Security overview

Coresteads OÜ | Version 0.10 | 19 October 2026

Baseline for client project controls. Agree exact measures and implementation evidence in the DPA and statement of work before processing. This overview is not an audit or compliance certification.

Coresteads builds AI agents, skills, subagent workflows and scheduled runs. The aim is to give your team control of data, access and important decisions.

Data flows and roles	Your accounts where practical. Data may still flow to a model API and other approved providers. The DPA identifies roles and sub-processors; directly contracted client services are identified separately.
Access and secrets	Named accounts, least privilege, MFA on supported administration accounts and access removal when no longer needed. Keys and passwords are held in a secret store or password manager.
Data protection	TLS, verified storage and device encryption, client data separation and synthetic or anonymous test data where possible. Implementation is checked for each project.
AI and human control	Coresteads does not train its own models on client data. Provider training use, retention and exceptions are checked separately. High-impact actions require agreed human approval.
Retention and exit	DPA Annex A sets periods for working copies, logs and backups. The template's log maximum is 90 days, shorter where possible. At exit data is normally returned or deleted within 30 days.
Testing and visibility	Agreed checks before handover and after material changes. Public methodology: review at least 8/10, trigger accuracy 85%, behavioural tests 80% and no blocking defects. These are not a reliability guarantee.
Incidents	The DPA requires notice without undue delay, no later than 48 hours after awareness. Information is supplemented and the client assisted; the client's statutory notification deadline is a separate obligation.

Before use, confirm owners, evidence, data flows, transfer safeguards and recovery. Recurring maintenance, budget limits and extra controls are agreed separately. GDPR and AI Act duties are assessed against the solution's role and risk; applicable AI interaction disclosures are added. No insurance or certification is asserted here.

Website inquiries are separate: Firebase Hosting -> Firestore (eur3) -> Trigger Email (europe-west1) -> Resend -> mailbox. Google Analytics loads with consent. Details: coresteads.com/en/privacy.

info@coresteads.com