Global Privacy & Data Protection Policy

Effective Date: 3 November 2025

1. Purpose and Scope:

This Global Privacy & Data Protection Policy ("Policy") explains how Bond Rebuild ("Company", "we", "our", "us") collects, uses, stores, discloses, and protects personal data of users, customers, and partners who engage with our digital platforms, including our website, online sessions, and related services.

This Policy applies globally to all users, irrespective of location, and is designed to comply with:

a. *General principles of GDPR (EU),*
b. *CCPA (California, USA), and*
c. *Other applicable international privacy laws.*

2. Definitions

a. *"Personal Data" means any information that can identify a person, directly or indirectly (such as name, email address, phone number, IP address, or device ID).*
b. *"Processing" means any operation performed on personal data, including collection, storage, use, transfer, or deletion.*
c. *"Data Subject" or "User" means an individual whose personal data is collected.*
d. *"Controller" means the Company that determines how personal data is processed.*
e. *"Processor" means any third party that processes data on behalf of the Controller.*

3. Types of Data Collected:

We may collect the following categories of personal data:

1. *Identification Data – Full name, email address, contact number, gender, and date of birth.*
2. *Account Data – Username, login credentials, and account preferences.*
3. *Transaction Data – Payment details (via PayPal or other gateways), billing address, and transaction history.*
4. *Usage Data – IP address, browser type, access logs, and interaction data with our platform.*
5. *Session Data – Audio, video, or text interactions during live or recorded sessions (with consent).*

4. Purpose of Processing:

We process personal data to:

a. *Provide and manage access to our services.*
b. *Process payments and deliver digital content.*
c. *Personalize user experiences.*
d. *Improve platform functionality and security.*
e. *Comply with legal obligations.*

f. *Communicate updates, offers, or relevant information (with consent).*

5. Legal Basis for Processing:

Depending on user location, we rely on one or more of the following legal bases:

a. *Consent – When users voluntarily provide data or agree to communications.*
b. *Contractual Necessity – When processing is required to fulfil service obligations.*
c. *Legitimate Interests – For platform security, analytics, or customer relationship management.*
d. *Legal Compliance – To meet regulatory or tax obligations.*

6. Data Retention:

Personal data is retained only as long as necessary to fulfil the purposes stated in this Policy, or as required by law. After expiration of retention periods, data is securely deleted or anonymized.

7. Data Sharing and Disclosure:

We may share data with:

a. *Service Providers – For hosting, payments, analytics, and communication.*
b. *Legal Authorities – When required by applicable law or judicial order.*
c. *Business Partners – For collaborative services or co-hosted events (with consent).*

All third-party service providers are contractually bound to maintain confidentiality and comply with applicable data protection laws.

8. International Data Transfers:

Where applicable, personal data may be transferred to or stored on servers located outside your country. We ensure appropriate data protection safeguards, such as Standard Contractual Clauses (SCCs) or equivalent protection measures.

9. Data Security:

We implement appropriate technical and organizational measures to prevent unauthorized access, alteration, or loss of data, including:

a. *Encrypted storage and transmission,*
b. *Secure login procedures,*
c. *Periodic system audits and monitoring,*
d. *Limited access to authorized personnel only.*

10. User Rights:

Depending on jurisdiction, users may exercise the following rights:

a. *Right to access and obtain a copy of personal data.*
b. *Right to request correction or deletion.*
c. *Right to restrict or object to processing.*
d. *Right to data portability.*
e. *Right to withdraw consent at any time.*

f. Right to lodge a complaint with a competent authority.

Requests can be made via _____ [Contact Email], and will be addressed within 30 days.

11. Cookies and Tracking Technologies:

Our platform uses cookies and similar tools for analytics and user experience optimization. Users can manage or disable cookies through browser settings, though this may limit functionality.

12. Payments and Financial Data

All payments are securely processed through PayPal and other integrated gateways in U.S. Dollars (USD). We do not store credit card or banking details directly. Such data is processed securely by third-party payment processors compliant with PCI-DSS standards.

13. Children's Privacy

Our services are not directed toward individuals under the age of 16. We do not knowingly collect data from minors. If such data is discovered, it will be promptly deleted.

14. Updates to This Policy

We may revise this Policy periodically. Any material changes will be notified via email or posted on our website with an updated "Effective Date."

15. Contact Information

For questions, requests, or complaints regarding this Policy, please contact:

Email:Support@bondrebuild.com

Annexure A: Data Processing Addendum (DPA)

1. Purpose:

This Data Processing Addendum ("DPA") forms an integral part of the Global Privacy & Data Protection Policy and governs the processing of personal data by third-party service providers ("Processors") engaged by Bond Rebuild ("Controller").

The DPA ensures that any such processing is conducted in compliance with applicable data protection laws, including the EU and UK GDPR, the California Consumer Privacy Act (CCPA), and other international privacy frameworks.

2. Roles and Responsibilities:

a. Controller: Bond Rebuild determining the purposes and means of processing.
b. Processor: Any third party that processes personal data on behalf of the Controller.

c. *Data Subject: The individual whose personal data is being processed.*

3. Processor Obligations:

Each Processor shall:

a. *Process personal data solely on documented instructions from the Controller;*
b. *Ensure confidentiality of data and restrict access to authorized personnel only;*
c. *Implement appropriate technical and organizational measures to ensure data security;*
d. *Promptly notify the Controller of any data breach, unauthorized access, or incident involving personal data;*
e. *Aid in fulfilling data subjects' rights and regulatory compliance obligations;*
f. *Upon termination of services, delete or return all personal data, unless retention is required by law.*

4. Sub-Processors:

Processors shall not engage sub-processors without prior written consent of the Controller. Where sub-processors are engaged, they must adhere to the same data protection obligations as set out in this DPA.

5. Data Transfers:

Where personal data is transferred across jurisdictions, the Processor must ensure compliance with applicable transfer mechanisms, including:

a. *Standard Contractual Clauses (SCCs) issued by the European Commission; or*
b. *Equivalent contractual protections under applicable privacy laws.*

6. Audit and Compliance Rights

The Controller reserves the right to conduct reasonable audits or assessments (directly or via a third-party auditor) to verify compliance with this DPA. Processors must provide all information necessary to demonstrate compliance.

7. Notification of Breach

Processors shall immediately notify the Controller upon becoming aware of any personal data breach, including:

a. *Nature of the breach,*
b. *Categories and number of affected data subjects,*
c. *Likely consequences, and*
d. *Measures taken to mitigate harm.*

Such notification shall occur within 72 hours of discovery of the breach.

8. Liability and Indemnification:

Each party shall be liable for damages caused by its own processing activities in violation of this DPA or applicable data protection laws. Processors agree to indemnify

and hold harmless the Controller against any claims arising from non-compliance with their obligations under this DPA.

9. Duration and Termination:

This DPA remains in effect as long as the Processor continues to process personal data on behalf of the Controller. Upon termination or expiry, all personal data must be securely deleted or returned to the Controller, as instructed.

10. Governing Law and Jurisdiction:

This DPA shall be governed by and construed in accordance with the laws of India, and subject to the exclusive jurisdiction of the courts in Bangalore, Karnataka, India, without regard to conflict of laws principles.

Executed by:
Ms. Pravallika Paricherla Aka Beulah
_____ *(Signature).*