Clearlane

Supplier assessment

Version 2.2 · 11 November 2026 · Information provided and approved by Maxime Ragionieri, owner of Maxime Ragionieri EI (brand: Clearlane Apps), for your supplier qualification file. Check what matters for your intended use. Previous version: 2.0, 3 November 2026 (first issue: 1.0, 8 October 2026).

Supplier

Legal form	Maxime Ragionieri EI, a French sole proprietorship (entreprise individuelle), trading under the brand Clearlane Apps; run by one person, Maxime Ragionieri
Registration	Legal name, SIRET and VAT number: legal notice, clearlaneapps.com/legal/
Contact	hello@clearlaneapps.com · help center clearlane.atlassian.net
Support	Every message read and answered as quickly as possible, in English, French or German

Products and hosting

Products	Apps for Jira and Confluence Cloud, sold on the Atlassian Marketplace
Hosting	Atlassian Forge, on Atlassian's infrastructure (Runs on Atlassian). The supplier operates no servers. Every install of our apps is traceable in Atlassian Admin Hub (who installed it, when and how).
Data location	Your Atlassian site. Stored app data follows your site's data residency (Forge hosted storage).
Data leaving Atlassian	None: the apps make no network call outside Atlassian.
Subprocessors for your content	Atlassian only: it hosts the apps (Forge), bills Marketplace purchases and runs the help center. The optional Rovo agents call no AI model themselves: answers come from your own Atlassian Rovo, under your agreement with Atlassian. List: clearlaneapps.com/trust/
Service status	The apps run on Atlassian Forge; their availability follows Atlassian's: clearlaneapps.com/status/ links to the live status pages of Forge, Jira and Confluence

Information security

Security questionnaire	Full CAIQ v4.1 answers listed in the CSA STAR Registry (Level 1 self-assessment, not an audit): https://cloudsecurityalliance.org/star/registry/clearlane-apps/services/clearlane-apps-for-jira-and-confluence . CAIQ-Lite answers: clearlaneapps.com/trust/
Certifications	None held by the supplier. Data kept only inside Forge is covered by the controls Atlassian applies to its platform (AES-256 at rest, TLS 1.2+ in transit).
Access control	Atlassian sign-in (your SSO and two-step verification apply). Apps act with each person's permissions; documented exceptions are listed in the security policy.
Supplier access to your content	None: it never reaches the supplier.
Electronic signatures	Signing passwords kept only as a salted scrypt hash; signing locks after repeated failures; SHA-256 fingerprint of signed content.
Logs	Technical counters only, never customer content.
Vulnerabilities	Dependency audit before every release; SBOM (CycloneDX) for each release; reports acknowledged within 2 business days and fixed within the deadlines of Atlassian's Security Bug Fix Policy for Marketplace apps.
Incidents	Affected customers notified without undue delay, and no later than 72 hours after becoming aware of it (this supplements the DPA, which prevails); also reported to Atlassian. Vulnerability reports acknowledged within 2 business days.

Quality of releases

Before each release	Automated tests of every workflow at the real Forge limits, simultaneous users and large volumes; runs on a real Atlassian site; access test with an account without rights; security review of the code; dependency audit.
Release information	Release notes on the Atlassian Marketplace. Updates are installed automatically by Atlassian; those that need new permissions wait for your administrator's approval.

Development, backup and continuity

Development lifecycle	Source code under version control (git). Each change is built and tested in a separate Forge development environment, on a real Atlassian test site, before it reaches production. Numbered versions; release notes on the Atlassian Marketplace.

Changes to signed records	At least 30 days' notice in the release notes before any functional change that affects signed records, signatures or approval workflows. Security fixes ship without delay; their release notes say why.
Backup	The source code is backed up automatically every day to a private Bitbucket repository, with versioned archives kept separately. Your data is not backed up by the supplier: it stays in your Atlassian site.
Continuity	The apps run on Atlassian's infrastructure and do not depend on any supplier server; exports (CSV, PDF evidence) work at any time. No source-code escrow. Business continuity statement: clearlaneapps.com/trust/
Training	No formal training programme (one-person supplier). Working rules follow Atlassian's Forge security requirements and the Marketplace Security Bug Fix Policy (policy last reviewed on 3 November 2026).
Supplier audits	Accepted in writing: questionnaires (a completed CAIQ-Lite is published on clearlaneapps.com/trust/), document requests and follow-up questions; first written reply within two business days. No on-site or video audits.

Validation materials

Available	OQ test scripts (Controlled Documents, Read & Understood, CAPA, Tests, CRA); mappings to 21 CFR Part 11, ISO 13485, IEC 62304 and the Cyber Resilience Act: clearlaneapps.com/validation/
Statement	The apps are designed to help you meet these requirements. They are not certified; compliance comes from your validated system and procedures.

Contract

Purchase	Atlassian Marketplace or your Atlassian Solution Partner; Atlassian handles quotes, invoices, payment and refunds.
Documents	Licence terms, privacy policy and security policy on clearlaneapps.com · French law
Uninstall	Atlassian deletes the app's stored data under its retention rules; export evidence files (PDF, CSV) first.

Customer review

Reviewed by	
Date	
Decision	

clearlaneapps.com/trust/