

Security and delivery context.

Published information about Windmill Digital and the controls to discuss for your engagement.

Entity and certification information

Windmill Smart Solutions AG is headquartered in Switzerland, with offices in Europe, the United States and India. The public Trust & Security page records ISO/IEC 27001:2022 certification and the transition announcement dated 21 August 2025.

Client data and hosting

The published delivery approach describes enterprise API terms, no foundation-model training on client data and zero-retention agreements. Swiss/EU hosting or deployment in the client's own cloud can be discussed for sandbox and production data. Confirm the actual providers, terms and configuration for the scope.

Access and operating records

The public controls describe private endpoints, tenant segregation, least-privilege tokens, session auditing and tamper-evident records of system actions and overrides. Agree the applicable architecture, access responsibilities and evidence with the delivery team.

AI quality and oversight

The approach includes regression checks using Audra Eval and explicit human review for high-stakes actions. Define the evaluation set, release thresholds, escalation and operational ownership around the system being delivered.

[Current Trust & Security page](#)

SCOPE-SPECIFIC REVIEW

What to request before you commit.

Use the published overview to start due diligence; obtain the supporting documents and project-specific answers for your review.

Certification evidence

Request the current certificate, covered legal entity, scope and validity dates. This overview is not a certificate and does not certify a client product or establish its regulatory compliance.

Data processing and suppliers

Request the applicable processing terms, sub-processor register, hosting locations, retention/deletion arrangements and provider-specific model-data terms. The public site does not currently publish a sub-processor register.

Responsibility and operations

Agree incident and escalation contacts, access ownership, monitoring, release approval, continuity arrangements and the scope of any continuing service. A named security-questionnaire owner is not currently published; request the accountable individual for your engagement.

Contact

Send security questionnaires and due-diligence requests to security@windmill.digital. For the proposed product or workflow, contact hello@windmill.digital. Agree confidentiality before sending sensitive architecture or customer material.

[Published security information and request route](#)