy of individuals who use our website, mobile applications, and related services (collectively, the "Service"). This Policy explains our data practices, your rights, and how to contact us.

Scope and applicability — Explanation:

This Privacy Policy applies to personal data we collect about:

1. Clients (people booking DJs).
2. DJ Operators (individuals or businesses offering DJs for rent).
3. Visitors to our website and mobile applications.

It covers information collected through forms, account creation, payments, phone calls, OTPs, support interactions, and automated technologies (e.g., cookies).

Definitions

-
- Personal Data / Personal Information: Any information that identifies or can reasonably identify an individual.
 - Sensitive Personal Data: Information that is highly sensitive and needs special protection (e.g., financial account credentials, authentication data). Where applicable, we treat financial details with strict safeguards.
 - Data Principal: The individual to whom the Personal Data relates (clients, DJ Operators).
 - Data Fiduciary: Basswala, as the entity determining the purposes and means of processing.
 - Consent: A free, specific, informed, and unambiguous indication of the Data Principal's wishes (opt-in) authorizing processing.

Information We Collect

We collect the following categories of personal data depending on the Service you use and the interactions you have with us:

A. Information from Clients (people who book DJs)

- Full name, email address, phone number.
- OTPs and transactional verification codes used during authentication.
- Call records (audio and metadata) if you call customer support or allow call verification.
- Billing information and payment instrument metadata (we do not store full card numbers unless explicitly required and secured; we prefer tokenized/card-on-file solutions provided by payment processors).
- Billing address and necessary KYC documents if required by law or payment providers.
- Booking history, preferences, reviews, ratings, and service feedback.
- Device and usage data (IP address, device identifiers, browser and app usage logs).
- Any other information you provide (messages, support requests, uploaded ID documents).

B. Information from DJ Operators

- Business and personal contact details: name, email, phone number.
- Bank account details and payout information (for receiving rental payouts).
- ID verification documents (e.g., government-issued ID) and tax registration details.
- License or certification details if applicable.
- Availability, service rates, location, and portfolio (images, demo audio).
- Communication logs and support interactions.

C. Payment & Financial Data

- Payment transaction metadata, last 4 digits and expiry for card identification when necessary, and externally-issued tokens used for recurring or one-click payments.
- We use third-party payment processors (such as Razorpay or similar); full card numbers are not retained by Basswala unless you explicitly choose a feature that requires it and we confirm industry-standard safeguards are in place.

D. Automated and Technical Data

- Cookies, pixel tags, mobile identifiers.
- Server logs, IP addresses, geolocation inferred from IP (approximate).
- Analytics data to improve the Service.

How We Collect Data — Explanation

- Directly from you when you register, book, submit forms, upload documents, or interact with support.
- From third-party services you choose to connect (e.g., payment processors, social login providers) and public sources (e.g., business listings).
- Automatically through cookies and tracking technologies when you visit our site or use our app.
- From DJ Operators when they enroll and provide bank/KYC details.

Purposes for Processing & Explanations

We process personal data for the following purposes (with short explanations for each):

1. To create and manage user accounts and profiles — Necessary to provide the Service (e.g., enable bookings, display operator profiles).
2. To facilitate bookings, payments, cancellations, and refunds — Processing is required to perform the contract between you and Basswala and to connect clients with DJ Operators.
3. To verify identity and prevent fraud — We use phone/OTP verification, KYC checks and may record verification calls to prevent misuse.
4. To process payouts to DJ Operators — Payment and bank details are used to disburse rental earnings, handle taxes and invoices.
5. For customer support and dispute resolution — We retain records of support interactions, call recordings (with consent), and messages to resolve issues.
6. For security, anti-fraud, and compliance — To protect user accounts and the integrity of the Service and to comply with applicable law.
7. For analytics and product improvement — To analyze usage patterns, improve features and the user experience.
8. For marketing and communication — With your consent, we may send promotional messages, offers, and newsletters. You may opt out at any time.
9. To comply with legal obligations — e.g., tax, financial regulations, court orders, and cooperation with law enforcement.

Legal Basis for Processing (where applicable)

Depending on the activity, Basswala relies on one or more legal bases for processing:

- Performance of a Contract: Processing necessary to provide the platform and complete bookings/payments.
- Consent: For processing activities that require explicit permission (e.g., marketing messages, call recordings, some uses of sensitive data).
- Legal Obligation: To comply with statutory or regulatory obligations (e.g., tax laws, financial record-keeping).
- Legitimate Interests: For fraud prevention, platform security, and internal analytics, balanced against individual rights.

Payment Processing, Card Data & Third-Party Gateways — Explanation and Clauses

1. Third-Party Payment Processors. We use PCI-compliant third-party payment processors (for example, Razorpay) to process payments and store/handle card data on our behalf. We do not routinely store full payment card numbers; instead, we rely on tokenization and secure vaulting performed by our payment partners. This reduces risk and keeps sensitive card data with certified payment processors. Explanation: Tokenization replaces card numbers with secure tokens that cannot be used outside the payment ecosystem. (See Razorpay documentation on tokenization and PCI standards for more details.) ■cite■turn0search13■turn0search2■
2. PCI-DSS Compliance. To the extent Basswala handles any cardholder data (e.g., card metadata or masked PAN), we follow PCI-DSS aligned practices or rely on our payment processors who are certified under the PCI Data Security Standard. Explanation: PCI DSS is the global standard for protecting payment card data and reducing fraud risk. ■cite■turn0search1■
3. RBI & Payment Data Localization. Certain payment-related data may be subject to Reserve Bank of India directions and storage requirements. Where applicable, we follow applicable RBI guidance and the requirements of our payment partners regarding the storage and localization of payment data. Explanation: Some Indian

regulations require payment-system data to be stored within India or be made available for supervisory access. Basswala will comply with such applicable requirements when they apply. ■cite■turn0search3■

Call Recording, OTPs and Voice Verification

- Call recording: We may record customer support calls or verification calls for training, quality assurance, and fraud prevention only after informing you and obtaining your consent where required by law. Explanation: Recording calls helps us investigate disputes and improve service but will be done only with notice and in accordance with applicable laws.
- OTPs: One-time passwords (OTPs) are used for authentication and verification. OTPs are short-lived and used only to confirm identity; they are not used for marketing. We may store limited metadata about verification attempts for fraud prevention.
- Phone calls & fraud: Where we store call recordings, we apply strict access controls and delete recordings after the retention period described below (or earlier at your request, subject to legal exceptions).

Sharing, Disclosure & Third Parties

We may share personal data with:

1. Service providers and subprocessors: payment processors (Razorpay and others), hosting providers (cloud services), analytics providers, messaging/OTP providers, and CRM vendors. These parties process data on our behalf under contract and are permitted to use personal data only to provide services to us.
2. DJ Operators: Basic booking-related information (name, contact number, event details) is shared with the DJ Operator engaged to provide the service so they can fulfill the booking.
3. Legal, safety and regulatory authorities: To comply with lawful requests, legal process, or to protect rights, property, or safety.
4. Business transfers: In the event of a merger, acquisition, reorganization, or sale of assets, personal data may be transferred as part of the transaction — with notice to affected users and legal safeguards.
5. Marketing partners: Only with your explicit consent.

Data Transfers and Cross-border Processing

Where Basswala or our subprocessors transfer personal data outside India (for example to cloud-hosting or analytics vendors), we will take reasonable steps to ensure appropriate safeguards are in place in compliance with applicable law. Under Indian law (for example the Digital Personal Data Protection Act, 2023), cross-border transfers may be subject to conditions and safeguards. Explanation: We will implement contractual and technical measures to protect your data in transit and at rest. ■cite■turn0search0■

Data Retention and Deletion

- Retention approach: We retain personal data only as long as necessary for the purposes described in this policy, to meet contractual and legal obligations (for example accounting/tax requirements), and to resolve disputes.
- Example retention periods (subject to variation depending on law or business need):
 - * Transaction records and receipts: retained for a period required by tax and financial law (commonly multiple years) or as required for audits.
 - * Account data and profile information: retained while the account is active and for a reasonable period after account closure for dispute resolution and legal compliance.
 - * KYC and verification documents: retained as required by law or payment provider agreements.
 - * Call recordings and OTP logs: retained for a limited period (for example 6–24 months) depending on the purpose and law; deleted earlier upon request if allowed by law.
- Deletion requests: You may request deletion of your personal data by contacting us (see Contact section). We will comply with requests subject to legal/regulatory retention requirements and internal legitimate needs (e.g., fraud investigations).

Security Measures

We have implemented organizational and technical safeguards designed to protect personal data against unauthorized access, alteration, disclosure, or destruction, including:

- Encryption in transit (TLS/HTTPS) and encryption at rest where feasible.
- Access controls and role-based permissions for staff and subprocessors.
- Regular security reviews and vulnerability testing.
- Limiting access to sensitive financial data; using tokenization and certified payment processors to reduce exposure.

- Incident response plans and (where applicable) notification to affected users and authorities in case of a data breach.

Your Rights and Choices

Subject to applicable law, you may have the following rights:

- Right of access: Request a copy of your personal data processed by us.
- Right to correction: Request correction of inaccurate or incomplete data.
- Right to deletion: Request deletion of personal data where there is no legal basis to retain it.
- Right to portability: Request a portable copy of data you provided in structured machine-readable form.
- Right to withdraw consent: Withdraw consent where processing is based on consent.
- Right to lodge a complaint: You may complain to our grievance officer (contact details below) or to the relevant supervisory authority.

How to Exercise Rights — Explanation:

To exercise any of the above rights, please contact us at the email or postal address given in the Contact section. We may need to verify your identity before acting on requests. We will respond to requests in accordance with applicable law.

Cookies and Tracking Technologies

We use cookies and similar technologies to provide the Service, remember preferences, and analyze traffic. You can control cookie preferences through your browser or device settings. Note that disabling certain cookies may limit functionality.

Children's Data

Basswala does not knowingly provide services to children under the age of 18. If we learn that we have collected personal data of a child under 18 without verifiable parental consent, we will take steps to delete that data. Under applicable Indian law (Digital Personal Data Protection Act, 2023), processing children's data requires parental or guardian consent and additional safeguards. [■cite■turn0search0■](#)

Automated Decision-making and Profiling

We may use automated systems for certain activities (e.g., fraud detection, recommending DJ Operators). Where automated decisions have a legal or similarly significant effect, you may request human review and contest the decision. Explanation: Automated systems help us scale, but human oversight is available for important outcomes.

Changes to This Privacy Policy

We may update this Privacy Policy to reflect changes in our practices or legal requirements. When material changes occur, we will notify users by email or prominent notice on our site and update the "Last Updated" date.

Contact, Grievance Officer & Complaints

If you have questions, requests or a complaint regarding this Privacy Policy or our data practices, please contact:

Grievance Officer:

Data Protection / Grievance Officer

Basswala (Private Limited)

Email: privacy@basswala.example

Postal: [Company registered address]

If you are located in India, you may also have the right to file a complaint with the Data Protection Board of India or other competent authority under applicable law (for example the Digital Personal Data Protection Act, 2023). [■cite■turn1search1■turn1search2■](#)

Legal Notice and Disclaimer

This Privacy Policy is intended as a comprehensive template for Basswala's privacy practices and includes recommended clauses and explanatory notes. It does not constitute legal advice. We recommend that Basswala consult a qualified legal professional to review and tailor this Privacy Policy to the company's operational,

regulatory, and jurisdictional needs.

Appendix: Key Practical Notes on Specific Data Types

- Card data: We recommend avoiding storing full Primary Account Numbers (PAN) on our servers. Use tokenization and let PCI-compliant payment processors (e.g., Razorpay) vault card data. ■cite■turn0search13■turn0search1■
- Bank account details for payouts: Keep minimal required data (account number, IFSC, account holder name) and secure storage. Consider masking data in UI and logs.
- OTPs and verification codes: Treat as authentication data; retain only necessary metadata and not the OTP value except for short durations needed for verification.
- Call recordings: Provide notice at the start of the call and keep recordings encrypted with strict role-based access.

End of Policy