DATA HANDLING AND PRIVACY

# Data handling and privacy

Written for the person who has to sign this off. Every statement below is drawn from Clairsyn's published Privacy Policy and Terms of Service (version 2.2, effective 29 July 2026, last updated 17 August 2026) and from clairsyn.com. Nothing here goes beyond them.

## The rule, before the detail

**Everything an individual tells Clairsyn is confidential to Clairsyn. The organisation receives patterns, never individual answers. Groups under three are merged or excluded, so nobody is ever identifiable.**

That holds for survey answers on Clairsyn Threshold and for anything said in an interview on the full diagnostic. What differs between the two is whether Clairsyn itself can see who said it, and we would rather set that out in a table than leave it to be found in a policy.

## What is held, by product

| | CLAIRSYN THRESHOLD | THE FULL DIAGNOSTIC |
|---|---|---|
| **What is recorded** | Survey responses (scores 1 to 5 or N/A per question), role group, function, tenure band and country. No name. No email address with the answers. | A longer piece of work involving interviews. Answers are recorded against the individual's name so Clairsyn knows who to follow up with. |
| **Identifiers** | Not collected with the answers. Where the organisation asks Clairsyn to email invitations (Managed Outreach), that list is kept separate from the responses and is not linked to them. | Recorded for follow-up during the engagement. In what is reported, personal identifiers are removed and evidence combined where needed, so findings focus on systemic patterns, not individuals. |
| **Who has responded** | Clairsyn cannot tell who has and has not responded, which is why reminders go to everyone, including people who have already taken part. | Known to Clairsyn, for follow-up. |
| **Can Clairsyn see who said what** | No. Threshold is anonymous: Clairsyn does not know who answered what. | Yes. Answers are recorded against the individual's name. |
| **Can the organisation** | No. Nobody at the organisation sees individual responses, only grouped patterns. | No. The organisation only ever sees patterns, never individual answers. |

**From purchasers, on either product:** name and email address; organisation name, sector, size and country; invoice and transaction records. Payment is processed by Stripe and Clairsyn does not store card details. Standard server logs (IP address, browser type, page access times) are kept for security monitoring, are not linked to individual users, and are retained for 30 days.

## What the information is used for

- To deliver the assessment purchased and generate the report; to send progress updates, reminders and the final report; to process payment and maintain financial records; to provide customer support.
- To improve the platform and methodology using anonymised, aggregated data, with no organisation identified; and to build anonymised sector benchmarks, with data de-identified before any benchmark use.
- Clairsyn does not use your information for advertising, does not sell your data, and does not use personal information to train AI models.
- Every report is built from a library of paragraphs written by Clairsyn's team, selected by the system based on the organisation's scores. Where AI tools are used in report assembly, they receive structured score data only, no personal information.

## Legal basis, and changes to the policy

For customers in the UK and EU: contract performance (delivering the assessment purchased), legitimate interests (security monitoring, anonymised product improvement and benchmarking) and legal obligation (financial records). Clairsyn complies with the New Zealand Privacy Act 2020 and the Australian Privacy Principles, with PIPEDA and applicable provincial legislation in Canada, and sets out its United States position in the Privacy Policy, section 10.

**Changes.** The current Privacy Policy is always published at clairsyn.com/privacy and material changes are communicated to active purchasers by email. Clairsyn Threshold is not directed at anyone under 18.

Full detail: clairsyn.com/privacy and clairsyn.com/terms · Questions: hello@clairsyn.com

WHERE IT LIVES, AND HOW IT IS PROTECTED

# Where it lives, and how it is protected

## Where it lives

| THIRD PARTY | PURPOSE | LOCATION |
|---|---|---|
| **Stripe** | Payment processing | United States |
| **Supabase** | Database and file storage | United States (AWS us-east-1) |
| **Vercel** | Application hosting and CDN | United States / Global |
| **Resend** | Transactional email delivery | United States |
| **OpenAI (Phase 2 only)** | Report narrative assembly, structured score data only, no personal information | United States |

Clairsyn does not share personal information with any other third parties. All processors are required to maintain appropriate security measures and process data only for the purposes Clairsyn specifies. Infrastructure providers are primarily based in the United States; by using Clairsyn Threshold you consent to information being transferred to and processed there. Safeguards: Stripe participates in the EU-US Data Privacy Framework; Standard Contractual Clauses apply for EEA/UK transfers with Supabase, Vercel and Resend.

## Security

- Encryption in transit (HTTPS/TLS) for all data, and encryption at rest for all database content.
- Row-level security: organisations cannot access each other's data.
- Time-limited signed URLs for report access.
- Environment-based secret management, no API keys in code.
- Staff access limited to what is necessary to deliver the service.
- Only essential cookies: a session cookie during a purchase and a Stripe cookie for payment security. No tracking, advertising or analytics cookies without consent.

## Retention

| DATA TYPE | RETENTION PERIOD | REASON |
|---|---|---|
| **Survey responses and scores** | 24 months after report generation | Product improvement and benchmarking |
| **Generated reports (PDF)** | 24 months, then customer may request a copy | Client access and reference |
| **Purchaser records (name, email, org)** | For as long as your account is active | Ordinary business record, client support and follow-up |
| **Financial and transaction records** | 7 years | Legal obligation (tax records) |
| **Respondent email addresses (managed outreach)** | 24 months from assessment close | Supports the re-measure comparison and aggregate research, then permanently removed |
| **Server logs** | 30 days | Security monitoring |

## Your rights, and what happens after a breach

**Your rights.** Under the NZ Privacy Act 2020 and the Australian Privacy Principles you can request access to, and correction of, personal information Clairsyn holds about you, and complain (privacy.org.nz; oaic.gov.au). In the UK and EU you can also object to processing and request erasure, restriction and portability, and lodge a complaint with your supervisory authority. Threshold survey answers are not linked to any individual, so no one, Clairsyn included, can find a single response to change it. Clairsyn responds to privacy requests within 20 working days.

**Breaches.** If Clairsyn becomes aware of a personal information breach likely to cause serious harm, it notifies affected individuals and the relevant regulator as soon as practicable: the Office of the Privacy Commissioner (NZ), the OAIC under the Notifiable Data Breaches scheme (AU), the relevant supervisory authority within 72 hours (UK/EU), and the Privacy Commissioner of Canada under PIPEDA.