TRUST CENTRE

Säkerhet och datasuveränitet.

Det här är sidan vi vill att kommunala inköpare, dataskyddsombud och säkerhetschefer ska kunna skicka till sin checklista. Inga buzzwords, bara vad vi har, vad vi inte har, och var data tar vägen.

Senast uppdaterad 2026-05-27 · Kontakt: kontakt@foundryai.se

HOSTING	KRYPTERING I VILA	KRYPTERING I TRANSIT	US-MOLNLEVERANTÖRER
Egen hårdvara i Sverige	AES-256-GCM	TLS 1.2+	Inga

PÅ DEN HÄR SIDAN

Var er data lagras

All produktionsdata, alla AI-modeller och alla kundfiler ligger på hårdvara som Foundry äger och driver, fysiskt placerad i Sverige. Vi använder inte AWS, Azure, Google Cloud eller någon annan molnleverantör som lyder under amerikansk eller annan utomeuropeisk jurisdiktion. Språkmodellerna (Qwen, baserade på öppna vikter) körs lokalt via Ollama på vår egen GPU. Inget prompt-innehåll och inga kundfiler lämnar svensk mark när AI:n bearbetar dem.

> SCHREMS II OCH ESAM
>
> eSams rättsliga vägledning slår fast att information ska anses röjd redan när den blir tekniskt åtkomlig för en leverantör som omfattas av utländska tvångsutlämningsregler (t.ex. amerikansk CLOUD Act). Eftersom Foundry inte använder några sådana leverantörer för produktionsdata uppstår inte den situationen.

Kryptering

I vila

Känsliga fält som användarprompter krypteras kolumnvis i SQLite med **AES-256-GCM**. Nyckeln laddas vid uppstart från miljövariabel och hålls aldrig i databasen. Formatprefix (`enc1:`) gör nyckelrotation möjlig utan att tappa historiska rader.

I transit

All inkommande trafik termineras med TLS 1.2 eller högre via reverse proxy. HSTS är aktiverat (`max-age=31536000; includeSubDomains`) så att webbläsare vägrar HTTP-fallback. Intern trafik mellan applikation och AI-runtime sker över lokal loopback och lämnar aldrig hostmaskinen.

Nyckelhantering

Krypteringsnycklar lagras separat från databasen, säkerhetskopieras offline, och roteras vid personalförändringar eller misstänkt kompromettering. Förlorad nyckel innebär oåterkalleligt dataförlust, vilket är medvetet val: nycklarna finns inte hos någon tredje part som kan tvingas lämna ut dem.

Åtkomst och autentisering

Kundinloggning på `/profil` sker via signerad e-postlänk (magic link). Sessioner är kortvariga och bundna till kundens organisations-id. Administratörsåtkomst till produktionsservern är begränsad till grundaren via SSH-nyckel, ingen lösenordsinloggning, och loggas vid varje access.

Job-tokens som identifierar enskilda körningar är 48 tecken slumpmässig hex (24 byte entropi). Jämförelser sker tidssäkert med `crypto.timingSafeEqual` så ingen sidkanal läcker gissningar.

> PÅ FÄRDPLANEN
>
> Multifaktor (MFA) för kundinloggning är näst på tur. Magic-link räcker i nuläget för låg-känsligt material men ersätts/kompletteras med TOTP eller hårdvarunyckel under 2026.

Nätverk och härdade endpoints

Applikationen kör bakom reverse proxy med strikta säkerhetsheaders (Helmet): Content-Security-Policy, X-Frame-Options DENY, Referrer-Policy strict-origin-when-cross-origin, nosniff. CORS är default-deny: enbart same-origin tillåts.

Per-route rate-limits skyddar mot bruteforce och DOS av betalflöde, avbeställningar och statusanrop. Body-storlek på inkommande JSON är begränsad till 32 kB.

SSRF-skydd

Vid alla utgående HTTP-anrop (t.ex. när en agent hämtar en sökresultatsida) löser vi hostnamn i förväg och blockerar anslutningar till privata IP-intervall: RFC1918, loopback, link-local, ULA, CGNAT, IPv4-mappade privata v6-adresser. Redirects valideras om vid varje hopp.

Loggning och spårbarhet

Operativa loggar redigeras automatiskt: prompter ersätts med `sha256:8 + längd`, Stripe-id maskeras, jobtokens trunkas. Detta gäller även dashboard-loggen som administratören ser. Råa prompter sparas aldrig på disk utanför den krypterade SQLite-kolumnen.

Säkerhetsrelevanta händelser (misslyckade webhook-signaturer, blockerade SSRF-försök, rate-limit-trigger) loggas separat och sparas i 12 månader.

Underbiträden

Foundry använder ett minimalt antal underbiträden, alla inom EU. Vi meddelar kunder minst 30 dagar i förväg om vi planerar att byta eller lägga till underbiträde.

UNDERBITRÄDE	FUNKTION	DATA SOM BEHANDLAS	JURISDIKTION
Stripe Payments Europe	Betalningshantering vid köp av Klara, både prova-på och abonnemang.	Namn, e-post, betalmetadata. Inte AI-prompter eller dokument.	Irland (EU). DPF-certifierad för eventuella US-överföringar.
Brevo (Sendinblue SAS)	Transaktions-mail (orderbekräftelse, magic-link, kontaktformulär).	Namn, e-postadress, ämnesrad, mailinnehåll vi själva skrivit.	Frankrike (EU).
Loopia AB	Domän och DNS för foundryai.se.	Inga personuppgifter. Endast DNS-records.	Sverige.
Google Fonts (CDN)	*Avvecklad i juli 2026.* Typsnitten ligger numera på vår egen server och laddas från foundryai.se.	Ingen. Besökarens webbläsare gör inga anrop till externa typsnittsdomäner.	Ej tillämpligt.

Vad vi inte använder: Inga US-hyperscalers (AWS, Azure, GCP). Inget OpenAI, Anthropic, eller andra externa LLM-API:er för produktionsdata.

Ingen analytics-tracker (Google Analytics, Hotjar, Mixpanel) på kundsidor.

Säker utveckling

- **Prepared statements överallt**. All SQL går via parametriserade frågor.
- **Path-traversal försvar i tre lager**. Whitelist-regex, `..`-rejection, och realpath-containment innan filskrivning.
- **Promptinjektionsförsvar**. All användardata wrappas i sentineluttryckta block (`USER_DATA`) i agentprompter, med systeminstruktion att ignorera instruktioner inne i blocket.
- **Atomiska filskrivningar**. Tempfil + rename, läge 0600 för filer, 0700 för kataloger.
- **Stripe-webhooks** signaturverifieras och idempotensspårning sker på event-id så att samma event aldrig processas dubbelt.
- **Dependency-uppdateringar** görs varje månad. Säkerhetsrelevanta CVE:er patchas inom 7 dagar.

Senaste interna säkerhetsgranskning genomfördes 2026-05-09 och finns dokumenterad. Tredjeparts penetrationstest är inplanerat med svensk leverantör innan första större kommun-/regionkund tas i drift.

Backup och kontinuitet

SQLite-databas och kundutdata säkerhetskopieras dagligen till separat krypterat lagringsmedium, fysiskt åtskilt från produktionsservern men inom samma jurisdiktion (Sverige). Backuper är krypterade i vila med separat nyckel, sparas i 30 dagar rullande, och testas en gång per kvartal genom återställning till en isolerad miljö.

Eftersom produkten kör på vår egen hårdvara har vi inget cloud-SLA att luta oss mot. Mål för återställning vid total hårdvaruförlust: under 24 timmar för applikationen, under 48 timmar för historiska kundutdata.

Incidenthantering

Vid säkerhetsincident som påverkar kunddata följer vi en intern process som triggas inom timmar:

- **0 till 6 h:** identifiering, containment, första statusrapport till påverkade kunder.
- **Inom 24 h:** formell notifiering till kund med vad som har hänt, vilka data som berörs, och vad vi gör. Detta ligger före kommunens egna NIS2/cybersäkerhetslagens 24h "early warning" till MSB, så er anmälningsskyldighet inte hänger på oss.
- **Inom 72 h:** uppdaterad bedömning, slutgiltig påverkan, rekommendation om vidare åtgärder.
- **Post-mortem inom 14 dagar:** rotorsak, åtgärd, vad vi ändrar för att förhindra upprepning. Delas med påverkade kunder.

Anmälningskanal: kontakt@foundryai.se med ämnesrad som börjar med "INCIDENT".

Datakvarhållning och radering

Det här är en sammanfattning av vår interna kvarhållningspolicy, som är det styrande dokumentet. Övriga sidor på webbplatsen hänvisar hit. Policyn i sin helhet delas med kunder på begäran.

- **Anbudsdata, 30 dagar:** förfrågningsunderlag och genererade utkast raderas automatiskt 30 dagar efter att anbudet levererats till er.
- **Profildokument, så länge kontot är aktivt:** certifikat, personallistor, referenser och tidigare vunna anbud som ni lagt in i företagsprofilen ligger kvar tills ni tar bort dem eller avslutar kontot. Radering på begäran enligt artikel 17 GDPR.
- **CV och personuppgifter om personal, högst 24 månader:** CV-filer som inte uppdaterats på 24 månader raderas automatiskt.
- **Kontaktförfrågningar, 12 månader:** uppgifter som skickas via kontaktformuläret raderas automatiskt efter 12 månader.
- **Legacy körningsoutput, 72 timmar:** råa utdata från den äldre prototyppipelinen raderas 72 timmar efter avslutad körning.
- **Backuper, 30 dagar:** krypterade säkerhetskopior roterar på 30 dagar. En begärd radering slår igenom i backuperna senast när rotationen passerat.
- **Kontoinformation och fakturor:** organisation, kontaktperson och faktureringshistorik sparas så länge kundförhållandet pågår, och fakturor därutöver i sju räkenskapsår enligt bokföringslagen.

Radering på begäran (artikel 17 GDPR) genomförs inom 30 dagar. Dataportabilitet (artikel 20) levereras som JSON+filarkiv inom samma tidsram. Full process beskrivs i vår DSAR-rutin som finns tillgänglig på begäran.

Se även: Integritetspolicy och Personuppgiftsbiträdesavtal.

Regelefterlevnad

På plats

GDPR

Personuppgiftsbiträdesavtal redo att signera. Artikel 30-register förs. DSAR-rutin dokumenterad.

På plats

EU AI Act

Foundrys produkter klassificeras som begränsad risk. Loggning och mänsklig översyn ingår från dag ett. Artikel 11-fil förs per produkt.

På plats

Cybersäkerhetslagen (NIS2) som underleverantör

Tekniska åtgärder enligt artikel 21 NIS2 är implementerade. Vi flow-down NIS2-likvärdiga krav i biträdesavtal med kunder som själva omfattas.

Pågående

SKR KLASSA

Självskattning för K2/R2/T2 (standardklass för kommunal verksamhet utan personnummer/sekretess) tillhandahålls på begäran inför upphandling.

Pågående

ISO/IEC 27001

Vi följer principerna i SoA och har gjort en intern gap-analys. Formell certifiering är planerad efter att grundkundbasen är etablerad.

Pågående

ISO/IEC 42001 (AI-ledningssystem)

Ramverk under införande. Vi bevakar utvecklingen kring AI-specifika ledningskrav som komplement till ISO 27001.

Inte aktuellt

SOC 2

SOC 2 är ett amerikanskt ramverk. ISO 27001 är bättre signal mot svensk offentlig sektor. Vi prioriterar inte SOC 2 i dagsläget.

Inte aktuellt

Säkerhetsskyddslagen

Foundry hanterar inte säkerhetsskyddsklassificerade uppgifter. För kunder som behöver SUA krävs särskild överenskommelse innan eventuell start.

Sårbarhetsanmälan

Hittat något vi borde fixa? Skicka oss en signal till kontakt@foundryai.se med ämnesrad som börjar med "SECURITY". Beskriv så detaljerat ni kan och hur ni vill bli krediterade om ni vill det.

- Vi bekräftar mottagandet inom 2 arbetsdagar.
- Vi accepterar PGP-krypterad korrespondens. Nyckel på begäran.
- Vi kör inte program med bug bounty just nu men erkänner alla rapporter offentligt om reportern vill det.
- Vi vidtar inga juridiska åtgärder mot personer som rapporterar i god tro och inte exfiltrerar data utöver vad som behövs för att demonstrera sårbarheten.

kontakt@foundryai.se