COOKIES AND TRACKING POLICY

RecallScope Pty LTD
Unit 7, 2 Elonera Street
Rydalmere, New South Wales 2116
Australia

Effective Date: November 12, 2025
Last Updated: November 12, 2025

1. INTRODUCTION AND SCOPE

This Cookies and Tracking Policy ("Cookie Policy") explains how RecallScope Pty LTD ("RecallScope," "we," "us," or "our") utilises cookies, tracking technologies, and similar data collection mechanisms in connection with the RecallScope mobile application and website at https://recallscope.com (collectively, the "Service").

This Policy supplements our Privacy Policy and Terms of Use, which govern the broader collection, processing, and protection of personal information. Where provisions of this Cookie Policy conflict with the general Privacy Policy, the specific provisions contained herein shall prevail with respect to cookies and tracking technologies.

RecallScope is subject to the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), the UK GDPR, the ePrivacy Directive (Directive 2002/58/EC as amended by Directive 2009/136/EC), and equivalent legislation in other jurisdictions where Users are located. Compliance with these frameworks requires that we obtain informed consent prior to deploying non-essential cookies and tracking technologies, except where such technologies are strictly necessary for Service functionality.

2. WHAT ARE COOKIES AND TRACKING TECHNOLOGIES

Cookies are small text files placed on your device (computer, smartphone, tablet) when you access websites or applications. Cookies enable the Service to recognise your device, store preferences, and collect information about your usage patterns.

In addition to cookies, the Service may employ similar tracking technologies, including but not limited to: web beacons (small transparent graphic images embedded in web pages or emails to track usage); local storage objects (data stored in your browser's local storage); software development kit identifiers (unique identifiers assigned to mobile applications); device fingerprinting techniques (collecting device configuration data to create unique identifiers); and session identifiers maintained by backend infrastructure.

Cookies may be classified as "first-party cookies" (set directly by RecallScope) or "third-party cookies" (set by external service providers whose services are integrated into the Service, such as Google AdMob or Firebase Analytics).

3. CATEGORIES OF COOKIES

RecallScope deploys cookies across four principal categories, consistent with standards established by the Interactive Advertising Bureau ("IAB") and prevailing regulatory guidance.

Strictly Necessary Cookies. These cookies are essential for the Service to function and cannot be disabled in our systems. Strictly necessary cookies facilitate core functionality, including authentication (maintaining login sessions), security (preventing fraudulent activity and protecting against malicious attacks), load balancing (distributing user requests across servers), and session management (preserving user state during navigation). Under Article 5(3) of the ePrivacy Directive and GDPR Recital 30, strictly necessary cookies do not require user consent.

Preference Cookies. Preference cookies (also known as "functional cookies") enhance user experience by remembering choices you make, such as language preferences, jurisdiction filters, notification settings, and display preferences. These cookies enable the Service to provide personalised features but are not strictly necessary for basic functionality. Deployment of preference cookies requires prior consent under the ePrivacy Directive and GDPR.

Statistics Cookies. Statistics cookies (also referred to as "analytics cookies" or "performance cookies") collect aggregated information about how Users interact with the Service, including pages viewed, features accessed, session duration, navigation paths, and error occurrences. RecallScope utilises Firebase Analytics (Google Analytics 4) to gather usage statistics that inform Service improvements and feature prioritisation. Analytics cookies are deployed only after obtaining user consent in jurisdictions where required.

Marketing Cookies. Marketing cookies (also termed "advertising cookies" or "targeting cookies") track user behaviour across websites and applications to deliver personalised advertisements and measure advertising effectiveness. RecallScope deploys Google AdMob for contextual advertising; personalised advertising based on user profiles requires explicit opt-in consent. Marketing cookies are subject to the most stringent consent requirements under GDPR Article 6(1)(a) and ePrivacy Directive Article 5(3).

4. SPECIFIC COOKIES DEPLOYED BY RECALLSCOPE

The following table identifies principal cookies and tracking technologies deployed through the Service:

Cookie Name / Identifier	Provider	Category	Purpose	Duration
_firebase_session	Firebase (Google LLC)	Strictly Necessary	Maintains user session state and authentication	Session
_ga	Google Analytics 4	Statistics	Distinguishes unique users for analytics	2 years
_ga_*	Google Analytics 4	Statistics	Stores session state for analytics	2 years
IDE	Google AdMob	Marketing	Delivers targeted advertisements (consent-dependent)	13 months
DSID	Google AdMob	Marketing	Links user activity across devices for advertising	14 days
user_consent_tc	RecallScope / Google UMP	Strictly Necessary	Stores IAB TCF consent string	13 months
euconsent-v2	IAB TCF Framework	Strictly Necessary	IAB Transparency and Consent Framework string	13 months

Additional cookies may be deployed by third-party processors identified in our Privacy Policy, including AppsFlyer (attribution analytics) and Apphud (subscription management).

5. CONSENT MANAGEMENT PLATFORM AND GOOGLE UMP

RecallScope implements the Google User Messaging Platform ("Google UMP") as our Consent Management Platform ("CMP") to collect, store, and manage user consent preferences in compliance with GDPR, UK GDPR, and ePrivacy Directive requirements.

Google UMP is a Google-certified CMP that complies with the IAB Transparency and Consent Framework version 2.2 ("IAB TCF v2.2"), enabling standardised communication of user consent choices across the digital advertising ecosystem. Beginning January 16, 2024, Google mandated that all publishers serving advertisements to users in the European Economic Area and United Kingdom must utilise a Google-certified CMP.

Consent String Generation. Upon user interaction with our consent banner, Google UMP generates a Transparency and Consent ("TC") String encoded according to IAB TCF specifications. The TC String contains: (a) consent or objection to each data processing purpose; (b) selected legal basis (consent or legitimate interest, where permitted); (c) user preferences per vendor; (d) timestamp of consent collection; and (e) CMP identifier.

TC Strings are stored locally on the user's device and transmitted to participating vendors (including Google AdMob, Firebase Analytics, and AppsFlyer) to govern data processing activities. Users may modify or withdraw consent at any time through the Privacy Settings menu within the Application.

Consent Refresh. Consent information is requested at every application launch using the requestConsentInfoUpdate() method, in accordance with Google UMP integration requirements. This ensures that consent status remains current and accounts for changes to privacy regulations, vendor lists, or data processing purposes.

6. USER RIGHTS AND CONSENT WITHDRAWAL

Under GDPR Article 7(3), ePrivacy Directive Article 5(3), and equivalent provisions in other jurisdictions, you possess the right to withdraw consent for non-essential cookies at any time.

Modifying Cookie Preferences. Users may modify cookie preferences through the following mechanisms: (a) accessing the "Privacy Settings" or "Cookie Preferences" menu within the Application; (b) adjusting browser settings to block or delete cookies (noting that this may impair Service functionality); or (c) contacting support@recallscope.app to request manual adjustment of consent preferences.

Withdrawal of consent shall not affect the lawfulness of processing conducted prior to withdrawal. Following consent withdrawal, RecallScope and third-party processors will cease deploying non-essential cookies; however, strictly necessary cookies will continue to operate to enable core Service functionality.

7. US STATE PRIVACY LAWS AND OPT-OUT MECHANISMS

For Users located in California, Virginia, Connecticut, Colorado, Utah, and other US states with comprehensive privacy legislation, RecallScope provides mechanisms to opt out of the "sale" or "sharing" of personal information as those terms are defined under the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA/CPRA") and equivalent state statutes.

Do Not Sell or Share My Personal Information. The Service includes a "Do Not Sell or Share My Personal Information" control accessible through in-application Privacy Settings. Activating this

control restricts the sharing of personal information with advertising partners and disables personalised advertising.

Global Privacy Control ("GPC"). RecallScope honours opt-out preference signals transmitted through the Global Privacy Control framework, a browser-based mechanism that automatically communicates user privacy preferences to websites. When a GPC signal is detected, RecallScope treats the signal as a valid request to opt out of data sales or sharing, consistent with requirements under California Code of Regulations Title 11, Section 7025 and equivalent regulations in other states.

Effective January 1, 2027, California's Opt Me Out Act (AB 566) will require web browsers to provide functionality enabling users to configure opt-out preferences at the browser level, further strengthening consumer privacy protections. RecallScope commits to complying with these evolving requirements as they take effect.

8. THIRD-PARTY COOKIES AND EXTERNAL LINKS

The Service integrates third-party services that deploy their own cookies, including Google LLC (Firebase, AdMob, Analytics), AppsFlyer Ltd. (attribution analytics), and Apphud Inc. (subscription management). These third parties function as data processors under contractual arrangements requiring compliance with GDPR, UK GDPR, and equivalent legislation.

RecallScope exercises no control over cookies deployed by third parties and is not responsible for their privacy practices. Users are encouraged to review the privacy policies and cookie policies of these service providers:

- Google Privacy Policy: https://policies.google.com/privacy
- AppsFlyer Privacy Policy: https://www.appsflyer.com/legal/privacy-policy/
- Apphud Privacy Policy: https://apphud.com/privacy

Where the Service contains links to external websites (including official government recall portals), those sites may deploy their own cookies governed by separate policies.

9. COOKIE RETENTION PERIODS

Cookies are retained for varying durations depending on their type and purpose. Session cookies are deleted when you close the Application or browser session. Persistent cookies remain on your device for the duration specified in Section 4 above, or until manually deleted through browser settings.

Consent records (including TC Strings) are retained for thirteen (13) months from the date of collection, consistent with IAB TCF requirements and GDPR accountability obligations. Upon expiration, consent is deemed withdrawn and must be re-obtained.

10. UPDATES TO THIS COOKIE POLICY

RecallScope may update this Cookie Policy periodically to reflect changes in technology, legal requirements, or Service functionality. Material modifications shall be communicated via email or in-application notice at least fourteen (14) days prior to the effective date. The "Last Updated" date at the top of this document indicates the most recent revision.

11. CONTACT INFORMATION

For questions regarding this Cookie Policy, to exercise your rights, or to adjust cookie preferences, contact:

RecallScope Pty LTD
Email: support@recallscope.app
Support: support@recallscope.com.