DATA PROCESSING AGREEMENT

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 Data Processing Agreement ("DPA") applies whenever Sojaru processes personal data on behalf of a Phinx customer ("you") while providing the Services. It forms part of the Terms of Service between you and Sojaru and applies automatically when you accept them. Terms not defined here have the meaning given in the Terms of Service. If this DPA conflicts with the Terms of Service on the processing of personal data, this DPA prevails.

1. ROLES

- For personal data of your End Users that we host or process for you ("Customer Personal Data"), you are the Data Fiduciary under the Digital Personal Data Protection Act, 2023 (the "DPDP Act") and the controller under the GDPR, and Sojaru is your Data Processor (the "processor" under the GDPR and the "service provider" under the CCPA).
- You are responsible for having a lawful basis for collecting Customer Personal Data, for the notices you give your End Users, and for the instructions you give us.
- This DPA does not cover personal data that Sojaru processes as a Data Fiduciary for its own purposes, such as your Account and billing data. Our Privacy Policy covers that.

2. SCOPE OF PROCESSING

The subject matter, nature, purpose and duration of the processing, the types of personal data and the categories of people concerned are set out in Annex 1.

3. OUR OBLIGATIONS

Sojaru will:

- process Customer Personal Data only on your documented instructions, which are these Terms, your configuration of the Services and any request you make through the dashboard or in writing, unless the law requires otherwise, in which case we will tell you first unless the law forbids it;
- tell you promptly if we believe an instruction breaks the DPDP Act, the GDPR or another data protection law;
- not sell, share for advertising, or otherwise use Customer Personal Data for our own purposes, and not combine it with personal data from other sources except as needed to provide the Services;
- not use Customer Personal Data to train artificial intelligence models made available to anyone else;

- ensure that everyone authorised to process Customer Personal Data is bound by confidentiality;
- apply the security measures in Annex 2; and
- make available to you the information you reasonably need to show compliance with this DPA.

4. WHERE DATA IS STORED

- Customer Personal Data, including databases, files and backups of your hosted Builds, is stored on Amazon Web Services data centres in India.
- System and security logs are kept within India for at least 180 days, as the CERT-In directions require.
- We will not move the primary storage of Customer Personal Data outside India without giving you at least 30 days' notice.
- Where a subprocessor in Annex 3 processes Customer Personal Data outside India, the transfer is made only as the DPDP Act and, where it applies, the GDPR permit, with the safeguards in section 9.

5. SUBPROCESSORS

- You authorise us to engage the subprocessors listed in Annex 3, which is also published on our website.
- We will tell you by email or in the dashboard at least 14 days before we add or replace a subprocessor. You may object on reasonable data protection grounds within that period. If we cannot resolve the objection, you may end the affected Services and receive a refund of any prepaid fees for them.
- We impose on every subprocessor, by written contract, data protection obligations no less protective than those in this DPA, and we remain responsible to you for their performance.

6. HELPING YOU RESPOND TO YOUR USERS

Taking into account the nature of the processing, we will help you respond to requests from End Users to exercise their rights, including access, correction, erasure and withdrawal of consent, within the time the law sets. If an End User contacts us directly, we will pass the request to you without undue delay and will not respond ourselves unless you ask us to.

7. PERSONAL DATA BREACHES

- We will notify you without undue delay, and in any case within 24 hours, after we confirm a personal data breach affecting Customer Personal Data.
- The notice will describe, as far as we know at the time, what happened, the data and people likely to be affected, the likely consequences, and the steps taken or proposed. We will add details as our investigation continues.
- We will take reasonable steps to contain the breach and reduce its effects, and help you prepare the notices that the DPDP Act, the GDPR or other laws require you to give to regulators and End Users. Unless you ask us to send a notice on your behalf, you remain responsible for sending it.

- Separately, we report cybersecurity incidents affecting our own systems to CERT-In within six hours, as Indian law requires.

8. DELETION AND RETURN AT THE END OF THE SERVICES

When your Account ends, we will, at your choice, return Customer Personal Data to you through an Exit Kit or delete it. Unless you ask for it to be deleted sooner, we keep it for 30 days after your Account ends and then delete it from live systems, and from backups within a further 30 days, except where the law requires us to keep it.

9. INTERNATIONAL TRANSFERS

Indian law

Transfers of Customer Personal Data outside India are made only to countries not restricted by the Government of India under section 16 of the DPDP Act, and subject to any sectoral rules that apply.

Customers subject to the GDPR

Where you are established in the European Economic Area, or the GDPR otherwise applies to your processing, and Customer Personal Data is transferred to Sojaru in India:

- the Standard Contractual Clauses adopted by European Commission Implementing Decision (EU) 2021/914, Module Two (controller to processor), are incorporated into this DPA by reference, with you as the data exporter and Sojaru as the data importer;
- Clause 7 (docking clause) applies; under Clause 9, option 2 (general written authorisation) applies with the notice period in section 5; the optional wording in Clause 11 does not apply; under Clause 13, the competent supervisory authority is that of your establishment or representative; under Clauses 17 and 18, the law and courts of Ireland apply;
- Annexes I and II of those clauses are completed by Annexes 1 and 2 of this DPA, and the list of subprocessors is Annex 3; and
- we will help you carry out any transfer impact assessment you need, and tell you if we can no longer comply with the clauses.

Customers subject to the UK GDPR

For transfers subject to the UK GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, issued by the UK Information Commissioner, is incorporated by reference, with the tables completed using the information in this DPA.

10. CUSTOMERS SUBJECT TO THE CCPA

Where the California Consumer Privacy Act, as amended by the California Privacy Rights Act, applies to Customer Personal Data, Sojaru acts as your service provider and:

- will not sell or share the personal information, or retain, use or disclose it for any purpose other than the business purposes in this DPA, or outside the direct business relationship with you;
- will not combine it with personal information received from others, except as the CCPA permits;

- will comply with the CCPA, provide the same level of privacy protection the CCPA requires, and tell you if we can no longer meet our obligations; and
- allows you to take reasonable steps to stop and remedy unauthorised use of the personal information.

11. INFORMATION AND AUDITS

On written request, and no more than once in any 12-month period unless a regulator requires it or a breach has occurred, we will answer a reasonable security questionnaire and provide summaries of our security measures. Where the law gives you a right to an audit, it will be carried out on 30 days' notice, during business hours, by you or an independent auditor bound by confidentiality, at your cost, and in a way that does not compromise other customers' data.

12. LIABILITY AND TERM

Each party's liability under this DPA is subject to the limits in the Terms of Service, except where those limits cannot apply under the Standard Contractual Clauses or the law. This DPA lasts for as long as we process Customer Personal Data for you.

13. ANNEX 1: DESCRIPTION OF THE PROCESSING

Subject matter	Hosting, building, testing, monitoring and maintaining the customer's websites and applications
Nature of processing	Storage, hosting, backup, transmission, scanning for security and readiness, testing, applying fixes, sending messages the customer configures, and deletion
Purpose	Providing the Services the customer has ordered
Duration	The term of the customer's Account, plus the deletion periods in section 8
Categories of people	The customer's End Users, such as visitors, customers, subscribers and staff, and other people whose data the customer chooses to store
Types of personal data	As determined by the customer, typically names, contact details, account credentials (stored hashed), order and booking details, messages, IP addresses and device data
Sensitive data	Not expected. The customer must not store health, financial account, biometric or children's data in the Services without telling Sojaru in writing first
Frequency	Continuous while the Services are in use

14. ANNEX 2: SECURITY MEASURES

- Hosting on Amazon Web Services data centres in India, with network isolation between customer environments.

- Artificial intelligence models used for scans, fixes, chatbots and drafts are open-source models hosted by Sojaru on systems it operates in India, so Customer Personal Data is not sent to an outside AI provider.
- Encryption of data in transit with TLS, and encryption of stored data and backups.
- Access to production systems limited to authorised Sojaru personnel who need it, using individual accounts and multi-factor authentication, with access reviewed regularly.
- Logging of access and system events, kept within India for at least 180 days, with clocks synchronised to Indian government time servers.
- Regular backups, kept in India, with restore procedures tested.
- Secrets and keys found in customer code are shown only in truncated form and never stored in full.
- Vulnerability scanning of our own systems, and prompt patching of critical issues.
- A written incident response procedure, including reporting to CERT-In within six hours.
- Confidentiality and data protection obligations for all partners, employees, interns and contractors, under Sojaru's internal data protection and cybersecurity norms.

15. ANNEX 3: SUBPROCESSORS

The current list of subprocessors is published in the Phinx Subprocessor List and forms part of this DPA.

16. CONTACT

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
Data protection questions	privacy@sojaru.com
Security incidents	security@sojaru.com