PRIVACY 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

RecallScope Pty LTD ("RecallScope," "we," "us," or "our") operates the RecallScope mobile application and associated web services accessible at https://recallscope.com (collectively, the "Service"). This Privacy Policy describes how we collect, use, disclose, retain, and protect personal information obtained from users ("you," "User") of the Service across iOS and Android platforms.

RecallScope functions as a data controller under the General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR"), the United Kingdom General Data Protection Regulation ("UK GDPR"), and the Australian Privacy Act 1988 (Cth) with respect to personal information processed through the Service. Where we engage third-party service providers to process personal information on our behalf, we act as controller and such providers function as processors under applicable data protection legislation.

This Policy applies to all Users globally, with particular attention to requirements imposed by the GDPR for European Economic Area and United Kingdom residents, the California Consumer Privacy Act as amended by the California Privacy Rights Act (collectively, "CCPA/CPRA") for California residents, and the Australian Privacy Principles ("APPs") contained within the Privacy Act 1988 (Cth). Where Users reside in jurisdictions with specific privacy legislation, including but not limited to Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"), such laws shall apply concurrently with this Policy to the extent they provide greater protections.

2. DATA CONTROLLER AND CONTACT INFORMATION

The data controller responsible for your personal information is RecallScope Pty LTD, a proprietary limited company registered in New South Wales, Australia. Our registered office is located at Unit 7, 2 Elonera Street, Rydalmere, NSW 2116, Australia.

For inquiries regarding this Privacy Policy, to exercise data subject rights, or to contact our privacy team, please use the following channels:

General Privacy Inquiries: support@recallscope.app
Data Protection Officer / Privacy Contact: support@recallscope.app
General Support: support@recallscope.com

Users located in the European Economic Area or United Kingdom may also contact supervisory authorities in their respective jurisdictions regarding data protection concerns.

3. CATEGORIES OF PERSONAL INFORMATION COLLECTED

RecallScope collects several categories of personal information necessary to provide the Service's core functionality and optional features. The scope of collection depends upon User choices, including Account type selected and features activated.

Account Authentication Data. When Users elect to create an Account through Apple Sign-In or Google Sign-In, we collect email addresses provided by these authentication services. Anonymous Account creation is also supported, in which case no directly identifying information is collected. Email addresses obtained through authenticated sign-in are used exclusively for delivery of the

optional weekly digest and essential account communications, subject to User consent where required by applicable law.

Watchlist and User Preferences. The Service permits Users to curate Watchlists containing product names, brand identifiers, vehicle identification numbers, batch codes, and barcode data. These Watchlist entries are stored to enable personalised recall notifications. We also collect notification preferences, including preferred delivery times, quiet hours settings, and jurisdiction filters selected by Users.

Search and Scan History. When Users conduct searches within the Application or utilise barcode scanning functionality, search queries and scanned product identifiers are temporarily retained to improve Service functionality and provide relevant recall matching. Such data constitutes usage information rather than profile data and is retained for periods specified in Section 8 below.

Technical and Device Information. The Service automatically collects certain technical data, including device identifiers, operating system versions, application version numbers, IP addresses, and device type. Firebase Analytics collects aggregated usage statistics, including screen views, session duration, and feature engagement metrics. Firebase Crashlytics automatically gathers crash reports containing device state information, stack traces, and application logs to facilitate debugging and improve Service stability.

Advertising Identifiers. For Users who have not subscribed to Pro tier and who have provided consent where required, we collect advertising identifiers (IDFA on iOS, AAID on Android) to deliver contextual advertisements through Google AdMob. Personalised advertising is disabled by default; Users may opt into personalised advertisements through in-application consent mechanisms.

Location Data. The Service does not collect precise geolocation data. Approximate location may be inferred from IP addresses for purposes of presenting jurisdiction-appropriate recall information. Users select preferred jurisdictions manually through application settings.

Subscription and Purchase Information. When Users subscribe to Pro tier, transaction data is processed by Apple Inc. (for iOS) or Google LLC (for Android) pursuant to their respective terms. RecallScope receives limited subscription status information, including subscription tier, purchase date, renewal date, and cancellation status, through our subscription management provider Apphud Inc. We do not receive or store complete payment credentials.

Sensitive Personal Information. RecallScope does not intentionally collect sensitive personal information as defined under GDPR Article 9, CCPA/CPRA Section 1798.140(ae), or Australian Privacy Act provisions regarding sensitive information. Should Users voluntarily include sensitive information within Watchlist entries or communications, such information shall be processed solely to the extent necessary to provide requested Service functionality.

4. LAWFUL BASES FOR PROCESSING

The legal bases for processing personal information vary according to User location and the specific processing activity undertaken.

Contractual Necessity. Processing of Account information, Watchlist data, notification preferences, and subscription status is necessary for performance of the contract formed when Users accept our Terms of Use. Without such processing, RecallScope cannot deliver core Service functionality, including personalised recall notifications and Pro subscription features.

Legitimate Interests. RecallScope processes technical data, usage analytics, and crash reports based on legitimate interests in maintaining Service security, preventing fraud, improving functionality, and optimising user experience. These interests are balanced against User privacy

rights; data minimisation principles are applied to ensure processing remains proportionate. Users retain rights to object to processing conducted under legitimate interests grounds.

Consent. Where required by applicable law, we obtain explicit consent for: (a) delivery of the optional weekly email digest; (b) non-essential cookies and tracking technologies; (c) personalised advertising; and (d) processing of email addresses obtained through third-party authentication. Consent may be withdrawn at any time through in-application settings or by contacting support@recallscope.app.

Legal Obligations. Certain processing activities are undertaken to comply with legal obligations, including responding to valid law enforcement requests, complying with court orders, and fulfilling mandatory data breach notification requirements under the Privacy Act 1988 (Cth), GDPR Article 33, and equivalent legislation.

5. PURPOSES OF DATA PROCESSING

Personal information collected through the Service is processed for the following purposes:

Service Delivery. We use Account information, Watchlist data, and notification preferences to deliver core Service functionality, including aggregating recall notices, matching User Watchlists against new recalls, transmitting push notifications and email digests, and providing personalised risk assessments.

Subscription Management. Purchase and subscription data is processed to provision Pro tier features, manage billing cycles, process cancellations, and respond to refund requests.

Service Improvement and Analytics. Aggregated usage data, crash reports, and feature engagement metrics are analysed to identify bugs, optimise performance, prioritise feature development, and enhance user experience. Analytics data is stored in de-identified or pseudonymised form where practicable.

Advertising. For free-tier Users, we display contextual advertisements through Google AdMob. Where Users have provided consent, advertising identifiers may be used to deliver personalised advertisements. Users may withdraw consent for personalised advertising through in-application privacy settings.

Security and Fraud Prevention. Technical data, including IP addresses and device identifiers, is processed to detect fraudulent activity, prevent unauthorised access, identify security vulnerabilities, and enforce our Terms of Use.

Legal Compliance. We process personal information as necessary to comply with applicable laws, respond to legal process, cooperate with regulatory investigations, and protect our legal rights.

6. THIRD-PARTY SERVICE PROVIDERS AND DATA PROCESSORS

RecallScope engages third-party service providers to facilitate Service delivery. These providers function as data processors under GDPR, UK GDPR, and equivalent Australian Privacy Act provisions, processing personal information solely on our instructions and subject to appropriate contractual safeguards.

Firebase Services (Google LLC). Firebase Firestore, Firebase Cloud Functions, Firebase Cloud Messaging, Firebase Storage, Firebase Authentication, Firebase Analytics (Google Analytics 4), and Firebase Crashlytics are deployed to provide backend infrastructure, push notifications, analytics, and crash reporting. Firebase processes personal information pursuant to Google's Data Processing and Security Terms, which incorporate Standard Contractual Clauses for international

data transfers. Firebase holds ISO 27001, ISO 27017, ISO 27018, SOC 2, and SOC 3 certifications.

Google AdMob (Google LLC). AdMob delivers contextual advertisements to free-tier Users. Where Users provide consent, AdMob may process advertising identifiers for personalised advertising purposes. AdMob operates as a service provider under CCPA/CPRA and processor under GDPR.

AppsFlyer Ltd. AppsFlyer provides attribution analytics to measure acquisition channels and campaign effectiveness. AppsFlyer processes device identifiers and usage data pursuant to data processing agreements incorporating Standard Contractual Clauses.

Apphud Inc. Apphud manages in-application subscriptions, processing subscription status, purchase dates, and renewal information. Apphud functions as a processor under contractual arrangements ensuring GDPR compliance.

Email Service Provider. RecallScope utilises [SendGrid/Mailgun/AWS SES – to be determined] to deliver the optional weekly digest and essential account communications. Email service providers process email addresses and delivery preferences solely on our instructions.

Apple Sign-In and Google Sign-In. When Users authenticate through Apple Inc. or Google LLC services, these providers process authentication credentials pursuant to their respective terms of service and privacy policies. RecallScope receives only email addresses, subject to User consent.

All processors are contractually obligated to implement appropriate technical and organisational measures, process data solely on documented instructions, maintain confidentiality, assist with data subject rights requests, notify us of data breaches, and delete or return data upon termination.

7. INTERNATIONAL DATA TRANSFERS

RecallScope is headquartered in Australia; however, personal information is transferred to and processed in the United States through our Firebase infrastructure and third-party processors.

Firebase Data Locations. Firebase Cloud Functions, Firebase Storage, and Firebase Firestore are configured to operate in the following regions: Firebase Functions (us-central1), Firebase Storage (us-central1), and Firestore (nam5 multi-region, United States). Firebase Analytics and Crashlytics utilise Google's default regional configurations, which may include both United States and European Union processing locations.

Transfer Safeguards. Transfers of personal information from the European Economic Area, United Kingdom, or Switzerland to the United States are governed by Standard Contractual Clauses approved by the European Commission pursuant to GDPR Article 46(2)(c). Google LLC (Firebase's operator) has executed Standard Contractual Clauses as data importer and has certified compliance with the EU-U.S., UK-U.S., and Swiss-U.S. Data Privacy Frameworks.

RecallScope has conducted Transfer Impact Assessments to evaluate whether laws and practices in recipient countries undermine protections afforded by Standard Contractual Clauses, as required under guidance from the European Data Protection Board. Based on these assessments and the supplementary safeguards implemented by our processors (including encryption, access controls, and transparency regarding government data requests), we have determined that transfers comply with GDPR Chapter V requirements.

Australian Cross-Border Disclosures. Under Australian Privacy Principle 8, RecallScope remains accountable for personal information disclosed to overseas recipients. We take reasonable steps to ensure overseas recipients comply with the APPs through contractual arrangements, due diligence, and ongoing monitoring.

8. DATA RETENTION PERIODS

RecallScope retains personal information only for as long as necessary to fulfil the purposes for which it was collected, comply with legal obligations, resolve disputes, and enforce agreements.

Account Information. Email addresses and Account credentials are retained for the duration of Account existence. Upon Account deletion, identifiers are permanently deleted within thirty (30) days.

Watchlist Data. Watchlist entries and notification preferences are retained for as long as the Account remains active. Users may delete individual Watchlist entries or entire Watchlists at any time through application settings.

Search and Scan History. Search queries and barcode scans are retained for one hundred eighty (180) to three hundred sixty-five (365) days to facilitate recall matching and Service improvement. Users may request deletion of search history by contacting support@recallscope.app.

Technical Logs and Crash Reports. Technical logs, including IP addresses and device identifiers, are retained for ninety (90) days. Firebase Crashlytics retains crash reports for up to ninety (90) days in identifiable form; aggregated crash statistics may be retained indefinitely.

Analytics Data. Firebase Analytics retains raw event data for fourteen (14) months by default, after which data is aggregated and anonymised. Aggregated analytics may be retained indefinitely for statistical and research purposes.

Backup Data. Backup copies of databases containing personal information are retained for thirty (30) days to facilitate disaster recovery. Backup deletion occurs automatically upon expiration of the retention period.

Subscription Records. Purchase history and subscription status information are retained for seven (7) years following subscription termination to comply with tax and financial record-keeping obligations under Australian law.

Upon expiration of applicable retention periods, personal information is securely deleted or anonymised such that it can no longer be attributed to an identified or identifiable individual.

9. YOUR RIGHTS UNDER APPLICABLE DATA PROTECTION LAWS

The rights available to you depend upon your jurisdiction of residence.

Rights Under GDPR and UK GDPR (EEA and UK Residents). You have the right to: (a) access personal information we hold about you and receive a copy thereof (Article 15); (b) rectify inaccurate or incomplete information (Article 16); (c) erasure ("right to be forgotten") where lawful grounds exist (Article 17); (d) restrict processing in certain circumstances (Article 18); (e) data portability, receiving your information in structured, commonly used, machine-readable format (Article 20); (f) object to processing conducted under legitimate interests grounds (Article 21); and (g) withdraw consent at any time where processing is based on consent, without affecting lawfulness of prior processing (Article 7(3)).

You also have the right to lodge a complaint with your national data protection authority if you believe we have violated your rights.

Rights Under CCPA/CPRA (California Residents). California residents have the right to: (a) know what personal information is collected, used, shared, or sold; (b) delete personal information subject to certain exceptions; (c) correct inaccurate personal information; (d) opt out of the sale or sharing of personal information for cross-context behavioural advertising; (e) limit use and disclosure of sensitive personal information; (f) receive data in portable format; and (g) non-discrimination for exercising privacy rights.

RecallScope does not "sell" personal information as defined under CCPA/CPRA. To the extent that sharing data with advertising partners constitutes "sharing" under CCPA/CPRA Section 1798.140(ah), Users may opt out through the "Do Not Sell or Share My Personal Information" control in application privacy settings.

Rights Under Australian Privacy Act. Australian residents have the right to: (a) access personal information held by RecallScope; (b) request correction of inaccurate or out-of-date information; (c) lodge complaints with the Office of the Australian Information Commissioner; and (d) request that we cease direct marketing communications.

Exercising Your Rights. To exercise any of the above rights, please submit a request to support@recallscope.app. We will verify your identity before processing requests and respond within timeframes mandated by applicable law (typically thirty (30) days under GDPR, forty-five (45) days under CCPA/CPRA, and thirty (30) days under Australian Privacy Act). In-application tools are available for account deletion and data export.

10. SECURITY MEASURES

RecallScope implements technical and organisational measures designed to protect personal information against unauthorised access, alteration, disclosure, or destruction.

Technical Safeguards. Data in transit is encrypted using Transport Layer Security (TLS) protocols. Data at rest within Firebase Firestore and Firebase Storage is encrypted using AES-256 encryption. Access to production systems is restricted through role-based access controls and multi-factor authentication. Firebase infrastructure is protected by Google's security controls, including intrusion detection systems, firewall policies, and continuous vulnerability scanning.

Organisational Measures. Personnel with access to personal information are subject to confidentiality obligations. Regular security training is provided to employees and contractors. We conduct periodic reviews of data processing activities and security controls.

Incident Response. In the event of a data breach affecting personal information, we will notify affected Users and relevant supervisory authorities within timeframes required by applicable law (seventy-two (72) hours under GDPR Article 33, twelve (12) hours for notifiable data breaches under Australian Privacy Act Section 26WK).

Notwithstanding the safeguards described above, no method of transmission or electronic storage is completely secure. RecallScope cannot guarantee absolute security of personal information.

11. COOKIES, TRACKING TECHNOLOGIES, AND CONSENT MANAGEMENT

The Service utilises cookies and similar tracking technologies. A detailed Cookies and Tracking Policy is available separately and forms part of this Privacy Policy.

For Users located in the European Economic Area, United Kingdom, or jurisdictions with equivalent consent requirements, we deploy a Consent Management Platform (Google User Messaging Platform) to obtain consent prior to activating non-essential cookies or tracking technologies. Consent preferences are stored and honoured throughout User sessions.

Users may modify cookie preferences at any time through in-application privacy settings or browser controls.

12. CHILDREN'S PRIVACY

The Service is not directed to individuals under eighteen (18) years of age. RecallScope does not knowingly collect personal information from children. If we become aware that personal information has been collected from an individual under the age threshold, we will promptly delete such information and terminate the associated Account.

Parents or guardians who believe a child has provided personal information to RecallScope should contact support@recallscope.app.

13. CHANGES TO THIS PRIVACY POLICY

RecallScope reserves the right to modify this Privacy Policy at any time. Material changes affecting User rights or expanding processing activities will be communicated via email or prominent in-application notice at least fourteen (14) days prior to the effective date. Immaterial changes, including clarifications or corrections, may be implemented without advance notice.

Continued use of the Service following the effective date of modifications constitutes acceptance of the revised Privacy Policy. The "Last Updated" date at the top of this document reflects the most recent revision.

14. CONTACT INFORMATION AND COMPLAINTS

For questions, concerns, or to exercise your rights under this Privacy Policy, please contact:

RecallScope Pty LTD
Unit 7, 2 Elonera Street
Rydalmere, NSW 2116
Australia

Email: support@recallscope.app
General Support: support@recallscope.com

Supervisory Authority Complaints. EEA and UK residents may lodge complaints with their national data protection authority. Australian residents may lodge complaints with the Office of the Australian Information Commissioner at https://www.oaic.gov.au.