

VIBEUP Data Processing Agreement

Effective Date: [DATE]

Last Updated: [DATE]

1. Introduction and Scope

This Data Processing Agreement (“DPA”) forms part of the VIBEUP Terms of Service and Privacy Policy and governs the processing of personal data by VIBEUP in compliance with applicable data protection laws, including the European Union General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and other applicable privacy regulations.

2. Definitions

For the purposes of this DPA:

- **“Data Controller”** means the natural or legal person who determines the purposes and means of processing personal data
- **“Data Processor”** means the natural or legal person who processes personal data on behalf of the Data Controller
- **“Data Subject”** means an identified or identifiable natural person whose personal data is processed
- **“Personal Data”** means any information relating to an identified or identifiable natural person
- **“Processing”** means any operation performed on personal data, including collection, use, storage, disclosure, or deletion
- **“Sub-processor”** means any third party engaged by VIBEUP to process personal data
- **“Supervisory Authority”** means an independent public authority responsible for monitoring compliance with data protection laws

3. Role of the Parties

3.1 VIBEUP as Data Controller

VIBEUP acts as a Data Controller when:

- Collecting user registration and profile information
- Processing data for platform operations and service delivery

- Using data for AI matching and personalization algorithms
- Processing data for analytics and platform improvement
- Managing user communications and notifications

3.2 VIBEUP as Data Processor

VIBEUP acts as a Data Processor when:

- Processing data on behalf of Business Account holders for client management
- Handling booking and scheduling data for wellness providers
- Managing community data on behalf of Community Account holders
- Processing payment information on behalf of third-party payment processors

4. Categories of Data Processed

4.1 Personal Data Categories

VIBEUP processes the following categories of personal data:

- **Identity Data:** Name, username, date of birth, profile photos
- **Contact Data:** Email address, phone number, postal address
- **Profile Data:** Wellness interests, intentions, lifestyle preferences, bio information
- **Technical Data:** IP address, device information, usage analytics, log files
- **Location Data:** City/town level location information, travel preferences
- **Communication Data:** Messages, posts, comments, interactions
- **Preference Data:** Account settings, notification preferences, privacy choices
- **Professional Data:** Work experience, skills, business information (for Business Accounts)

4.2 Special Categories of Personal Data

VIBEUP may process limited special categories of personal data:

- **Health and Wellness Data:** General wellness interests and practices (not detailed medical information)
- **Lifestyle Data:** General lifestyle preferences related to wellness and mindfulness

4.3 Data Subjects

Data subjects include:

- Individual users with Personal Accounts

- Business representatives with Business Accounts
- Community members and organizers
- Website visitors and prospective users

5. Purposes of Processing

5.1 Lawful Bases for Processing

VIBEUP processes personal data based on the following lawful bases:

- **Consent:** User consent for AI matching, marketing communications, and optional features
- **Contract Performance:** Processing necessary for platform services and account management
- **Legitimate Interests:** Platform security, fraud prevention, and service improvement
- **Legal Obligation:** Compliance with applicable laws and regulations

5.2 Processing Purposes

Personal data is processed for:

- Platform account creation and management
- AI-powered matching and content personalization
- Communication and notification services
- Location-based discovery and connections
- Community safety and content moderation
- Business analytics and platform improvement
- Legal compliance and dispute resolution

6. Data Subject Rights

6.1 Individual Rights

Data subjects have the following rights under applicable data protection laws:

- **Right of Access:** Request access to their personal data
- **Right to Rectification:** Request correction of inaccurate personal data
- **Right to Erasure:** Request deletion of personal data (“right to be forgotten”)
- **Right to Restrict Processing:** Request limitation of processing activities
- **Right to Data Portability:** Request export of personal data in a structured format

- **Right to Object:** Object to processing based on legitimate interests
- **Right to Withdraw Consent:** Withdraw consent for consent-based processing

6.2 Exercising Rights

Data subjects may exercise their rights by:

- Using in-app privacy controls and settings
- Contacting VIBEUP at privacy@vibeup.io
- Submitting formal requests through designated channels
- Contacting VIBEUP's designated representative (where applicable)

6.3 Response Timeframes

VIBEUP will respond to data subject requests:

- Within 30 days for GDPR requests (extendable to 60 days for complex requests)
- Within 45 days for CCPA requests (extendable to 90 days for complex requests)
- According to applicable local law requirements for other jurisdictions

7. Data Security and Protection

7.1 Technical Safeguards

VIBEUP implements technical security measures including:

- End-to-end encryption for private communications
- SSL/TLS encryption for data in transit
- Secure cloud storage with access controls
- Multi-factor authentication options
- Regular security audits and vulnerability assessments
- Automated content scanning for safety and compliance

7.2 Organizational Safeguards

VIBEUP maintains organizational security measures including:

- Employee data protection training and awareness programs
- Access controls and need-to-know principles
- Data protection impact assessments for high-risk processing
- Incident response and data breach notification procedures
- Regular review and update of security policies and procedures

7.3 Data Breach Notification

In the event of a personal data breach:

- VIBEUP will assess the risk to data subjects
- Supervisory authorities will be notified within 72 hours (where required)
- Data subjects will be notified without undue delay if high risk is determined
- Breach details will be documented and investigated
- Remedial measures will be implemented to prevent future breaches

8. International Data Transfers

8.1 Transfer Locations

Personal data may be transferred to and processed in:

- United States (primary data centers)
- European Union (for EU data subjects)
- Canada (for Canadian users)
- Australia (for Asia-Pacific users)
- Other countries where sub-processors operate

8.2 Transfer Safeguards

International transfers are protected by:

- **Standard Contractual Clauses (SCCs)** for EU data transfers
- **Adequacy Decisions** where applicable
- **Certification Schemes** and approved codes of conduct
- **Binding Corporate Rules** where appropriate

8.3 EU Representative

For EU data subjects, VIBEUP may appoint an EU representative to serve as a local point of contact with supervisory authorities and data subjects regarding data protection matters.

VIBEUP will appoint local representatives as required by applicable data protection laws, including:

- EU representative under GDPR Article 27 (if required)
- UK representative under UK GDPR (if required)
- Other jurisdictional representatives as legally required

Users will be notified of representative appointments through Privacy Policy updates.

9. Sub-processors and Third Parties

9.1 Authorized Sub-processors

VIBEUP engages the following categories of sub-processors:

- **Cloud Infrastructure:** Supabase, Google Cloud Platform
- **Analytics Services:** Google Analytics, Facebook Analytics
- **Communication Services:** SendGrid (email), Twilio (SMS)
- **AI Services:** OpenAI, Anthropic, Cursor, Super Agent
- **Payment Processing:** Stripe
- **Other Service Providers:** As necessary for platform operations

9.2 Sub-processor Obligations

All sub-processors must:

- Provide appropriate technical and organizational security measures
- Process personal data only according to documented instructions
- Maintain confidentiality of personal data
- Assist with data subject rights requests
- Notify VIBEUP of any data breaches
- Delete or return data upon termination of services

9.3 Sub-processor Changes

VIBEUP will:

- Maintain a current list of sub-processors
- Provide notice of new sub-processors or changes
- Allow users to object to new sub-processors
- Provide alternative solutions or account termination for objections

10. Data Retention and Deletion

10.1 Retention Periods

Personal data is retained for:

- **Account Data:** Duration of active account plus 30 days
- **Communication Data:** According to user preferences and legal requirements
- **Usage Analytics:** Aggregated and anonymized after 2 years
- **Legal and Safety Data:** As required by applicable law
- **Business Records:** As required for tax and regulatory compliance

10.2 Deletion Procedures

Upon account deletion or data retention expiry:

- Personal data is permanently deleted from active systems
- Backup copies are deleted according to standard backup cycles
- Aggregated, anonymized data may be retained for analytics
- Legal hold data is retained only as required by law

11. Compliance Monitoring and Audits

11.1 Compliance Monitoring

VIBEUP maintains compliance through:

- Regular review of data processing activities
- Privacy impact assessments for new features or changes
- Monitoring of sub-processor compliance
- Training and awareness programs for employees
- Documentation of processing activities and legal bases

11.2 Audit Rights

Upon reasonable notice, VIBEUP will:

- Provide information necessary to demonstrate compliance
- Allow and contribute to audits conducted by data controllers
- Cooperate with supervisory authority investigations
- Implement recommended improvements from audit findings

12. Data Protection Officer and Contact Information

12.1 Data Protection Contact

For data protection matters, contact:

- **Email:** privacy@vibeup.io
- **Address:** 8 THE GREEN, DOVER, DE 19901
- **EU Representative:** [EU CONTACT] (if appointed)

12.2 Supervisory Authority Contact

EU data subjects may lodge complaints with their local supervisory authority or the lead supervisory authority for VIBEUP's EU operations.

13. Updates and Modifications

13.1 DPA Updates

This DPA may be updated to:

- Reflect changes in applicable data protection laws
- Address new processing activities or technologies
- Improve clarity and compliance effectiveness
- Respond to regulatory guidance or requirements

13.2 Notification

Material changes will be communicated through:

- Email notification to account holders
- Platform notifications and announcements
- Updates to the DPA document with version control
- Reasonable notice period before implementation

14. Termination and Data Return

14.1 Service Termination

Upon termination of services:

- Personal data will be deleted according to retention policies
- Data subjects may request immediate deletion
- Backup data will be deleted according to standard cycles
- Legal hold requirements will be observed

14.2 Data Export

Before account termination, users may:

- Export their personal data through account settings
- Request data export assistance from customer support
- Receive data in commonly used, machine-readable formats
- Transfer data to alternative service providers

15. Governing Law and Jurisdiction

This DPA is governed by:

- **Primary Jurisdiction:** Delaware, United States
- **EU Data Subjects:** Applicable EU member state law and GDPR
- **Other Jurisdictions:** Local data protection laws where applicable

16. Effective Date and Acceptance

This DPA becomes effective upon your use of VIBEUP services and acceptance of the Terms of Service and Privacy Policy. Continued use of services constitutes acceptance of any updates to this DPA.

Last Updated: [DATE]