

MEMVY PRIVACY POLICY

Falcon 9324, LLC

Current as of April 16, 2026

1. Introduction

This Privacy Policy describes how Falcon 9324, LLC ("Memvy," "we," "us," or "our") collects, uses, and shares information when you use the Memvy service, including our native iOS application available through the Apple App Store, our native Android application available through the Google Play Store, our Progressive Web App (PWA), and our website at memvy.com (collectively, the "Service").

We built Memvy to help people capture and share memories with the people who matter to them. Privacy and ownership are part of the product, not an afterthought. Before we get into the details, here is what we want you to know up front:

- **We do not sell your personal information.**
- **We do not sell your behavioral information or browsing activity.**
- **We do not show you advertisements, and we do not share your information with advertisers.**
- **We do not build advertising or marketing profiles about you.**
- **We limit our tracking to what we need to operate, secure, and improve the Service.**
- **Memvy is intended for users age 13 and older. We do not knowingly collect information from children under 13.**

By using the Service, you agree to the practices described in this Privacy Policy. If you do not agree, please do not use the Service.

2. Scope — How You Access Memvy

This Privacy Policy applies to all of the ways you can access Memvy:

- **Apple App Store native app** — the Memvy app installed from the Apple App Store on iPhone and iPad.
- **Google Play Store native app** — the Memvy app installed from the Google Play Store on Android devices.
- **Progressive Web App (PWA) and website** — Memvy accessed through a web browser on a computer, phone, or tablet.

The native apps and the PWA offer substantially the same core Memvy experience, but they are not identical. The native apps have additional capabilities that depend on device-level features (for example, push notifications and certain camera and photo library integrations). Some features available in the native apps may be unavailable, limited, or work differently in the PWA. Where a data practice differs based on how you access the Service, we note the difference in the relevant section below.

Subscription sign-up and payment currently occur through the PWA in all cases, including when you begin the process from inside the native app. See Section 4.1 (Information You Provide Directly) and Section 16 (Third-Party Services) for details.

3. Definitions

For clarity, the following capitalized terms are used throughout this Privacy Policy:

Account. A unique Memvy account created by you to access the Service.

Affiliate. An entity that controls, is controlled by, or is under common control with Falcon 9324, LLC.

Collaborator. A User who has been invited by a Creator to contribute content to a Story. Collaborators must have their own Memvy Account.

Consumer Account. A Memvy Account held by an individual User for personal, non-commercial use.

Corporate Account. A Memvy Account held by an organization for use in connection with that organization's activities. Corporate Accounts include features not available to Consumer Accounts, such as the Permanent Admin function.

Country. The United States of America, where Memvy is operated.

Creator. The User who creates a Story and who owns and controls that Story.

Device. Any device you use to access the Service, such as a computer, phone, or tablet.

Falcon 9324, Memvy, we, us, our. Falcon 9324, LLC, the company that operates the Service.

Native App. The Memvy application distributed through the Apple App Store or the Google Play Store.

Permanent Admin. A Corporate-Account-only role that allows designated individuals to create and administer Stories at the account level. Not available to Consumer Accounts.

Personal Data / Personal Information. Information that identifies, relates to, or could reasonably be linked with you or your household.

Progressive Web App or PWA. The web-based version of Memvy accessed through a browser at memvy.com.

Service. The Memvy applications (Native App and PWA) and the Memvy website, taken together.

Service Provider. A third party that processes information on our behalf to help us operate the Service, under a written contract that limits their use of your information to providing that service to us.

Story. A collection of memories, contributed by a Creator and invited Collaborators, organized for interactive viewing within Memvy.

Usage Data. Information collected automatically when you use the Service, such as IP address, device type, and the pages or screens you view.

User, you, your. The individual using the Service, or, for Corporate Accounts, the organization on whose behalf the individual is using the Service.

Viewer. A person who views a Story. Viewers may or may not have a Memvy Account, depending on how the Creator has published the Story.

4. Information We Collect

We collect four categories of information: information you provide directly to us; content you upload to the Service; information collected automatically; and information collected through device permissions you grant.

4.1 Information You Provide Directly

When you create an Account or use the Service, you may provide us with:

- Your first and last name
- Your email address
- Your phone number (optional)
- A password, which we store only in hashed form using industry-standard bcrypt
- For Corporate Accounts, organization name and authorized contact details
- Information you provide when you contact us for support

For subscriptions, payment is processed by Stripe through the PWA. When you subscribe, Stripe collects your payment card information directly. Memvy does not receive, see, or store your full payment card number. We receive from Stripe a limited set of billing information, which may include your name, billing address, the last four digits of your card, the card brand, and a Stripe customer identifier, so that we can associate the subscription with your Account, provide receipts, and handle renewals and refunds. Stripe's handling of your payment information is governed by Stripe's own privacy policy.

4.2 Content You Upload

Memvy is a platform for User-generated content. When you use the Service as a Creator or Collaborator, you may upload:

- Photographs and other images
- Video recordings
- Audio recordings
- Text, captions, comments, and responses to prompts
- Metadata associated with your uploads (for example, the time the file was created on your Device, the type of Device, and, if present in the file, location information and camera details)

You are in control of what you upload. You can choose whether to include location or other metadata before uploading. We do not require it. See Section 7 (Your Content — Ownership and Control) for how ownership and visibility work.

4.3 Information Collected Automatically

When you use the Service, we automatically collect limited technical information to operate, secure, and improve the Service:

- IP address
- Device type, operating system, and version
- Browser type and version (for PWA and website use)
- App version (for Native App use)
- Pages or screens you view and approximate time spent
- Date and time of access
- Diagnostic and crash data
- General geographic location inferred from IP address (for example, country or region)

We use this information to keep the Service running, to detect and prevent fraud and abuse, and to improve the product. We do not use it for advertising, and we do not sell it.

SDKs and third-party tools in use. The Memvy Native Apps and PWA use a limited set of third-party software development kits (SDKs) for user authentication, payment processing, push notification delivery, and basic product analytics. The specific SDKs we use and their purposes are:

- **Google Identity Services (Google)** — enables secure user authentication via Google accounts.
- **Sign in with Apple (Apple)** — enables secure user authentication via Apple accounts.
- **Facebook Login SDK (Meta)** — enables secure user authentication via Facebook accounts.
- **Stripe (Stripe, Inc.)** — processes Subscription payments securely. Payment details are handled by Stripe and are not stored by Memvy.
- **Firebase Cloud Messaging (Google)** — delivers push notifications and service-related communications to the Native Apps.
- **Firebase (Google)** — supports application functionality, including push notifications and related backend services.
- **Google Analytics (Google)** — helps us understand aggregated usage and improve the Service. Google Analytics is configured with advertising features disabled and ad personalization disabled, so the data is not used for advertising purposes.

A note about authentication SDKs. When you choose to sign in using Google, Apple, or Facebook, the identity provider you select receives information about your authentication with Memvy (for example, the fact that you are authenticating to the Memvy app, the time of authentication, and identifiers associated with your account at that provider). The identity provider's handling of that information is governed by its own privacy policy, not by this Privacy Policy. You can avoid this by signing in with a standard email-and-password account rather than through an identity provider.

Memvy does not use advertising SDKs, behavioral advertising networks, or cross-context tracking SDKs.

4.4 Information Collected Through Device Permissions

Some features of the Service require your permission to access parts of your Device. You control these permissions through your Device settings. The permissions that may apply include:

- **Camera.** To let you capture photos and videos directly within the Memvy Native App.
- **Photo library.** To let you select existing photos and videos to upload. You may grant access to your full library or to selected items only, depending on your Device.
- **Microphone.** To let you record audio within the Service.
- **Push notifications (Native Apps only).** To let us send you notifications about activity in your Stories, account security, and important Service updates. Push notifications are not available through the PWA in the same way. You can disable push notifications at any time in your Device settings.
- **Location.** Memvy does not require precise location access. If location metadata is embedded in a photo or video you upload, you control whether to include or strip that metadata before uploading.

4.5 Cookies and Similar Technologies

The PWA and websites use a limited set of cookies and similar technologies:

- **Strictly necessary cookies** — required for features like signing in, keeping you signed in, maintaining session state, and preventing fraud. Without these, the Service cannot function.
- **Functional cookies** — remember preferences such as language and interface choices so you do not have to re-enter them.
- **Basic analytics (first-party or privacy-respecting)** — help us understand how the Service is used in aggregate so we can improve it.

We do not use advertising cookies and we do not allow third-party advertising networks to set cookies through the Service. You can control cookies through your browser settings. Blocking strictly necessary cookies may prevent the Service from working.

5. How We Use Your Information

We use the information described in Section 4 only for the following purposes:

- To provide, operate, and maintain the Service, including hosting and displaying Stories you create or are invited to contribute to.
- To create and manage your Account, authenticate you, and keep you signed in.
- To process subscription payments (through Stripe) and to provide receipts, renewals, and refunds.
- To communicate with you about your Account, your Stories, security notices, policy changes, and customer support.
- To protect the security of the Service, detect and prevent fraud, abuse, and unauthorized access, and enforce our Terms.
- To comply with legal obligations, respond to lawful requests, and protect our rights and the rights and safety of Users and the public.
- To analyze, troubleshoot, and improve the Service, including fixing bugs, improving performance, and developing new features.
- For Corporate Accounts, to administer the Corporate Account and its Permanent Admin and other account-level features.

What we do not do. We do not sell Personal Information. We do not sell behavioral information. We do not share Personal Information with advertisers or data brokers. We do not build advertising or marketing profiles. We do not use your content, uploads, or viewing activity to target ads, on Memvy or anywhere else. We do not use your content to train generative AI models for our own commercial use or for any third party.

6. How We Share Your Information

We share information only in the limited circumstances described below.

6.1 With Service Providers

We share information with Service Providers who help us operate the Service — for example, our cloud hosting provider (Amazon Web Services), our payment processor (Stripe), email and customer support tools, and crash reporting and analytics providers. Service Providers are bound by written contracts that require them to use information only to provide services to us, protect that information, and not sell or use it for their own purposes.

6.2 Based on Your Sharing Choices

Memvy is a collaborative platform. When you create a Story, you choose how it is shared:

- **Private Story.** Only the Creator and invited Collaborators can access the Story.
- **Public Story.** The Creator makes the Story publicly viewable. Anyone with the link can view it. The Creator controls this choice and can change it.

When you upload content to a Story, that content will be visible to the other Users the Creator has authorized to access the Story, consistent with the Creator's sharing choices. If the Story is Public, your content may be visible to anyone who accesses it. Use good judgment about what you upload.

Sharing by User action is not the same as Memvy sharing your information. We do not share your Account information or your Personal Information with other Users beyond what you have chosen to make visible within a Story.

6.3 For Legal Reasons and Safety

We may disclose information when we believe in good faith that disclosure is necessary to:

- Comply with applicable laws, regulations, subpoenas, court orders, or other valid legal process;
- Cooperate with law enforcement, including in matters involving child safety (see Section 11);
- Enforce our Terms and policies, including investigating potential violations;
- Protect the rights, property, or safety of Memvy, our Users, or others, including to prevent fraud or security incidents.

6.4 Business Transfers

If Falcon 9324, LLC is involved in a merger, acquisition, financing, reorganization, or sale of all or part of its assets, your information may be transferred as part of that transaction. If a transfer will result in a material change in how your information is handled, we will notify you before the change takes effect and, where required, give you a choice about continued use of the Service.

6.5 With Your Consent

We may share information for purposes not described above with your specific consent.

6.6 What We Do Not Share

- We do not share Personal Information with advertisers or advertising networks.
- We do not share Personal Information with data brokers.
- We do not share Personal Information with “business partners” for their own marketing or promotional purposes.

- We do not share Personal Information with our Affiliates for their independent use.

7. Your Content — Ownership and Control

Memvy's approach to content reflects how memories actually work: more than one person can own the same moment.

- **The Creator of a Story** has full, perpetual rights to keep, publish, and repurpose all content contributed to that Story, subject to the Memvy End User License Agreement ("EULA") and applicable law.
- **Each Collaborator** simultaneously retains ownership of content that Collaborator personally submitted and the rights associated with it.

Both parties own. Neither party's ownership excludes the other. The visibility of a Story — private or public — is controlled by the Creator. Within that, you can request that content you personally submitted be removed from a Story; we describe how in Section 9.

You can download copies of content in your Account. If a Subscription ends — whether by cancellation or non-payment — the EULA describes how your content is retained during a two-year Hold Period, how the raw media is offered for download, and what happens after the Hold Period. See Section 17.4 of the EULA and Section 8 of this Privacy Policy for details.

8. Data Retention

We retain your information only as long as we need it for the purposes described in this Privacy Policy or as required by law.

- **Account information** is retained while your Account is active.
- **Story content** is retained in accordance with the Creator's Subscription status. If a Creator's Subscription ends — whether by cancellation or by non-payment — Memvy retains the Creator's Stories (both published and in development) in storage for up to two (2) years from the end of the then-current paid term (the "Hold Period"). The Hold Period applies in every case, whether or not the Creator exercises the download option. For cancellation, the Creator may download the raw media from the Creator's Account at any time during the remainder of the paid term and for at least thirty (30) days thereafter. For non-payment lapse, the Creator is offered a download window of at least thirty (30) days following the end of the paid term. If the Creator re-starts the Subscription during the Hold Period, full access is restored on the terms described in the EULA. If the Creator does not re-start within the Hold Period, the Content is removed from the Service. See Section 17.4 of the EULA for the full description.
- **Usage Data** is retained for a shorter period, only as long as needed for security, troubleshooting, and Service improvement, unless we are required by law to retain it longer.
- **Payment records** are retained as required by tax and accounting law.
- **Records related to child safety and abuse reports** are retained in accordance with applicable law, including preservation obligations under 18 U.S.C. § 2258A.

When information is no longer needed, we delete or de-identify it.

9. Your Rights and Choices

You have rights over the information we hold about you. Some rights apply to all Users; others apply based on where you live (see Sections 14 and 15). Regardless of where you live, you can:

- **Access your information.** Request a copy of the Personal Information we hold about you.
- **Correct your information.** Update inaccurate or incomplete information. Much of this you can do yourself in your Account settings.
- **Delete your Account and information.** You can request deletion of your Account and the Personal Information associated with it. Deletion is available both in-app and through a web resource at memvy.com, so that you can request deletion without installing the app.
- **Export your content.** You can download content associated with your Account.
- **Opt out of non-essential communications.** You can unsubscribe from informational emails at any time. Transactional messages (for example, security alerts and billing notices) will continue while your Account is active.
- **Control device permissions and notifications** through your Device settings and, for push notifications, within the Native App.

To exercise any of these rights, contact us at contact@memvy.com. We will respond within the timeframe required by applicable law and typically within 45 days.

We will not discriminate against you for exercising any of these rights.

10. Children's Privacy — Age 13 and Older

Memvy is intended for Users age 13 and older. We do not knowingly collect Personal Information from children under 13.

If we learn that we have collected Personal Information from a child under 13 without verified parental consent, we will take reasonable steps to delete that information promptly and to close the associated Account.

If you are a parent or guardian and you believe that a child under 13 has provided Personal Information to Memvy, please contact us at contact@memvy.com and we will take appropriate action. Parents and guardians also have the right to review the Personal Information we have collected about their child, to request its deletion, and to refuse to permit its further collection or use.

Because every Collaborator must have their own Memvy Account, the 13-and-older requirement applies to Collaborators as well as to Creators. If you invite a Collaborator, you are representing that the Collaborator is 13 or older.

In jurisdictions where the digital age of consent is higher than 13 (for example, 16 in some countries under the GDPR), users below that local age of consent may be required to obtain parental consent before using the Service, where applicable law requires.

11. Child Safety Standards

Memvy has zero tolerance for child sexual abuse and exploitation. This section sets out our published standards, in accordance with the Google Play Child Safety Standards policy and applicable law, and describes the mechanisms we use to enforce them.

11.1 Prohibited Content and Conduct

The following are strictly prohibited on Memvy:

- **Child Sexual Abuse Material (CSAM)**, meaning any visual depiction — including photographs, videos, and computer-generated imagery — involving a minor engaging in sexually explicit conduct.
- **Child Sexual Abuse and Exploitation (CSAE)**, including any content or behavior that sexually exploits, abuses, or endangers children. This includes grooming a child for sexual exploitation, sextortion of a child, trafficking of a child for sex, and any other form of sexual exploitation of a child.
- Any use of the Service to facilitate contact between an adult and a child for the purpose of sexual exploitation or abuse.
- Any content that sexualizes a minor, including through captioning, commentary, or editing of otherwise non-sexual imagery.
- Any attempt to evade, bypass, or defeat moderation, reporting, or age-related controls in the Service.

Violations will result in immediate removal of the content, termination of the Account, and, where applicable, reporting to law enforcement and the National Center for Missing & Exploited Children (NCMEC).

11.2 In-App Reporting Mechanism

The Service includes an in-app mechanism for Users to report content, Users, and concerns without leaving the app. Reports can be submitted from within the Memvy Native App and the PWA. Reports relating to child safety concerns are prioritized for review.

You may also contact us directly at contact@memvy.com for any child safety concern. If you believe a child is in immediate danger, contact your local law enforcement first.

11.3 Our Response to CSAM and CSAE

When we obtain actual knowledge of CSAM on the Service, we will:

- Remove the content;
- Preserve the content and related records to the extent required by 18 U.S.C. § 2258A and other applicable law;
- Report the content to the National Center for Missing & Exploited Children (NCMEC) through the CyberTipline, as required by U.S. federal law;
- Terminate the Account(s) involved; and
- Cooperate with law enforcement as permitted by applicable law.

When we receive credible reports of CSAE conduct, we will investigate promptly, take appropriate action under our policies, and, where required or appropriate, report to law enforcement.

11.4 Block and Restrict

Users can block other Users and can limit who may contribute to or view their Stories. Creators control Collaborator invitations and can remove a Collaborator from a Story at any time.

11.5 Compliance with Child Safety Laws

Memvy complies with applicable child safety laws and regulations, including the U.S. Children’s Online Privacy Protection Act (COPPA) and the reporting requirements of 18 U.S.C. § 2258A. We maintain the processes necessary to report confirmed CSAM to NCMEC and to cooperate with law enforcement.

11.6 Child Safety Point of Contact

Memvy’s designated Child Safety Point of Contact is the Co-Founder and CEO of Falcon 9324, LLC. Notifications from Google Play, Apple, law enforcement, or other parties regarding potential CSAE content on the Service can be directed to:

- Email: contact@memvy.com (please include “Child Safety” in the subject line)
- Mail: Falcon 9324, LLC, Attn: Child Safety Point of Contact, 1089 Reynolds Farm Rd, Grovetown, GA 30813

11.7 Where These Standards Are Published

These Child Safety Standards are published in this Privacy Policy and are incorporated by reference into the Memvy End User License Agreement. Both are accessible from within the Native App, the PWA, and at memvy.com.

12. Security

We take security seriously and use industry-standard measures to protect your information, including:

- Encryption in transit using HTTPS with TLS 1.2 or higher.
- Encryption at rest within our database and storage layers.
- Password hashing using bcrypt. We do not store passwords in plain text.
- Role-based access control and authentication using secure JSON Web Tokens (JWT).
- Network firewalls and tightly restricted administrative access.
- Continuous monitoring for uptime, performance, and security anomalies.
- Hosting in U.S.-based Amazon Web Services data centers in the US East (N. Virginia) region.

No system is perfectly secure. We cannot guarantee absolute security, but we work to protect your information and to respond quickly if an issue arises. If a data breach occurs that affects your Personal Information, we will notify you and applicable authorities as required by law.

13. International Users and Data Transfers

Memvy is operated in the United States, and our servers and data are hosted in the United States. If you are accessing the Service from outside the United States, your information will be transferred to, stored in, and processed in the United States. Data protection laws in the United States may differ from those in your country.

By using the Service, you consent to the transfer of your information to the United States. Where required by law, we rely on appropriate transfer mechanisms — for example, standard contractual clauses — to protect your information when it is transferred internationally.

14. U.S. State-Specific Privacy Rights

This section describes rights that apply to residents of certain U.S. states. To exercise any right described below, contact us at contact@memvy.com. We will not discriminate against you for exercising your rights.

14.1 California (CCPA / CPRA)

If you are a California resident, you have the right to:

- Know what Personal Information we have collected about you, the sources of that information, the purposes for collecting it, and the categories of third parties with whom it is shared.
- Request deletion of Personal Information we hold about you, subject to limited exceptions.
- Correct inaccurate Personal Information.
- Opt out of the sale or sharing of Personal Information — although, as stated throughout this Privacy Policy, Memvy does not sell or share Personal Information as those terms are defined by the CCPA/CPRA.
- Limit the use and disclosure of sensitive Personal Information — although Memvy does not use sensitive Personal Information to infer characteristics about you.
- Not be discriminated against for exercising these rights. We do not offer financial incentives in exchange for Personal Information.

Categories of Personal Information collected, sources, purposes, and recipients are summarized in Sections 4 through 6 of this Privacy Policy.

14.2 Other State Privacy Laws

Residents of Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Delaware, Iowa, Indiana, Tennessee, Minnesota, Maryland, New Jersey, New Hampshire, Kentucky, Rhode Island, and other states with comparable privacy laws may have rights similar to those described above, including rights to access, correct, delete, and port Personal Information, and to opt out of targeted advertising, sale, and certain profiling. Memvy does not engage in targeted advertising, does not sell Personal Information, and does not engage in profiling that produces legal or similarly significant effects about you.

If applicable law allows an appeal of a denied rights request, you may submit an appeal by replying to our decision or contacting contact@memvy.com with “Appeal” in the subject line.

15. Regional Privacy Rights

15.1 European Economic Area (EEA), United Kingdom, and Switzerland

If you are in the EEA, the UK, or Switzerland, the General Data Protection Regulation (GDPR), the UK GDPR, or the Swiss Federal Act on Data Protection (FADP) may apply to your use of the Service. In that case:

- **Legal bases.** We process your Personal Information on the following legal bases: performance of a contract with you (to provide the Service you have signed up for); our legitimate interests (to secure and improve the Service, and to protect against fraud and abuse); compliance with legal obligations; and, where required, your consent.

- **Your rights.** You have the right to access, correct, delete, restrict, and object to processing of your Personal Information, and the right to data portability. Where processing is based on consent, you have the right to withdraw consent at any time; withdrawal does not affect the lawfulness of prior processing.
- **International transfers.** Your Personal Information is transferred to the United States. Where required, we use appropriate safeguards, such as standard contractual clauses.
- **Right to complain.** You have the right to lodge a complaint with your local data protection authority.

To exercise these rights, contact us at contact@memvy.com.

15.2 Canada

If you are in Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) and applicable provincial laws may apply. You have the right to access and correct your Personal Information and to withdraw consent, subject to legal and contractual restrictions. To do so, contact us at contact@memvy.com.

15.3 Other Jurisdictions

Residents of other jurisdictions may have additional rights under local law. If you have a request or question based on your local law, contact us at contact@memvy.com.

16. Third-Party Services

The Service relies on a limited set of third-party providers. Their own privacy policies govern their handling of information they collect or process. The providers we use are:

- **Apple (Apple App Store; Sign in with Apple).** When you download the Memvy app from the Apple App Store or interact with App Store mechanisms, Apple's privacy practices apply. Sign in with Apple is also provided by Apple when you choose to authenticate with an Apple account. See Apple's privacy policy at apple.com/privacy.
- **Google (Google Play Store; Google Identity Services; Firebase; Firebase Cloud Messaging; Google Analytics).** When you download the Memvy app from the Google Play Store or interact with Google Play mechanisms, Google's privacy practices apply. We also use Google services for optional Google-account authentication, for push notification delivery, and for aggregated product analytics. Google Analytics is configured with advertising features disabled and ad personalization disabled. See Google's privacy policy at policies.google.com/privacy.
- **Meta (Facebook Login SDK).** When you choose to authenticate with a Facebook account, the Facebook Login SDK is provided by Meta. Meta's handling of authentication-related information is governed by Meta's privacy policy.
- **Stripe.** We use Stripe as our payment processor for Subscriptions. Stripe collects and handles payment card information directly. See Stripe's privacy policy at stripe.com/privacy.
- **Amazon Web Services (AWS).** We host the Service on AWS in the US East (N. Virginia) region.

See Section 4.3 for a bullet-by-bullet description of each SDK and what it is used for. Memvy does not use third-party advertising SDKs, behavioral advertising networks, cross-context tracking SDKs, or data broker services.

16.1 Subscriptions and Account-Based Access

Users may create an Account and access certain features of the Service without purchasing a Subscription. Subscription plans are associated with a User Account and may be purchased and managed through the PWA. Once a Subscription is activated, Users may access applicable Subscription features across supported platforms, including the Native App, by logging into their Account.

The Service is designed to be accessible across multiple platforms, and certain features require an active Subscription.

17. Push Notifications and Communications

We may contact you in the following ways, depending on how you use the Service:

- **Push notifications (Native App only).** For activity in your Stories, security events, and important Service updates. You can disable push notifications at any time in your Device settings.
- **Email (all access methods).** Transactional emails relate to your Account, Stories, Subscriptions, security, and customer support. These continue while your Account is active. Informational emails about new features, tips, and similar content can be unsubscribed from at any time, either by using the unsubscribe link in the email or by contacting us.

We do not send marketing emails on behalf of third parties, and we do not rent or share your email address for others' marketing.

18. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. The "Current as of" date at the top of this document shows when it was last updated. If we make material changes, we will notify you by email and/or a prominent notice within the Service before the changes take effect. We encourage you to review this Privacy Policy periodically.

19. How to Contact Us

If you have questions, requests, or concerns about this Privacy Policy or Memvy's privacy practices, please contact us:

- **General privacy inquiries and data rights requests:** contact@memvy.com
- **Child Safety Point of Contact:** contact@memvy.com (include "Child Safety" in the subject line)
- **Copyright (DMCA) complaints:** dmca@memvy.com
- **Mail:** Falcon 9324, LLC, 1089 Reynolds Farm Rd, Grovetown, GA 30813, United States