PRIVACY POLICY

Phinx, a product of Sojaru Corp LLP

Effective Date: 12 November 2026
Last Updated: 12 November 2026

Phinx is a product of Sojaru Corp LLP ("Sojaru", "we", "us" or "our"), a limited liability partnership registered in India under the Limited Liability Partnership Act, 2008 (LLPIN ACR-3169, GSTIN 19AFSFS5111B1ZZ), with its registered office at 2nd Floor, Flat 2A, 3/97 Chittaranjan Colony, Jadavpur, Kolkata 700032, West Bengal, India.

This Privacy Policy explains how we gather, use, share, store and protect personal data when you visit phinx.in, use the Phinx dashboard at app.phinx.in, or use any Phinx service (together, the "Services"). It is written to meet the Digital Personal Data Protection Act, 2023 and the Digital Personal Data Protection Rules, 2025 (together, the "DPDP Law"), the Information Technology Act, 2000 and the rules made under it.

Please read it together with our Terms of Service and Cookie Policy.

1. OUR ROLE

We act in two different roles, and this policy says which applies:

- **Data Fiduciary.** For the personal data of our own customers, website visitors and people who contact us, we decide why and how the data is processed.
- **Data Processor.** For the personal data of the visitors and customers of a website or application that you host with us or ask us to build or test ("End Users"), you are the Data Fiduciary and we process that data only on your behalf and on your instructions. If you are an End User of a site built on Phinx, please contact the owner of that site first. We will help them respond to you.

2. PERSONAL DATA WE PROCESS

Category	What it includes	Where it comes from
Account data	Name, email address, mobile number, business name, sign-in records	You, when you sign up or update your profile
Billing data	Billing name and address, GSTIN (if any), plan, invoices, payment status and transaction reference	You and our payment gateway. We do not receive your full card or bank details
Service data	Links you ask us to scan, scan and test results, code and files you upload, Builds you host, release history and logs	You and the Services
Payment setup data	Only if you ask for help setting up payments: PAN, GSTIN, business registration details, bank account details for settlement, address and contact details, and identity documents that a provider asks for	You, with your consent, for the specific application

Category	What it includes	Where it comes from
Communications	Messages, support requests, call notes and feedback	You
Technical data	IP address, browser and device type, pages requested, timestamps and security logs	Our servers, automatically

We do not ask for your Aadhaar number. Where a payment provider or registration portal requires Aadhaar verification, you complete that step directly with them, using your own OTP.

Scans read only what a visitor's browser can see on the links you give us, or the code you upload for a deep scan. If a scan finds a secret key or password, we show only its type and last four characters and never store it in full.

3. WHY WE USE IT, AND ON WHAT BASIS

Purpose	Legal basis under the DPDP Law
Creating and running your Account, and providing the Services you ask for	Your consent, and the use you have voluntarily provided the data for
Billing, invoicing and keeping tax and accounting records	Your consent, and compliance with law
Helping you register a business or apply for a payment gateway	Your specific consent, given separately for that application
Keeping the Services secure, preventing fraud and abuse, and investigating incidents	Legitimate use for security, and compliance with law
Answering questions and complaints	Your consent
Telling you about changes to the Services or these policies	Your consent, and compliance with law
Sending product news or offers	Only with your separate consent, which you can withdraw at any time

We do not sell personal data, use it for third-party advertising, or build profiles of you for marketing.

4. CONSENT AND WITHDRAWAL

Where we rely on your consent, we ask for it in clear terms, for a specific purpose. You may withdraw consent at any time by writing to privacy@sojaru.com or using the settings in your dashboard. Withdrawing is as easy as giving consent. It does not affect processing already carried out, but we may no longer be able to provide the Services that depend on it.

5. WHO WE SHARE IT WITH

We share personal data only as needed for the purposes above, and only with:

- **Service providers who work for us**, under written contracts that require them to protect the data and use it only on our instructions. These include cloud hosting and storage, email and SMS delivery, our business email service, and our payment gateway for our own billing. Our subprocessor list names each one and where it processes data.
- **Payment providers and registration authorities you choose**, only when you ask us to help with a payment gateway application or business registration, and only the information that application needs.
- **Authorities**, where the law requires it, such as in response to a valid order from a court, CERT-In, the Data Protection Board of India or another competent authority.
- **A successor business**, if Sojaru is restructured, merged or sold, subject to this policy and with notice to you.

We do not share your code or the personal data of your End Users for any purpose other than providing the Services to you, and we do not use them to train artificial intelligence models made available to anyone else.

6. WHERE YOUR DATA IS STORED, AND TRANSFERS ABROAD

- **Hosting in India.** The Services, including your Account data, hosted Builds, databases, backups and our system logs, run on Amazon Web Services data centres located in India.
- **Logs stay in India.** We keep security and system logs within India for at least 180 days, as the CERT-In directions require.
- **AI hosted by us.** For scans, fixes, chatbots and drafts we use open-source artificial intelligence models that we host ourselves, on systems Sojaru operates in India. Your code and your End Users' data are not sent to an outside AI provider.
- **Limited processing abroad.** Our business email service, which we use to write to our own customers, may store emails in data centres outside India. Our subprocessor list names each provider and where it processes data.
- **Indian law.** We transfer personal data outside India only as the DPDP Law permits, never to a country that the Government of India has restricted, and with contracts that require the same level of protection.
- **People in the European Union and the United Kingdom.** If you are in the EU, the EEA or the UK, your personal data is transferred to India, which does not currently have an adequacy decision. We protect these transfers with the Standard Contractual Clauses approved by the European Commission and, for the UK, the International Data Transfer Addendum, and we assess the risks of each transfer. You can ask for a copy of the relevant safeguards at privacy@sojaru.com.
- **Customers' End User data.** Where we process End User data for you, our Data Processing Agreement governs where it is stored and how it may be transferred.

7. HOW LONG WE KEEP IT

Data	How long
Account data	While your Account is active, and for 30 days after it closes
Customer content and hosted Builds	While your Account is active, and for 30 days after it closes, so that you can request an Exit Kit
Scan results	90 days, then deleted
Payment setup documents	Deleted within 30 days after the application is approved, rejected or withdrawn
Invoices and billing records	As long as tax and accounting laws require, currently up to eight years
Security and access logs	At least one year, as the DPDP Rules require, and up to two years, stored in India
Support messages	Up to two years after the request is closed

When a retention period ends, we delete the data or make it permanently anonymous, unless a law or a pending legal claim requires us to keep it longer.

8. HOW WE PROTECT IT

We use reasonable security safeguards suited to the nature of the data, including:

- encryption of data in transit using TLS, and encryption of stored data;
- access limited to personnel who need it, with individual credentials and multi-factor authentication;
- logging and monitoring of access to systems that hold personal data;
- regular backups and tested restore procedures; and
- confidentiality obligations on everyone who works with us.

No system is completely secure. If you believe your Account or data is at risk, write to security@sojaru.com straight away.

9. PERSONAL DATA BREACHES

If a personal data breach affects data for which we are the Data Fiduciary, we will:

- tell the affected people without delay, through their account or their preferred contact method, explaining what happened, the likely consequences, what we are doing and what they can do to protect themselves;
- inform the Data Protection Board of India without delay, and give it a detailed report within 72 hours of becoming aware of the breach, or within any longer period it allows; and
- report cybersecurity incidents to CERT-In within six hours of noticing them, as required by the CERT-In directions.

If a breach affects End User data that we process for you, we will tell you without undue delay and help you meet your own obligations.

10. YOUR RIGHTS

Under the DPDP Law you have the right to:

- get a summary of the personal data we hold about you and how we use it, and the identities of those we have shared it with;
- have inaccurate or incomplete data corrected, completed or updated;
- have your data erased when it is no longer needed for the purpose it was given for, unless the law requires us to keep it;
- withdraw your consent;
- nominate another person to exercise your rights if you die or become unable to do so; and
- have your grievance addressed by us, and then, if you are not satisfied, complain to the Data Protection Board of India.

To exercise a right, write to privacy@sojaru.com from the email address on your Account, or include your registered mobile number, so that we can verify your identity. We respond within 30 days, and in any case within the 90-day outer limit set by the DPDP Rules.

11. CHILDREN

The Services are for adults using them in the course of a business, profession or project. We do not knowingly collect personal data of anyone under 18. If you believe a child has given us personal data, write to privacy@sojaru.com and we will delete it.

If your Build is directed at children, you must obtain verifiable parental consent as the DPDP Law requires. We can help you set this up.

12. COOKIES

Our marketing website does not use analytics or advertising cookies. The dashboard uses only the cookies needed for sign-in and security. Our Cookie Policy gives the details.

13. CHANGES TO THIS POLICY

We may update this policy. We will post the new version on this page with a new "Last Updated" date and, for material changes, tell you by email or in the dashboard before they take effect.

14. CONTACT AND GRIEVANCE REDRESSAL

For privacy questions or requests, write to privacy@sojaru.com. For complaints, contact our Grievance Officer, who acknowledges complaints within 24 hours and aims to resolve them within 15 days:

- Grievance Officer: Soubhik Biswas, Designated Partner, Sojaru Corp LLP
- Email: grievance@sojaru.com
- Phone: +91 91470 50755
- Address: 2nd Floor, Flat 2A, 3/97 Chittaranjan Colony, Jadavpur, Kolkata 700032, West Bengal, India

Legal entity	Sojaru Corp LLP (LLPIN ACR-3169)

Registered office	2nd Floor, Flat 2A, 3/97 Chittaranjan Colony, Jadavpur, Kolkata 700032, West Bengal, India
GSTIN	19AFSFS5111B1ZZ
Privacy requests	privacy@sojaru.com