SECURITY PACK

Security description

VERSION	ISSUED BY	CONTACT
2026-10-16	Brickstream AB, 556792-7644	info@brickstream.se

Brickstream AB, reg. no. 556792-7644, Linköping, Sweden · Version 2026-10-16 · Contact: info@brickstream.se (subject "Security")

This description covers Brickstream's fixed-price services (for example Bid support, Requirements review, Test cases and Supplier questionnaires – security, quality and environment), the free sample and the platform app.brickstream.se, as built and configured on the version date. We state openly what is not yet in place (section 11).

1 Overview

Part	Provider	Location
Website and server functions	Vercel	Stockholm (region arn1)
Database, sign-in and files (your material and the delivery)	Supabase	Stockholm (AWS eu-north-1)
AI processing of the material	Anthropic (commercial API)	USA, under the EU standard contractual clauses (section 4)
E-mail from the platform	Resend	EU (Ireland)
Bot protection in the forms (IP address and browser signals, not the form content)	Cloudflare (Turnstile)	Cloudflare's global network, normally the EU; company in the USA

The full list with safeguards and agreements is in the Sub-processors document. Brickstream has no server room of its own, and we need no access to your systems: you send files.

2 Your material in an order or a free sample

Storage	the files are kept in private storage in Stockholm that only your order can reach. Upload and download use short-lived signed links. Encrypted in transit (TLS) and at rest.
No e-mail attachments	we never send material or deliveries as attachments. You download the delivery in the platform, and the free sample through a download link valid for 30 days.
Who sees it	the AI team during the run and, in an order, Brickstream's senior final reviewer. The final reviewer works under a non-disclosure agreement, reads and corrects in the platform with two-step sign-in and cannot download the files; every opening is logged. No other consultants and no other customers see anything. Two competitors in the same tender never get the same reviewer.

Only for your order	the material never improves deliveries to another customer and is not used in any knowledge base, template or example. The AI team is trained on published tenders – never on your material.
Erasure	the material and the delivery are erased automatically 30 days after delivery, and at once if the order is cancelled or declined. A free sample and its documents are erased at the latest 30 days after the sample has been delivered or declined. Only what the Swedish Accounting Act requires remains.

- **Brickstream's internal AI assistant** (for operations, development and e-mail) never opens customers' material in assignments.

3 What we do not accept

Security-classified information or material under a security protection agreement, and export-controlled technical information (for example military equipment, dual-use items, ITAR or EAR). In a free sample we also do not accept sensitive personal data or personal identity numbers. The platform searches for classification and export-control markings before the work starts; on a hit the work stops, the files are erased and we contact you. Other personal data is no obstacle – you decide yourselves whether to mask names under your policy.

4 AI processing

- The AI team calls Anthropic's models (Claude) through Anthropic's **commercial API** – not a chat app or consumer service.
- The content is **not used to train the models** (Anthropic's commercial terms).
- **Processing currently takes place in the USA**, under the European Commission's standard contractual clauses in Anthropic's data processing terms. At the AI provider, inputs and outputs are deleted within 30 days; longer only if something is flagged for breaching the provider's usage policy.
- **AI processing in the EU is prepared** (Claude through Amazon Bedrock in Stockholm, eu-north-1, with an EU profile that keeps processing within the EU). It is not switched on yet. On the day it is switched on, this description, the sub-processor list and the privacy notice are updated. If your policy requires processing in the EU, tell us before you upload anything.
- During the run the AI team has no access to the internet or to other customers' data. Text in your material is treated as data: instructions in it are not followed.
- Everything the AI team produces in an order is final-reviewed by a person. The free sample is an AI draft that is not final-reviewed and is marked as such.

5 Sign-in and access control

- Passwordless sign-in: one-time link and one-time code by e-mail, with an intermediate page that protects against e-mail scanners.
- Two-step verification (TOTP) is required for Brickstream's accounts, for final reviewers and for customer users without company sign-in. The requirement is enforced in the database, not only in the interface.
- Row-level security in the database on all tables: a customer sees only its own organisation's orders, and line managers see no prices.

- Sessions for Brickstream’s accounts and customer users end after at most 12 hours.

6 Encryption and secrets

All traffic uses TLS with HSTS. Data at rest is encrypted by the providers. API keys exist only as protected environment variables at the hosting provider, never in the code or in logs.

7 Logging

The security log cannot be altered afterwards: the database blocks changes and removals, and the rows are linked with a SHA-256 hash chain. Logged among other things: sign-ins, orders and declarations, uploaded files (name, size, checksum), every opening and download of material and deliveries, reviewer assignments and erasure. You may ask for an extract for your order.

8 Operations, monitoring and changes

Availability is checked every five minutes, and operations are followed daily. Every week the platform itself checks that its keys to the providers work, without anyone seeing the keys. The code is in a private repository; every change passes type checking, automated tests and a build before it is deployed, and database changes are additive. Operations, development and security checks are largely done by Brickstream’s AI team under the CEO’s responsibility and a written set of rules; the team may never relax security or permissions or handle secrets.

9 If something happens

If your material may have reached someone who should not have it, or another security problem has affected it, we tell you within 24 hours of discovering it: what happened, what is affected, what we have done and what we will do next. We stop processing the affected material until the cause is clear. If it concerns personal data in your material, you are told without undue delay so that you can notify the supervisory authority within 72 hours.

Report security issues to info@brickstream.se with the subject "Security" (see also /.well-known/security.txt).

10 Agreements

The terms for assignments (brickstream.se/villkor/uppdrag) include confidentiality and a data processing agreement (annex 1). If you want a separate signed DPA, the template is in this pack, and we sign a non-disclosure agreement on request.

11 Known limitations

Area	Status
ISO/IEC 27001	Not certified. The way of working follows the standard where reasonable for the company’s size.
Independent penetration test	Not yet carried out.
AI processing in the EU	Prepared, not switched on. Today AI processing takes place in the USA (section 4).
Security-classified information	The platform is not intended or accredited for it.
Erasure receipt per file	The platform shows that the files have been erased, but gives no receipt with checksums yet.