

Information, with clear boundaries.

This brief describes the Ayan website, inquiry service, meeting requests, and client workspace as reviewed on 10 October 2026. Controls for a separately delivered client system depend on its agreed architecture and contract.

HOW INFORMATION MOVES

An inquiry

The contact form sends your chosen details to the website service. Inquiry content is encrypted before database storage. The administration notification contains an inbox link rather than the message body. Authorized administration can read the saved inquiry and reply by email.

An executive brief

Draft entries stay in the current browser page memory. PDF export runs in the browser and downloads to your device. Exporting does not submit the brief. Choosing to send it uses the inquiry service and its retention rules.

A client workspace

An administrator manages project membership. Authorized members sign in with an emailed one-time code and can access their project material. Proposals, messages, decisions, approvals, and uploaded files are encrypted in the website database.

A meeting request

Contact details, business context, time zone, and preferred times are stored as an encrypted request for administrator review. A request is not a confirmed appointment. An administrator decision can send email and, for a confirmed time, a calendar invitation.

Controls that support the service.

Transport and stored content

The website uses HTTPS. Stored inquiry, workspace, and meeting content is protected with application-level AES-256-GCM encryption using random nonces and record-specific authentication context. Identifiers, timestamps, status fields, and keyed lookup values remain available as operational metadata.

Authentication and authorization

Administrator and client-workspace sessions are separate. Sign-in uses time-limited email codes. Twelve-hour session cookies are Secure, HttpOnly, and SameSite=Strict. The server checks project membership for client access; removing membership or closing a project withdraws that access.

Integrity of project decisions

Workspace writes use request identifiers and revision checks to handle duplicate requests and concurrent changes. Approval records identify the member and the version reviewed. A newer version requires a fresh review rather than silently inheriting an old approval.

Hosting, email, and provider boundaries

Cloudflare supplies the website hosting, network protection, database, and email transport. Accepted incoming emails may be forwarded to the business mailbox. Mail providers process correspondence and attachments. Hosting and encryption do not establish a single-country processing commitment.

Public browsing and AI use

The public site has no advertising trackers or third-party analytics. Submitting an inquiry does not subscribe you to a marketing list. The website inquiry workflow does not send submissions to a generative AI model.

The service can decrypt content for authorized use. This is not end-to-end encryption. Email and separately operated engagement systems have their own boundaries.

Know what stays. Agree what follows.

Website conversations

Daily cleanup removes inbox conversations after 365 days without new conversation activity. Incoming messages and newly recorded outgoing reply attempts restart the period. Reading or archiving a conversation does not extend it.

Client projects

Active project workspaces are retained while open. Closed project records and files are scheduled for removal after 365 days from closure through daily cleanup. Reopening cancels closure-based cleanup. Revoking membership does not itself delete the project.

Meeting and authentication records

Meeting requests become eligible for cleanup after 365 days from the later of their last update and their confirmed time, or latest requested time if unconfirmed. Cleanup is batched. Expired authentication and request-limiting records are also removed through cleanup.

Deletion from these website systems does not automatically erase separate mailbox copies, infrastructure logs, backups, or records governed by an engagement agreement.

BEFORE AN ENGAGEMENT

Share the information classification, required providers or regions, access model, retention requirements, and procurement checklist. Any confidentiality terms, data-processing agreement, service commitments, or assurance evidence should be settled before the relevant project data is shared.

Security and procurement: hello@withayan.com

Current privacy policy

For a privacy request, identify the email address used and enough context to locate the record. For a security concern, describe the affected page and observed behavior without sending passwords, secrets, or unrelated personal data.