Gnomeo Security & Data Protection Policy

Version 1.0 | Date 2026-05-09 | Scope: Public policy document for Gnomeo

Formal guidance on how Gnomeo protects uploaded ad data, generated reports, workspace context, and administrative access.

PURPOSE AND SCOPE

This policy explains how Gnomeo protects uploaded ad data, generated reports, workspace context, and administrative access. It applies to customer-facing use of the product, private storage and access handling, and the current manual beta operating model.

WHAT GNOMEO PROTECTS

Raw ad exports are commercially sensitive. They can reveal budget structure, campaign performance, audience segments, and operational decisions. Gnomeo is designed to protect that material as private customer data.

SECURITY PRINCIPLES

- Workspace data remains private by default.
- Raw uploads are handled as temporary processing data.
- Reports and analytical memory are kept separate from raw export files.
- Customer data is isolated by workspace and access scope.
- Public exposure of uploaded files is avoided.

RAW UPLOAD HANDLING

- Raw uploads are not sold.
- Raw uploads are not publicly shared.

Gnomeo Security & Data Protection Policy

Version 1.0 | Date 2026-05-09 | Scope: Public policy document for Gnomeo

- Temporary processing files are removed when practical after processing.
- Raw uploads are not meant to be retained indefinitely.

PRIVATE STORAGE AND ACCESS

- Customer files are stored in private locations.
- Short-lived access methods are used when files need to be downloaded.
- Public file access is avoided unless a file is intentionally public.
- Workspace isolation is preserved across customer records.
- Service credentials remain server-side only.

ADMINISTRATIVE ACCESS

Administrative endpoints are protected by server-side access controls for the current manual beta. Administrative secrets are not exposed in frontend code.

SECRETS MANAGEMENT

- Secrets are not committed to git.
- Frontend code must not contain service credentials.
- Operational secrets are stored on the server.
- If exposure is suspected, secrets should be rotated without delay.

TRANSPORT AND LOGGING

- Customer-facing requests are expected to use encrypted transport.

- Operational records are retained only as long as needed for support, reliability, or incident review.

- Access to sensitive operations is limited.

DELETION AND RETENTION

Security and retention are linked. Keeping less raw data reduces exposure. Users may request deletion of workspace data, and temporary files are intended to be removed as soon as they are no longer needed.

INCIDENT RESPONSE

- If a secret or customer file is exposed, credentials should be rotated.

- Affected storage paths and access logs should be reviewed.

- Exposure should be contained by keeping customer data private by default.

- Corrective action should be documented before broader rollout.

CURRENT MANUAL BETA LIMITATIONS

The current manual beta uses a simpler administrative access model than a mature production system. It is appropriate for controlled operation, but it does not replace fully scoped user authorization, complete audit trails, or long-term security hardening.

FUTURE SECURITY IMPROVEMENTS

- Stronger user authentication and workspace-scoped authorization.

- More complete audit logging for administrative actions.

- Further access-control hardening as paid usage expands.