SÄKERHETSPAKET

Säkerhetsbeskrivning

VERSION	UTFÄRDAT AV	KONTAKT
2026-10-16	Brickstream AB, 556792-7644	info@brickstream.se

Brickstream AB, org.nr 556792-7644, Linköping · Version 2026-10-16 · Kontakt: info@brickstream.se (ämne "Säkerhet")

Beskrivningen gäller Brickstreams tjänster till fast pris (till exempel Anbudsstöd, Kravgranskning, Testfall och Leverantörsformulär – säkerhet, kvalitet och miljö), gratisprovet och plattformen app.brickstream.se, som de är byggda och konfigurerade på versionsdatumet. Vi redovisar öppet det som ännu inte är på plats (avsnitt 11).

1 Översikt

Del	Leverantör	Plats
Webbplats och serverfunktioner	Vercel	Stockholm (region arn1)
Databas, inloggning och filer (ert underlag och leveransen)	Supabase	Stockholm (AWS eu-north-1)
AI-bearbetning av underlaget	Anthropic (kommersiellt API)	USA, under EU:s standardavtalsklausuler (avsnitt 4)
E-post från plattformen	Resend	EU (Irland)
Botskydd i formulären (IP-adress och webbläsarsignaler, inte formulärets innehåll)	Cloudflare (Turnstile)	Cloudflares globala nätverk, normalt EU; bolaget i USA

Hela listan med skyddsåtgärder och avtal står i dokumentet Underbiträden. Brickstream har ingen egen serverpark, och vi behöver ingen åtkomst till era system: ni skickar filer.

2 Ert underlag i en beställning eller ett gratisprov

Lagring	filerna ligger i en privat lagringsplats i Stockholm som bara er beställning når. Uppladdning och nedladdning sker med kortlivade signerade länkar. Krypterat vid överföring (TLS) och vid lagring.
Ingen e-postbilaga	vi skickar aldrig underlag eller leverans som bilaga. Leveransen hämtar ni i plattformen, och gratisprovet som en nedladdningslänk som gäller i 30 dagar.
Vem ser det	AI-teamet under körningen och, i en beställning, Brickstreams senior slutgranskare. Slutgranskaren arbetar under sekretessavtal, läser och rättar i plattformen med tvåstegsinloggning och kan inte ladda ned filerna; varje öppning loggas. Inga andra konsulter och inga andra kunder ser något. Två konkurrenter i samma upphandling får aldrig samma granskare.

Bara för er beställning	underlaget förbättrar aldrig leveranser till någon annan kund och används inte i någon kunskapsbas, mall eller exempel. AI-teamet tränas på publicerade upphandlingar – aldrig på ert material.
Radering	underlaget och leveransen raderas automatiskt 30 dagar efter leverans, och direkt om beställningen avbryts eller avböjs. Ett gratisprov och dess underlag raderas senast 30 dagar efter att provet har levererats eller avböjts. Kvar finns bara det bokföringslagen kräver.

- **Brickstreams interna AI-assistent** (för drift, utveckling och e-post) öppnar aldrig kunders underlag i uppdragen.

3 Det här tar vi inte emot

Säkerhetsskyddsklassificerade uppgifter eller underlag under säkerhetsskyddsavtal, och exportkontrollerad teknisk information (till exempel krigsmateriel, produkter med dubbla användningsområden, ITAR eller EAR). I ett gratisprov tar vi inte heller emot känsliga personuppgifter eller personnummer. Plattformen söker efter klassnings- och exportkontrollmärkningar innan arbetet börjar; vid träff stoppas arbetet, filerna raderas och vi hör av oss. Personuppgifter i övrigt är inget hinder – ni avgör själva om ni maskerar namn utifrån er policy.

4 AI-bearbetningen

- AI-teamet anropar Anthropics modeller (Claude) via Anthropics **kommersiella API** – inte en chattapp eller konsumenttjänst.
- Innehållet används **inte för att träna modellerna** (Anthropics kommersiella villkor).
- **Bearbetningen sker i dag i USA**, under EU-kommissionens standardavtalsklausuler i Anthropics biträdesvillkor. Hos AI-leverantören raderas in- och utdata inom 30 dagar; längre bara om något flaggas för brott mot leverantörens användarregler.
- **AI-bearbetning i EU är förberedd** (Claude via Amazon Bedrock i Stockholm, eu-north-1, med en EU-profil som håller bearbetningen inom EU). Den är inte påslagen ännu. Samma dag som den slås på ändras den här beskrivningen, underbiträdeslistan och integritetspolicyn. Kräver er policy EU-behandling: säg det innan ni laddar upp något.
- Under körningen har AI-teamet ingen åtkomst till internet eller till andra kunders data. Text i ert underlag behandlas som data: instruktioner i det följs inte.
- Allt AI-teamet tar fram i en beställning slutgranskas av en människa. Gratisprovet är ett AI-utkast som inte är slutgranskat och är märkt så.

5 Inloggning och behörighet

- Inloggning utan lösenord: engångslänk och engångskod via e-post, med en mellansida som skyddar mot e-postskannrar.
- Tvåstegsverifiering (TOTP) krävs för Brickstreams konton, för slutgranskare och för kundanvändare utan företagsinloggning. Kravet kontrolleras i databasen, inte bara i gränssnittet.
- Behörighet per rad i databasen (Row Level Security) på alla tabeller: en kund ser bara sin egen organisations beställningar, och linjechefer ser inga priser.
- Sessioner för Brickstreams konton och kundanvändare avslutas efter högst 12 timmar.

6 Kryptering och hemligheter

All trafik går över TLS med HSTS. Data i vila krypteras av leverantörerna. API-nycklar finns bara som skyddade miljövariabler hos driftleverantören, aldrig i koden eller i loggar.

7 Loggning

Säkerhetsloggen kan inte ändras i efterhand: databasen stoppar ändringar och borttag, och raderna länkas med en SHA-256-hashkedja. Loggas bland annat: inloggningar, beställningar och intyg, uppladdade filer (namn, storlek, kontrollsumma), varje öppning och nedladdning av underlag och leverans, tilldelning av granskare och radering. Ni kan be om ett utdrag för er beställning.

8 Drift, övervakning och ändringar

Tillgängligheten kontrolleras var femte minut, och driften följs dagligen. Varje vecka kontrollerar plattformen själv att dess nycklar till leverantörerna fungerar, utan att någon ser nycklarna. Koden finns i ett privat repo; varje ändring passerar typkontroll, automatiska tester och bygge innan den driftsätts, och databasändringar görs additivt. Drift, utveckling och säkerhetskontroller görs till stor del av Brickstreams AI-team under VD:s ansvar och enligt en skriftlig arbetsordning; teamet får aldrig lätta på säkerhet eller behörigheter eller hantera hemligheter.

9 Om något händer

Om ert underlag kan ha hamnat hos någon som inte ska ha det, eller något annat säkerhetsproblem har påverkat det, meddelar vi er inom 24 timmar från att vi upptäckt det: vad som har hänt, vad som berörs, vad vi har gjort och vad vi gör härnäst. Vi stoppar bearbetningen av berört material tills orsaken är klarlagd. Gäller det personuppgifter i ert underlag får ni beskedet utan onödigt dröjsmål, så att ni kan anmäla till Integritetsskyddsmyndigheten inom 72 timmar.

Rapportera säkerhetsproblem till info@brickstream.se med ämnet "Säkerhet" (se också /.well-known/security.txt).

10 Avtal

Villkoren för uppdrag (brickstream.se/villkor/uppdrag) innehåller sekretess och ett personuppgiftsbiträdesavtal (bilaga 1). Vill ni ha ett eget undertecknat PUB-avtal finns mallen i det här paketet, och ett sekretessavtal tecknar vi på begäran.

11 Kända begränsningar

Område	Läge
ISO/IEC 27001	Inte certifierat. Arbetssättet följer standarden där det är rimligt för bolagets storlek.
Oberoende penetrationstest	Inte genomfört ännu.
AI-bearbetning i EU	Förberedd, inte påslagen. I dag sker AI-bearbetningen i USA (avsnitt 4).
Säkerhetsskyddsklassad information	Plattformen är inte avsedd eller ackrediterad för det.
Raderingskvitto per fil	Plattformen visar att filerna är raderade, men ger inget kvitto med kontrollsummor ännu.