JOINBASH DATA POLICY

Last Updated: February 2, 2026
Effective Date: February 2, 2026
Version: 1.0

1. INTRODUCTION

This Data Policy provides detailed information about how EAO Holdings LLC ("EAO Holdings," "Company," "we," "us," or "our") collects, processes, stores, and protects data through the JoinBash platform.

This document supplements our Privacy Policy with technical and procedural details about our data handling practices. Please read both documents to fully understand how we handle your information.

2. DATA COLLECTION METHODS

2.1 USER INPUT

We collect data you directly provide through account registration, profile creation and editing, event creation, review and rating submissions, payment information entry, identity verification, and support requests or communications.

2.2 AUTOMATED COLLECTION

We automatically collect data when you use the platform, including authentication tokens and session data, device identifiers, app usage patterns and timestamps, IP addresses during verification, and push notification delivery data.

2.3 THIRD-PARTY AUTHENTICATION

We receive data from authentication providers when you sign in, including your email, name, and profile photo URL from Google Sign-In, your email and name from Apple Sign-In (as permitted), and information you provide via email/password authentication.

2.4 WEBHOOK DATA

We receive data from third-party services, including payment confirmations and transaction status from payment processors, and verification results and risk assessments from identity verification providers.

2.5 FILE UPLOADS

We collect user-uploaded content, including profile photos, event images, identity documents for

KYC, and expense proof documents.

==

3. DATA CLASSIFICATION

==

We classify data into categories based on sensitivity:

3.1 PUBLIC DATA

The following information is visible to other platform users, display name, profile photo, bio (if public), public events you create, and event reviews you post, and is displayed on the platform and cached for performance

3.2 PRIVATE DATA

The following information is visible only to you and authorized platform operations, email address, phone number, date of birth, gender, location, interests, saved events, and notification preferences, and is encrypted at rest with access controls in place.

3.3 SENSITIVE DATA

The following data requires enhanced protection, password hashes, government ID documents, biometric verification data, facial recognition data, and addresses from identity documents, and is encrypted at rest and in transit, with strict access controls, limited retention, and processing only by certified providers.

3.4 FINANCIAL DATA

Payment and transaction information, including platform credit balances, transaction history, payment processor identifiers, and withdrawal records, is encrypted, processed through PCI-DSS compliant providers, and retained for seven years for compliance purposes.

==

4. DATA STORAGE INFRASTRUCTURE

==

We use industry-standard cloud service providers to store and process data. Our infrastructure includes:

4.1 PRIMARY DATABASE

We use an industry-standard cloud database service to store data such as user accounts, events, groups, transactions, and reviews, with encryption at rest and in transit, network isolation, automated backups, and industry-recognized security certifications.

4.2 FILE STORAGE

We use an industry-standard cloud storage service to store profile photos, event images, and uploaded documents, with server-side encryption, access control via signed URLs, and lifecycle policies for data retention.

4.3 AUTHENTICATION

We use an industry-standard authentication service that processes user credentials and authentication tokens, secured through token-based authentication, automatic token refresh, and secure session management.

4.4 CACHING

We use an industry-standard caching service to store session tokens and temporary verification codes, with security measures including in-memory storage, short retention periods, and automatic expiration.

4.5 EMAIL DELIVERY

We use an industry-standard email delivery service to process email addresses and notification content, secured through TLS encryption and industry-standard email authentication protocols.

==

5. DATA PROCESSING ACTIVITIES

==

5.1 AUTOMATED PROCESSING

A. Event Recommendations

We use a matching algorithm that analyzes your interests, location, and past event attendance to generate a ranked list of recommended events for you. This process is used solely for personalization purposes and does not have a legally or otherwise significant impact on you.

B. Host-Defined Eligibility Filtering

Event listings are filtered using user profile attributes and eligibility criteria set by Hosts. The Platform does not impose or endorse discriminatory restrictions, and Hosts are solely responsible for ensuring their eligibility criteria comply with applicable laws.

C. KYC Verification

Identity documents, facial photos, and personal information are processed by a certified third-party provider using automated document and biometric analysis to produce a verification decision (approved, rejected, or review required). This process has a significant impact as it affects access to financial features, and users retain the right to request a human review.

D. Payment Processing

Payment card details and transaction amounts are processed by a PCI-DSS-compliant payment processor to authorize and capture transactions, resulting in a payment success or failure and enabling execution of financial transactions.

E. Fraud Detection

Transaction patterns, account activity, and device information are analyzed to identify suspicious behavior and assign risk scores, generating risk flags for manual review. This process may result in temporary account restrictions, subject to human review.

5.2 MANUAL PROCESSING
Certain activities are handled by human reviewers, including customer support inquiries, dispute resolution cases, content moderation appeals, manual KYC reviews for accounts in “review” status, and investigations into potential Terms violations.

==

6. DATA RETENTION SCHEDULE

==

6.1 RETENTION PERIODS

Data Category	Retention Period	Legal Basis
Active user account	Account lifetime	Contract
Deleted account (soft)	30-90 days	Recovery window
Deleted account (hard)	Permanently deleted	User request
Transaction records	7 years	Financial regulations
KYC verification data	5 years post-activity	AML compliance
Event data (completed)	2 years	Platform operations
Event review	Indefinite (anonymous)	Platform integrity
Device Token	Until logout/refresh	Service operation
Push notification logs	90 days	Debugging
Server/access logs	90 days	Security
Support tickets	3 years	Service improvement
Marketing consent records	Duration + 3 years	Compliance proof

6.2 SOFT DELETE PROCESS
When a user requests account deletion, the deletion request is received, the account is marked for deletion, excluded from active queries, login access is disabled, and the public profile is

hidden on Day 0.

From Day 1 to Day 30, the account enters a recovery window during which the user may contact support to restore the account. During this period, data is retained but remains inaccessible.

On Day 31, hard deletion is initiated, personal data is permanently removed, profile photos are deleted, authentication records are deleted, and deletion requests are sent to applicable third-party providers.

Transaction records are retained for seven (7) years in anonymized form, KYC data is retained in accordance with regulatory requirements, and reviews may be anonymized and retained.

6.3 HARD DELETE PROCESS

Permanent deletion includes the deletion of database records, removal of file storage objects, deletion of authentication records, cache invalidation, and the submission of third-party data deletion requests where permitted by law or contractual obligations.

==

7. DATA SUBJECT RIGHTS

==

7.1 RIGHT TO ACCESS

You have the right to request a copy of all personal data we hold about you. To exercise this right, you must submit a request to privacy@joinbash.com. We will verify your identity to prevent unauthorized access, compile the requested data within 30 days, and deliver the data securely.

The exported data will be provided in a structured JSON file, with media files delivered in their original formats and a PDF summary included for readability. The data package may include your profile information, events created and attended, transaction history, reviews you have posted, notification preferences, device information, and your KYC verification status (excluding identity documents).

7.2 RIGHT TO RECTIFICATION

You have the right to request correction of inaccurate or incomplete personal data. Profile information may be updated directly through the app settings, or you may request support assistance by contacting privacy@joinbash.com. If the requested change involves identity-related data, additional verification may be required. Once the correction is completed, you will receive confirmation of the update.

7.3 RIGHT TO ERASURE

You have the right to request deletion of your personal data. Deletion requests may be submitted through the app or by email. Upon receiving a request, we will check for any outstanding obligations, initiate a soft delete, provide a 30-day recovery period, and then execute a hard delete. A confirmation will be sent once the process is complete.

Certain data may be retained where legally required, including transaction records, KYC data retained for regulatory compliance, data necessary for legal claims, and anonymized analytics.

7.4 RIGHT TO RESTRICTION

You may request that we restrict the processing of your personal data. Requests must specify the desired restrictions and will be reviewed and implemented where applicable. You will receive confirmation once the restrictions have been applied.

During a restriction period, we will only process your data for storage purposes, legal claims, protection of the rights of others, or reasons of important public interest.

7.5 RIGHT TO DATA PORTABILITY

You have the right to receive your personal data in a machine-readable format. To exercise this right, you must submit a portability request, after which we will prepare a data export in JSON format and provide a secure download link that expires after 24 hours.

Portable data includes personal data you provided to us and data generated from your use of the Platform.

7.6 RIGHT TO OBJECT

You may object to the processing of your personal data where processing is based on our legitimate interests, in which case we will cease processing unless compelling legitimate grounds exist. You may also object to direct marketing, which will result in immediate cessation, and to profiling used for event recommendations.

7.7 AUTOMATED DECISION RIGHTS

Where automated decisions produce significant effects, such as KYC verification outcomes, you have the right to request human review, express your point of view, contest the decision, and obtain an explanation of the logic involved in the decision-making process.

7.8 RESPONSE TIMEFRAMES

Standard data protection requests are processed within 30 days. Complex requests may take up to 90 days, in which case you will be notified. Requests under the CCPA are processed within 45 days. Emergency requests may receive expedited handling where applicable.

==

8. THIRD-PARTY DATA PROCESSING

==

8.1 DATA PROCESSING AGREEMENTS

We maintain Data Processing Agreements (DPAs) with all service providers that process personal data on our behalf. These agreements are designed to ensure compliance with applicable data protection laws, including the GDPR, and include Standard Contractual Clauses for international data transfers where required. They also impose data minimization obligations, define security commitments, and require timely breach notification.

8.2 SERVICE PROVIDER CATEGORIES
Our service providers include:

Category	Purpose
Authentication provider	User authentication, notifications
Payment processor	Payment processing
Identity verification	KYC compliance
Cloud infrastructure	Hosting, storage
Database provider	Data persistence
Email delivery	Transactional communications

8.3 INTERNATIONAL TRANSFERS
Where personal data is transferred outside your jurisdiction, appropriate safeguards are implemented to ensure adequate protection. These safeguards include the use of Standard Contractual Clauses for transfers from the European Union, Data Processing Addenda with all processors, reliance on adequacy decisions where applicable, and the implementation of supplementary measures as required by law.

==

9. SECURITY MEASURES

==

9.1 TECHNICAL CONTROLS
We implement industry-standard encryption protocols to protect personal data during transmission and encrypt stored data at rest. User passwords are secured using industry-standard hashing algorithms, and additional encryption is applied to sensitive data fields where appropriate.

Access to personal data is strictly controlled through role-based access control (RBAC), token-based authentication mechanisms, and secured APIs. Access permissions are granted based on the principle of least privilege to ensure users and systems only have access to data necessary for their functions.

Our network infrastructure is protected through network isolation, firewall controls, distributed denial-of-service (DDoS) protection, and rate-limiting measures to prevent abuse and unauthorized access.

Application-level security measures include input validation and sanitization, properly configured cross-origin resource sharing (CORS) policies, cross-site request forgery (CSRF) protection, injection prevention mechanisms, and safeguards against cross-site scripting (XSS) attacks.

9.2 OPERATIONAL CONTROLS

We maintain operational security through regular security awareness training for personnel, periodic access reviews, documented incident response procedures, ongoing vulnerability management, and routine security assessments. System activity is logged and monitored to detect and respond to potential security incidents.

9.3 COMPLIANCE CERTIFICATIONS

Our service providers maintain industry-recognized security certifications and compliance standards, including PCI-DSS for payment processing, ISO/IEC 27001, and SOC 2, to ensure the protection of personal data and system integrity.

==

10. DATA BREACH PROCEDURES

==

10.1 DETECTION

The Platform employs automated monitoring and alerting, log analysis, security monitoring tools, and user reports to detect potential security incidents.

10.2 ASSESSMENT

Upon suspicion of a data breach, immediate containment measures are taken, followed by an assessment of the scope and impact. The categories of affected data are determined, the risk level is classified, and a root cause analysis is performed.

10.3 NOTIFICATION

Internal escalation occurs immediately upon detection. Regulatory notifications are made as required by applicable law, including notification to supervisory authorities within 72 hours under GDPR if there is a risk to individuals, notifications under CCPA as required by California law, and notifications in other jurisdictions in accordance with local legal obligations.

For high-risk breaches, affected users are notified without undue delay. Notifications include the nature of the breach, the data affected, measures taken, and recommended user actions, delivered via email and/or in-app notifications.

10.4 DOCUMENTATION

All security incidents and breaches are fully documented, including the date and time of detection, the nature of the incident, data categories affected, the number of individuals affected, measures taken, notifications sent, and findings from the post-incident review.

==

11. COOKIES AND TRACKING

==

11.1 MOBILE APPLICATION

Our mobile application uses local storage to retain user preferences and session data, device tokens to enable push notifications, and aggregated, non-identifying analytics to improve the service.

11.2 TRACKING TECHNOLOGIES

Technology	Purpose	Duration
Session tokens	Authentication	Session
Device tokens	Push notifications	Until logout
Preference storage	User settings	Persistent
Analytics data	Usage analytics (aggregate)	Per service terms

11.3 MANAGING PREFERENCES

You can manage tracking and notifications through your app notification settings, device privacy settings, account preferences, or by contacting privacy@joinbash.com.

==

12. CHILDREN'S DATA

==

12.1 AGE REQUIREMENTS

Users must be at least 18 years old to use the Platform. We do not knowingly collect personal data from users under 18, and age verification may be required for certain features.

12.2 PARENTAL NOTIFICATION

If we discover personal data from a user under 18, all data processing will cease, the parent or guardian will be notified if contact information is available, the data will be promptly deleted, and the account will be terminated.

12.3 COPPA COMPLIANCE

We comply with the Children’s Online Privacy Protection Act (COPPA). Our services are not directed at children under 13, we do not intentionally collect data from children, and any such data discovered will be promptly deleted.

==

13. REGIONAL COMPLIANCE

==

13.1 EUROPEAN UNION (GDPR)

For users in the EU/EEA, all data processing activities are documented with legal bases, and data subject rights are fully honored. Appropriate safeguards, including Standard Contractual Clauses (SCCs), are implemented for international data transfers. Data Protection Impact Assessments are conducted where required, and users have the right to lodge complaints with supervisory authorities.

13.2 CALIFORNIA (CCPA/CPRA)

For California residents, users have the right to know the categories and purposes of personal information collected, the right to request deletion of personal information, the right to correct inaccurate information, and the right to opt out of the sale of personal information.

NO SALE OF PERSONAL INFORMATION:

JoinBash does not sell, rent, or share personal information for cross-context behavioral advertising purposes and does not disclose personal information to third parties for their direct marketing purposes.

Categories of Personal Information Collected:

The categories of personal information collected include identifiers (such as name, email, and phone number), financial information (including transaction history), biometric information for KYC purposes, internet activity and usage data, geolocation information related to events, professional information for Hosts, and inferences used for interest-based recommendations.

13.3 OTHER JURISDICTIONS

We strive to comply with applicable data protection laws in all jurisdictions where the Platform operates. Users may contact us for inquiries regarding specific local compliance requirements.

==

14. DATA GOVERNANCE

==

14.1 RESPONSIBILITY

EAO Holdings LLC serves as the data controller for JoinBash.
Privacy Contact: privacy@joinbash.com

14.2 DATA PROTECTION PRACTICES

We follow privacy by design principles and implement data minimization, purpose limitation, and storage limitation measures. Regular compliance reviews are conducted to ensure adherence to these practices.

14.3 VENDOR MANAGEMENT
All data processors undergo due diligence before engagement, and contractual data protection requirements are established. Regular compliance assessments are performed, and vendors are required to promptly notify us of any security or data protection incidents.

===

15. APP STORE PROVIDERS

===

JoinBash is available through Apple App Store and Google Play Store. Please note that Apple Inc. and Google LLC are not parties to this Data Policy and are not responsible for the JoinBash application or its content. Your use of the app stores is subject to their respective terms and privacy policies.

===

16. UPDATES TO THIS POLICY

===

We may update this Data Policy from time to time. Material changes will be posted on the Platform and notified via email. Changes take effect after a reasonable notice period. Users should review the "Last Updated" date to see when this policy was last revised.

===

17. CONTACT INFORMATION

===

For questions about these Terms, please contact us:
EAO Holdings LLC
Email: privacy@joinbash.com
Address: 5900 BALCONES DRIVE SUITE 100 AUSTIN, TX 78731

Response Time: Within 30 days

For EU users, you may also contact your local data protection authority.

===

This Data Policy is part of and supplements the JoinBash Privacy Policy and Terms of Service.

EAO Holdings LLC
A Wyoming Limited Liability Company

END OF DATA POLICY