

Tessera Privacy Notice Version 1.0 Effective 27 October 2026

This notice explains how Tessera Security Ltd ("Tessera", "we", "us") collects and uses personal data when you visit our website (Part 1) and when you or your organisation use the Tessera Design service, including the Tessera MCP connector and the agent API (Part 2). It covers personal data we control. System descriptions, documents, diagrams and the designs produced from them ("Customer Content") are processed on your organisation's behalf under our Data Processing Agreement, not under this notice (see 2.9).

Who we are. Tessera Security Ltd, registered in England and Wales, company number 17336112. Registered office: Office 444, Unit 5, 399–405 Oxford Street, London W1C 2BU. We have not appointed a Data Protection Officer; data-protection queries go to hello@tesseractsecurity.ai. We are registered with the Information Commissioner's Office, registration number **ZC240262**.

Part 1 — The website (tesseractsecurity.ai)

1.1 Request-access form

Name, work email, organisation, optional role, short description of intended use. Purpose: respond and assess pilot fit. Lawful basis: legitimate interests (Art. 6(1)(f)); consent for contact about access (Art. 6(1)(a)). Delivered by Web3Forms. Retained until actioned plus 12 months, or sooner on request.

1.2 Server logs

IP address, browser type, pages requested, recorded by our hosting provider (Amazon Web Services, London). Purpose: operating and securing the site. Lawful basis: legitimate interests. Retained for as long as the provider retains them.

1.3 Theme preference

Stored only in your browser; not sent to us. We set no analytics or advertising cookies. (If analytics is ever added, this section changes first and we tell you.)

Part 2 — The Tessera Design service

2.1 Who this covers

People who use Tessera Design through an organisation's workspace (consultants, reviewers, administrators, invitees), people who contact us for support, and billing contacts. Your organisation decides who is invited and what content is uploaded.

2.2 What we collect and why

Data	Purpose	Lawful basis	Retention
Account and	Create and secure	Contract (Art.	Life of the

Data	Purpose	Lawful basis	Retention
identity — name, work email, role, identity-provider subject id, MFA enrolment state, sign-in events	your account; authorise what you can do; invitations and setup	6(1)(b)); legitimate interests in security (Art. 6(1)(f))	account, then 30 days after the account or workspace is removed
Workspace membership and review records — which workspace you belong to; which elements you validated, challenged, commented on or signed off, with timestamps	Provide the service; keep the provable review record ("golden thread") that is the product's purpose	Contract; legitimate interests in integrity	Life of the workspace
Terms-acceptance record — your identifier, the Terms/DPA versions you accepted, timestamp	Evidence of acceptance	Contract; legal obligation / legitimate interests	Life of the account plus 6 years
Audit log — security-relevant events (sign-in, invitations, token issue/revocation, exports, acceptance, deletions) with your identifier and email	Security monitoring, incident investigation, accountability to customers	Legitimate interests in security; contract	Life of the workspace
Billing contacts — name, email, organisation, payment status, invoices	Charge for credits and subscriptions; tax and accounting	Contract; legal obligation (tax)	Financial records 6 years + current year. Card details held by Stripe only, never by us
Support and incident	Respond to queries, defects,	Contract; legitimate	24 months after closure

Data	Purpose	Lawful basis	Retention
correspondence	incidents	interests	
Transactional messages — email address, workspace name, one-time links, verification codes; optional SMS	Invitations, account setup, notifications you turn on	Contract	Delivery logs ~90 days
Service telemetry — content-free logs (routes, counts, error types, element references); never element text, never emails	Reliability, security, cost	Legitimate interests	~90 days
Integration credentials (if your administrator connects Slack, Teams, Jira or Miro) — the tokens supplied	Send notifications and findings to your organisation's own services	Contract	Encrypted; held until disconnected
API tokens (agent API / MCP) — a hashed token bound to your organisation, its expiry and last use	Authenticate programmatic access; rate-limit and revoke	Contract; legitimate interests in security	Hash kept until expiry/revocation, then 30 days

We do not use your personal data for marketing without asking, and we do not sell it.

2.3 Where it is processed

Tessera Design runs on Amazon Web Services in the United Kingdom (eu-west-2, London). All non-global AWS services we use — compute, database, object storage, identity (Amazon Cognito), email (Amazon SES), SMS (Amazon SNS) and logs (CloudWatch) — are in eu-west-2. Customer Content is hosted at rest in the UK; the only point at which it leaves AWS is the minimised transmission to Anthropic for inference (2.4).

2.4 Who we share it with (sub-processors)

- **Amazon Web Services EMEA SARL** — hosting, identity, email, SMS, logs — United Kingdom (eu-west-2). No restricted transfer.
- **Anthropic Ireland, Limited** — AI generation. Before any content is sent, we minimise the text to remove identifiers and secrets at a single enforced point; this text-minimisation does not extend to text inside images, diagrams or screenshots. Processing is transient, under a **zero-data-retention** and **no-training** arrangement, and carried out principally in the **United States**. Anthropic receives Customer Content, not your account data, except where a name or email appears inside uploaded material.
- **Stripe** — payments; receives billing-contact details and handles card data directly.
- **Web3Forms** — the website request-access form only (Part 1).
- Your organisation's own connected services (Slack, Teams, Jira, Miro), only if an administrator connects them; those are controlled by your organisation, not sub-processors of ours.
- Professional advisers, insurers and authorities where the law requires.

The current Customer-Content sub-processor list and the transfer mechanisms are in the DPA at tesseractsecurity.ai/legal/dpa; we give at least 30 days' notice of changes.

2.5 International transfers

Your account data and all Customer Content are hosted at rest in the UK. Where a sub-processor processes personal data outside the UK:

- **Anthropic** (principally the US) — under the **UK Addendum to the EU Standard Contractual Clauses (Module Three)** incorporated in Anthropic's Data Processing Addendum, with zero data retention, no training, text-minimisation and encryption in transit as supplementary measures.
- **Stripe** (US) — under Stripe's standard contractual clauses and UK Addendum.

2.6 How we protect it

Invite-only access with mandatory multi-factor authentication; sessions bound to a verified load-balancer identity; tenant isolation at every route; identifier minimisation before any model call; encryption at rest with customer-managed keys and TLS 1.3 in transit; content-free logging; least-privilege database access; independent security review with findings tracked to closure; an incident-response and breach-notification procedure. We notify affected customers without undue delay of any personal-data breach affecting them, as the DPA requires.

2.7 Retention and deletion

Account data: as in 2.2. Customer Content: uploaded source files are deleted once the run that reads them finishes (success, failure, cancellation or a sweep after a crash), and each deletion is logged; the extracted model, your entered text and the Outputs are kept for the life of the workspace, or for a longer period your organisation may select under the DPA's extended-retention (write-once) option. On termination you have 30 days to export, after which we delete Customer Content within a further 30 days and from backups within 90 days, unless the law requires otherwise. There is no model training on any of it.

2.8 Automated processing

Outputs are generated by automated means for your review. We do not use your data to make decisions about individuals, and a named human validates the Outputs before they are relied on.

2.9 Customer Content is governed by the DPA

System descriptions, documents, diagrams and the designs produced from them belong to your organisation. For that content we are a processor acting on your organisation's instructions under the Data Processing Agreement, and your organisation is the controller (or a processor for its own client). Questions about that content go to your organisation.

2.10 Your rights

You can ask to access, correct or erase your personal data, to restrict or object to its processing, to receive it in a portable form, and to withdraw any consent. Write to hello@tesseractsecurity.ai; we respond within one month. Where your data sits inside your organisation's workspace, we may route the request through your organisation, which controls that workspace. You can complain to the ICO (ico.org.uk); please contact us first.

2.11 Children

The service is for business use by adults. We do not knowingly collect data about anyone under 18.

2.12 Changes

We post changes here with a new version number and effective date, and keep earlier versions at tesseractsecurity.ai/legal/changes. Where a change is material, signed-in users are asked to acknowledge the new version.

Contact: hello@tesseractsecurity.ai · Tessera Security Ltd, Office 444, Unit 5, 399–405 Oxford Street, London W1C 2BU.