

Networker Google API Data Use

Google API Services disclosure for Networker users

Effective Date: July 24, 2026

1. Scope and Consent

This disclosure explains how Networker accesses, uses, stores, shares, and protects Google user data when a user signs in with Google. Networker uses Google OAuth only after the user grants consent and only for the account the user authorizes.

When a user signs in with Google, Networker requests openid, email, and profile permissions only. Networker uses those permissions to identify the account, maintain authentication, display basic profile information, protect security, and provide user-directed support.

Users may revoke Networker's Google sign-in access in Google Account permissions or contact tanish@trynetworker.com for access, correction, deletion, or privacy requests.

2. Gmail Access Is Not Requested

Networker does not request Gmail scopes, does not connect Google as an email sender, and does not use Google APIs for outreach drafts or sending.

Campaign drafting, Microsoft draft creation, approved sending, scheduled sending, provider message identifiers, and sender token refresh run through the Microsoft sender connection only.

3. Google User Data Collected and Used

Google user data may include the signed-in account email address, Google account identifiers, profile name, profile image, and session information needed to operate authentication.

Campaign drafts, Microsoft provider identifiers, send metadata, audit records, and workflow logs may be retained to operate outreach workflows, enforce account limits, troubleshoot failures, maintain security, comply with law, and provide user-directed support. Those sending records are not created through Google sender APIs.

4. Limited Use Commitments

Networker's use and transfer to any other app of information received from Google APIs will adhere to the Google API Services User Data Policy, including the Limited Use requirements.

Networker uses Google user data only to provide or improve prominent user-facing features in Networker, maintain security, prevent abuse, troubleshoot issues, comply with law, enforce terms, or act on the user's direction.

Networker does not sell Google user data, use Google user data for advertising, use Google user data for retargeting or personalized advertising, transfer Google user data to advertising platforms, transfer Google user data to data brokers or information resellers, use Google user data for credit-worthiness or lending decisions, use Google user data for surveillance, or use Google user data to train generalized artificial intelligence or machine learning models.

Networker does not use Gmail access because Gmail access is not requested.

5. Sharing and Service Providers

Networker may disclose Google sign-in data to service providers that help provide hosting, storage, authentication, security, logging, support, and troubleshooting. These providers are authorized to process Google user data only for Networker and only as needed to provide the service, maintain security, comply with law, or prevent abuse.

Networker may disclose Google user data if required to comply with law, legal process, regulator requests, security investigations, fraud prevention, abuse prevention, enforcement of terms, or protection of users and the service.

Networker does not sell Google user data and does not disclose Google user data to data brokers, advertising networks, or information resellers.

6. Human Access

Networker personnel, contractors, and service providers may access Google user data only where necessary to provide support requested by the user, investigate security or abuse issues, comply with law, maintain or troubleshoot the service, or process data in aggregated or de-identified form for permitted internal operations.

Unauthorized browsing of Google sign-in data or user workspace data is prohibited. Human access is limited by role-appropriate access controls, confidentiality obligations, and operational need.

7. Storage, Security, and Deletion

Google sign-in identity data is retained only as needed to operate the account or as otherwise necessary for security, troubleshooting, legal compliance, abuse prevention, or account recovery.

Networker uses administrative, technical, and organizational safeguards designed to protect Google sign-in data, including access controls, provider security controls, encryption in transit where appropriate, and logging. No online service is completely secure.

Users may revoke Google sign-in access through Google Account permissions, delete workflow records where product functionality allows, or contact tanish@trynetworker.com to request access, correction, deletion, or privacy help. Networker may retain limited records where required or permitted for legal compliance, security, fraud prevention, dispute resolution, transaction records, backups, or legitimate business purposes.

8. Contact

Questions about Networker's Google API data use may be sent to tanish@trynetworker.com. Please include enough information for Networker to understand and verify the request.