



Passly Privacy Policy

Effective Date: 01/08/2026 | Last Updated: 01/08/2026 | Document Version: 2026-08-01

1. Introduction and Overview

Passly (hereinafter referred to as “we,” “us,” “our,” or the “Company”) recognizes the paramount importance of safeguarding your privacy and is dedicated to the comprehensive protection of your personal data. This Privacy Policy document (hereinafter “Policy”) has been meticulously crafted to delineate with precision how we collect, process, utilize, disclose, and implement protective measures for your personal information in strict accordance with applicable global data protection frameworks, including but not limited to the General Data Protection Regulation (EU) 2016/679 (“GDPR”), the California Consumer Privacy Act of 2018 (“CCPA”), the Kenya Data Protection Act, 2019, and other relevant data protection laws and regulations that may apply to our operations and your jurisdiction.

By accessing, installing, registering for, or utilizing the Passly platform (hereinafter referred to as the “Platform”), which encompasses our website, mobile applications, and related digital services, you hereby acknowledge that you have thoroughly read, comprehensively understood, and unequivocally consented to the collection, processing, utilization, and disclosure of your personal data as meticulously detailed within this Privacy Policy. If you disagree with any aspect of this Policy, we respectfully request that you discontinue use of our Platform immediately.

2. Scope and Applicability of this Privacy Policy

This Privacy Policy applies, without limitation, to all individuals who interact with the Passly Platform or attend an event at which Passly facilitates or commissions photography, audio recording, or video recording, including but not limited to registered account holders, occasional visitors, event organizers, ticket purchasers, attendees, guests, performers, vendors, and any entity engaging with our services in any capacity whatsoever. The Policy elucidates with granularity the categories of personal data we collect, the methodologies employed in processing such data, the purposes for which data is processed, the legal bases for such processing, and the comprehensive rights you possess regarding your information.

This Privacy Policy shall be binding upon all territories and jurisdictions wherein the Passly Platform is accessible, subject to variations that may be necessitated by local legal requirements. In cases of jurisdictional conflicts, specific addenda may be appended to this Policy to ensure full compliance with local regulations.

3. Detailed Information We Collect

Passly collects various categories of personal data from users, with the scope and nature of collected information contingent upon the specific manner and extent of your interaction with the Platform. The data we collect is classified into the following comprehensive categories:

a. Account and Registration Information

When you establish an account on the Passly Platform, we collect and process the following personal identifiers:

- Complete legal name (first, middle, and last names where applicable)
- Email address (primary and secondary, if provided)
- Contact telephone number(s), including country code
- Cryptographically secured and irreversibly encrypted password
- Account creation timestamp and geographical location
- Terms of service acceptance records

b. Comprehensive Transactional and Payment Information

To facilitate secure ticket purchases, resales, and other financial transactions on our Platform, we collect and process:

- Username and associated email address for transactional record-keeping
- Unique User Identifier (UUID) for audit and verification purposes (Note: This UUID is rendered functionally irrelevant and inaccessible upon permanent account deletion)
- Payment method particulars, which may include but are not limited to:

- Mobile money account details (where applicable)
- Credit/debit card type, expiration date, and last four digits (Note: Full payment card numbers are never stored on our systems)
- Digital wallet identifiers
- Transaction timestamps, amounts, and descriptors
- Billing address information
- Transaction history and purchase patterns

Important Notice: All payment transactions are processed through secure third-party payment service providers (Paystack) who maintain PCI DSS (Payment Card Industry Data Security Standard) compliance. Passly does not store complete payment card numbers, CVV codes, or similar sensitive financial data on our servers.

c. Profile and Preference Information

Should you elect to personalize your user experience on the Platform, we may collect and process:

- Profile picture or avatar (entirely optional)
- Public biographical information (entirely optional)
- Event preferences and categorizations
- Notification preferences and communication settings
- Saved venues, artists, or event categories of interest
- User interface customization settings
- Location preferences for event discovery
- Language and accessibility preferences

d. Device and Technical Information

For security enhancement, service optimization, and analytical purposes, we collect and process:

- Device type, model designation, and manufacturer
- Operating system version, build number, and device identifiers
- Internet Protocol (IP) address and approximate geolocation
- Language and regional settings
- Browser type and version (for web access)
- Connection type and network information

e. Analytics and Usage Data

To continuously improve user experience, service quality, and Platform performance, we track and analyze:

- Application usage metrics (session duration, screen view sequences, interaction patterns)
- Feature engagement statistics and service utilization patterns
- Error reports, crash analytics, and debugging logs
- Feature adoption rates and abandonment patterns
- Performance benchmarks and response time metrics
- Search queries and results interaction
- Content engagement patterns

Analytics and Diagnostics Provider Notice: We use PostHog to understand feature usage, navigation, and aggregate service performance. We use Sentry to receive crash reports, diagnostic information, performance traces, and sampled session replays that help us identify and fix technical issues. These services process the data described in this Policy only to provide analytics, diagnostics, and service-improvement functions for Passly. You may review their independent privacy policies at posthog.com/privacy and sentry.io/privacy.

f. Communication and Customer Support Data

When you contact our customer support team or engage with our communication channels, we may collect:

- WhatsApp phone number and messaging consent status
- WhatsApp message metadata (such as delivery/read status where available)
- Correspondence content and timestamps
- Support ticket information and resolution details
- Feedback submissions and survey responses

- Communication preferences and history
- Call recordings (with prior notification)
- Chat transcripts and interaction logs

g. Event Photography, Audio, and Video

At selected events facilitated by Passly, we may commission or create photographs, audio recordings, and video recordings for Passly's own editorial, educational, promotional, and marketing materials. These recordings may include:

- Your identifiable image, likeness, voice, appearance, and actions at the event
- The event name, date, venue, and the context in which the recording was made
- Any name, role, testimonial, or interview response that you separately choose to provide

Where you are identifiable, Passly will provide notice and obtain express consent before making or using the recording for these purposes. Notices may be provided during ticket registration, at event entry, on signs in recording areas, or directly by the photographer or production team. We will provide a practical way to decline recording or request an alternative non-recorded area where reasonably available. Attendance or ticket purchase alone does not constitute consent to identifiable promotional recording.

We do not use event recordings for facial recognition, biometric identification, or automated decision-making. Photography or recording by an Event Organizer or another independent third party for its own purposes is governed by that party's privacy notice, unless Passly jointly determines the purpose and means of the recording.

4. Comprehensive Use of Your Information

We process your personal data for the following specific, explicit, and legitimate purposes:

- To create, authenticate, maintain, and manage your user account and profile
- To facilitate secure ticket purchases, transfers, resales, and related transactions
- To send service communications via WhatsApp, email, push, and in-app channels, including ticket confirmations, reminders, support, and service updates
- To provide personalized customer support and efficiently address user inquiries
- To customize and continuously improve user experience based on preferences and behavior patterns
- To conduct sophisticated data analysis to enhance Platform performance, stability, and security
- To communicate service updates, promotional offers, and critical notifications in accordance with your communication preferences
- To detect, prevent, and mitigate fraudulent activities, security breaches, unauthorized access attempts, and technical issues
- To develop and enhance new features and services based on user feedback and engagement patterns
- To generate aggregated, anonymized statistical data for internal business intelligence
- With express consent, to create, edit, publish, distribute, and display event photographs, audio, and video in Passly's websites, applications, social media, presentations, press materials, advertising, training resources, and media or marketing guides
- To maintain compliance with applicable legal and regulatory requirements
- To enforce our Terms of Service, User Agreement, and other applicable policies
- To protect the rights, property, or safety of Passly, our users, or the public as required or permitted by law

Legal Bases for Processing (GDPR Compliance)

For users protected by the GDPR, we process personal data under one or more of the following legal bases:

- Contractual Necessity: Processing necessary for the performance of our contract with you
- Legitimate Interests: Processing necessary for our legitimate interests, provided these interests do not override your fundamental rights and freedoms
- Legal Obligation: Processing necessary for compliance with a legal obligation to which we are subject
- Consent: Processing based on your freely given, specific, informed, and unambiguous consent

5. Data Sharing, Disclosure, and International Transfers

a. Third-Party Service Providers and Data Processors

We may engage and share your information with trusted third-party service providers who perform services on our behalf, subject to appropriate contractual safeguards. These providers include, but are not limited to:

- Payment processors and financial institutions to securely handle and verify transactions

- Analytics and diagnostics providers (such as PostHog and Sentry) to improve Platform performance, user experience, and technical reliability
- Cloud hosting and infrastructure providers to securely store and process data
- Customer support and ticketing system providers
- Email delivery and communication service providers
- Photographers, videographers, editors, production agencies, printers, publishers, and social media or advertising platforms that help us create and distribute consented event media
- Fraud detection and security enhancement services
- IT and system maintenance service providers
- Legal and professional advisors

All third-party service providers are contractually obligated to use your personal data solely for the purposes specified by us and in compliance with this Privacy Policy and applicable data protection laws.

b. Legal and Regulatory Requirements

We may disclose personal data if required to do so by law, court order, or governmental or regulatory authorities to:

- Comply with applicable legal obligations in relevant jurisdictions
- Respond to lawful requests from government agencies, law enforcement, or judicial bodies
- Enforce or apply our Terms of Service and other agreements
- Protect and defend the rights, property, or safety of Passly, our users, or others
- Detect, investigate, and prevent fraud, security breaches, or technical issues
- Facilitate corporate transactions, such as a merger, acquisition, or asset sale (subject to appropriate confidentiality measures)

c. International Data Transfers

If you access or use Passly from locations outside our primary server locations, your data may be transferred to, stored, and processed in jurisdictions with differing privacy regulations and data protection standards. By using our Platform, you consent to such transfers.

We implement appropriate safeguards to ensure that your personal data receives an adequate level of protection when transferred internationally, which may include:

- Standard Contractual Clauses approved by the European Commission
- Binding Corporate Rules for transfers between our entities
- Derogations for specific situations as permitted by applicable law
- Data Protection Addenda with third-party service providers
- EU-US Data Privacy Framework certification (where applicable)

6. Data Retention and Deletion Policies

We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, including operational requirements, legal obligations, dispute resolution, and compliance with regulatory frameworks.

Retention Periods

- Active accounts: All account data is retained for the duration of your account's existence and active usage
- Inactive accounts: Data may be archived after 24 months of inactivity, with prior notification
- Account deletion: Upon account deletion, personal data is permanently removed from our active systems within 30 days, unless retention is required by law
- Transactional data: Basic transaction records may be retained for up to 7 years for tax, accounting, and legal compliance purposes
- Transactional UUIDs: These identifiers become irrelevant and functionally inaccessible upon account deletion
- Analytics data: Usage data is anonymized after 36 months
- Communication records: Support tickets and communication logs are retained for 24 months after resolution
- Event media: Unselected source photographs and recordings are ordinarily deleted within 12 months after the event. Media selected for Passly materials, together with the related consent record, may be retained for up to 5 years after its most recent publication or use, subject to an annual review and any valid withdrawal, objection, legal hold, or longer period required by law

User Control Mechanisms

Passly provides comprehensive in-app functionality for users to:

- Download a complete copy of their personal data in a structured, commonly used, and machine-readable format
- Request deletion of their accounts and associated personal data
- Update or correct inaccurate personal information
- Manage communication preferences and notification settings

Consistent with Apple's privacy practices, we retain personal data associated with your account for as long as your account is active or as needed to provide you with requested services. If you delete your account, we will delete or anonymize your information unless we need to retain certain information to comply with legal or regulatory requirements, resolve disputes, prevent fraud and abuse, or enforce our agreements.

7. Your Comprehensive Rights Under Applicable Data Protection Laws

a. General Data Protection Regulation (GDPR - EU Users)

If you are located in the European Economic Area (EEA), you have the following rights under the GDPR:

- Right to Access: The right to request confirmation of whether we process your personal data and, if so, to obtain a copy of such data along with specific information about the processing
- Right to Rectification: The right to request correction of inaccurate personal data or completion of incomplete personal data
- Right to Erasure (Right to be Forgotten): The right to request the deletion of your personal data under certain circumstances
- Right to Restriction of Processing: The right to request the limitation of processing your personal data under specific conditions
- Right to Data Portability: The right to receive your personal data in a structured, commonly used, and machine-readable format and to transmit such data to another controller
- Right to Object: The right to object to the processing of your personal data on grounds relating to your particular situation
- Right Not to be Subject to Automated Decision-Making: The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects or similarly significantly affects you
- Right to Withdraw Consent: The right to withdraw your consent at any time, where processing is based on your consent

b. California Consumer Privacy Act (CCPA - California Residents)

If you are a resident of California, you have the following rights under the CCPA:

- Right to Know: The right to request information about the personal information we collect, use, disclose, and sell about you
- Right to Delete: The right to request deletion of personal information we have collected about you
- Right to Opt-Out: The right to opt-out of the sale of your personal information (Note: Passly does not sell personal information as defined by the CCPA)
- Right to Non-Discrimination: The right not to receive discriminatory treatment for exercising your privacy rights

c. Kenya Data Protection Act, 2019

If you are located in Kenya, you have the following rights under the Kenya Data Protection Act:

- Right to Information: The right to be informed about the collection and use of your personal data
- Right to Access: The right to access your personal data and information about how it is processed
- Right to Correction: The right to have inaccurate personal data corrected or completed
- Right to Deletion: The right to have your personal data deleted under certain circumstances
- Right to Data Portability: The right to receive your personal data in a structured, commonly used, and machine-readable format
- Right to Object: The right to object to the processing of your personal data in certain circumstances
- Right to Protection: The right to protection from processing that is unnecessary or disproportionate to the purpose

d. Exercise of Rights and Response Timeline

To exercise any of these rights, you may contact us using the contact information provided in Section 14 of this Policy. We will respond to all legitimate requests within the timeframes mandated by applicable law (typically within 30 days for GDPR requests). We may need to verify your identity before processing certain requests to ensure the security of your personal data.

For any privacy-related inquiries, you may contact our designated Data Protection Officer at: privacy@passly.co.ke.

You may withdraw consent to future use of identifiable event media at any time by emailing privacy@passly.co.ke with the event name, date, and enough information to identify the relevant recording. Withdrawal does not affect processing that was lawful before withdrawal. We will stop new uses and remove the media from channels under our control where reasonably practicable, but may be unable to recall printed materials already distributed or copies independently shared by others.

8. Comprehensive Security Measures

We implement and maintain stringent administrative, technical, and physical security measures designed to protect your personal data from unauthorized access, disclosure, alteration, and destruction. Our security protocols include, but are not limited to:

- End-to-end encryption for data transmission
- Advanced data encryption at rest for sensitive information
- Multi-factor authentication for access to critical systems
- Regular security audits and vulnerability assessments
- Strict access controls and permissions management
- Employee training on data protection and security practices
- Intrusion detection and prevention systems
- Regular security updates and patch management
- Data backup and disaster recovery protocols
- Physical security measures at our facilities

However, despite our best efforts, no security system is impervious to all potential threats. We cannot guarantee the absolute security of your personal data during transmission or while stored on our systems. We strongly advise users to adopt safe online practices, including:

- Creating strong, unique passwords
- Enabling two-factor authentication where available
- Regularly updating device software and applications
- Being vigilant against phishing attempts
- Avoiding public or unsecured Wi-Fi networks for sensitive transactions
- Logging out of your account after each session

In the event of a data breach that may compromise your personal data, we will notify you and the relevant supervisory authorities in accordance with applicable law and take appropriate measures to mitigate any potential harm.

9. Children's Privacy Protections

Creating a Passly User Account, acting as an Event Organizer, reselling Tickets, receiving payments, or entering another legally binding transaction through the Platform requires you to be at least 18 years old or the applicable age of majority in your jurisdiction, whichever is greater. This account requirement does not mean that every Event is inaccessible to people under 18. Events may include minors, and Passly may handle purchaser, attendee, and guest-purchase data where necessary to provide the ticketing service, with the lawful consent and protections required for the relevant person and purpose. Passly will not intentionally make or publish an identifiable promotional photograph, audio recording, or video recording of a child without verifiable consent from the child's parent or legal guardian and an assessment that the use protects and advances the child's rights and best interests.

If you believe that we may have inadvertently collected personal data from or about a child under the applicable age, please contact us immediately at privacy@passly.co.ke, and we will take appropriate steps to investigate and address the issue, including the prompt deletion of any such data.

Parents or legal guardians who believe that their child has submitted personal information to our Platform without their consent may request the removal of the information by contacting us.

We will provide non-recorded or camera-free arrangements where reasonably practicable for children who do not have the required consent. We will not condition a child's access to an event on promotional media consent unless the recording is genuinely necessary for the particular activity and permitted by law.

10. International Data Transfers and Storage

Passly operates globally and may transfer, store, and process your personal data in countries other than your country of residence, including the United States, European Union member states, and other countries with potentially differing data protection laws. By using the Passly Platform, you acknowledge and consent to such international transfers of your personal data.

We employ appropriate safeguards to ensure that your personal data receives adequate protection when transferred internationally, which may include:

- Implementing Standard Contractual Clauses approved by the European Commission
- Adhering to Binding Corporate Rules (BCRs) approved by relevant data protection authorities

- Participating in approved certification mechanisms, such as the EU-US Data Privacy Framework, where the recipient is certified under that framework
 - Obtaining your explicit consent for specific transfers where appropriate
 - Ensuring that recipients of your data are contractually bound to maintain a level of protection equivalent to that required in your home jurisdiction
- Our data storage infrastructure utilizes state-of-the-art cloud services with comprehensive security protocols and redundancy measures to ensure data integrity and availability.

11. Compliance with Apple App Store and Google Play Policies

This Privacy Policy is designed to comply with both Apple App Store Review Guidelines and Google Play's User Data Policy, ensuring complete transparency regarding data collection, usage, sharing, and security practices for applications distributed through these platforms.

For users accessing Passly through iOS devices, we adhere to Apple's privacy standards, including:

- Requesting permission before accessing device data when Apple requires it for a feature, such as photos, camera, location, notifications, calendar, or biometrics
- Disclosing our analytics and diagnostics practices, including PostHog and Sentry, in this Policy and in applicable App Store privacy disclosures
- Using Apple's App Tracking Transparency framework if our data practices require it
- Implementing "Privacy Nutrition Labels" in our App Store listing
- Supporting applicable Sign in with Apple functionality
- Respecting device-level privacy settings

Similar to Apple's practices, we retain personal data associated with your account for as long as your account is active or as needed to provide you with services. If you delete your account, we will delete your information unless we are required to maintain it under applicable law or for legitimate business purposes.

11A. Meta WhatsApp Platform Data Disclosures

If you interact with Passly through the Meta WhatsApp Business Platform, we may receive information made available through WhatsApp APIs and permissions that you authorize.

- We only request and process data needed to provide WhatsApp customer communications and support.
- We do not sell WhatsApp-sourced personal data.
- We use WhatsApp-sourced data in accordance with this Privacy Policy and applicable Meta and WhatsApp Business Platform terms.
- You may stop or limit WhatsApp communications by following the opt-out instructions in our messages or contacting us directly.
- Where required by law or platform rules, we delete or de-identify WhatsApp-sourced personal data when it is no longer needed for the disclosed purpose.

For WhatsApp-related privacy or data deletion requests, contact us at privacy@passly.co.ke and include sufficient account details for verification.

12. Cookies and Similar Technologies

The Passly Platform utilizes cookies, web beacons, pixel tags, and similar technologies to enhance user experience, analyze usage patterns, and improve our services.

You may manage your cookie preferences through your browser settings. However, please note that disabling certain cookies may impact the functionality and features of our Platform.

12A. WhatsApp Communication Basis and Opt-Out

Passly uses WhatsApp as an additional customer communication channel, alongside email, push notifications, and in-app notices, for service-related messages including ticket confirmations, event reminders, transfer notices, account security notices, and support responses.

- Transactional and service messages are sent where necessary to provide the services you request.
- Marketing or promotional WhatsApp messages are only sent where permitted by applicable law and your preferences.
- You may opt out of non-essential WhatsApp messages at any time by following the instructions in the message or contacting privacy@passly.co.ke.

- Opting out of non-essential messages does not affect required service or legal notices.

13. Changes and Updates to this Privacy Policy

We reserve the right to modify, update, or amend this Privacy Policy at any time to reflect changes in our data practices, applicable laws, or Platform functionality. Users will be notified of significant changes to this Policy through:

- WhatsApp notices to the number linked to your account (where enabled)
- Notices on our website homepage
- Email, push notifications, and in-app notifications

Material changes will be effective no less than thirty (30) days following such notification, except where immediate implementation is required by law or to address security concerns. Our notice will identify the updated document version and effective date. Continued use of the Passly Platform after that effective date constitutes acceptance of the updated Privacy Policy. If you do not agree, you should stop using the Platform and contact privacy@passly.co.ke.

We encourage users to periodically review this Privacy Policy to stay informed about our data practices. The "Last Updated" date at the top of this document indicates when this Policy was most recently revised.

14. Contact Information and Data Protection Officer

For any inquiries, concerns, requests regarding your data, or questions related to this Privacy Policy, please contact us at:

Company Name: Passly Events and Ticketing

Email Address: privacy@passly.co.ke

We are committed to addressing your concerns and resolving any complaints about our collection or use of your personal data. If you believe that we have not adequately addressed your concerns, you may have the right to lodge a complaint with your local data protection authority.

15. Governing Law and Dispute Resolution

This Privacy Policy shall be governed by and construed in accordance with the laws of Kenya, without regard to its conflict of law provisions. Any dispute arising from or relating to this Privacy Policy or your use of the Passly Platform shall be subject to the exclusive jurisdiction of the courts of Kenya, except where prohibited by applicable law.

16. Severability

If any provision of this Privacy Policy is found to be unenforceable or invalid under any applicable law, such unenforceability or invalidity shall not render this Privacy Policy unenforceable or invalid as a whole, and such provisions shall be deleted without affecting the remaining provisions herein.

17. Acknowledgment and Acceptance

By using the Passly Platform, you acknowledge that you have read, understood, and agree to be bound by the terms of this Privacy Policy. If you do not agree with any aspect of this Policy, you should immediately discontinue use of our Platform and services.

© 2026 Passly Events and Ticketing. All Rights Reserved.