

Record of Processing Activities

Article 30, UK GDPR and EU GDPR

Richard Flook Limited · Internal · Draft for legal review

Article 30, UK GDPR and EU GDPR

Controller	Richard Flook Limited
Company number	12542030
Registered address	86 Shirehampton Road, Bristol BS9 2DR, United Kingdom
Contact for data protection	frankie@richardflook.com
Document version	1.0 — draft for legal review
Date	1 October 2026
Review cycle	Annually, and on any change of processor, purpose or data category

1. SCOPE OF THIS RECORD

This record covers all processing of personal data carried out by Richard Flook Limited in the delivery of Eclipse, The Study, and the Quantum Turn, and in the related analytical pipeline (Harmonic Fractal Mapping, the Octon Map, and OpenEvolve runs).

2. PURPOSE A — DELIVERY OF GUIDED VOICE SESSIONS AND COMPUTATIONAL ANALYSIS

Description. A client is taken through a guided voice session. Session content is transcribed, analysed mathematically against the client's Fractal Mapping Chart, and run through the computational pipeline to produce a personalised report.

Field	Detail
Categories of data subject	Adult clients aged 18 and over. Guardians of clients below the minimum age, where guardian access has been granted.
Categories of personal data	Name; contact details; date, time and place of birth; health and wellbeing information disclosed in session; session transcripts and practitioner notes; Fractal Mapping Chart data; derived computational outputs.
Special category data	Yes — data concerning health (Article 9(1))
Purpose	Provision of the contracted service; personalisation of sessions; generation of client-facing reports.
Lawful basis (Article 6)	Article 6(1)(b) — performance of a contract with the data subject.
Condition (Article 9)	Article 9(2)(a) — explicit consent. See the accompanying Article 9 condition memo.
Recipients / processors	Mistral AI (EU endpoint) — language model inference. Gadium — voice synthesis and transcription. Hosting and email providers as listed in section 6.
	International transfers
Retention	90 days after the last visit, then deletion. Backups are held for a further 10 days, then deleted.
Source of data	The data subject.
Automated decision-making	No solely automated decision with legal or similarly significant effect. A human practitioner reviews and authors every client-facing output (Article 22 safeguard).

Voice. Eclipse speaks with a catalogue voice, or with Richard's own cloned voice under his own consent. No client voice is cloned or reproduced, so voice biometric data is not processed on the

client path. If a client voice were ever cloned, that would be a new processing activity requiring its own Article 9 entry, its own explicit consent instrument, and an Enterprise zero-retention arrangement covering the voice sample.

3. PURPOSE B — RESEARCH, TEACHING AND PRODUCT IMPROVEMENT

Description. Mathematical and structural outputs from the pipeline are used to improve the method, to teach it, and to publish methodology.

Field	Detail
Categories of data subject	Clients whose mathematical outputs inform the method.
Categories of personal data	Derived mathematical outputs only. No personal, trauma or name-identifying content.
Special category data	None, on the condition that identifying and trauma content is excluded before use.
Purpose	Method development, teaching, publication of methodology.
Lawful basis (Article 6)	Article 6(1)(a) — consent.
Condition (Article 9)	Not engaged where content is genuinely non-identifying. Where any identifying element is retained, Article 9(2)(a) explicit consent applies.
Recipients	None external for any identified data.
Retention	As per the underlying client record.

Legal flag. The line between "mathematical output" and "personal data" must be demonstrable, not assumed. Where a derivative could be re-linked to an individual — combined with a chart, a date of birth, or a quote — it remains personal data and may remain special category data. A re-identification risk assessment should sit behind this row.

4. PURPOSE C — CLIENT ADMINISTRATION, BILLING AND CORRESPONDENCE

Field	Detail
Categories of personal data	Name; contact details; subscription tier; payment records; correspondence.
Special category data	Incidental only, where a client volunteers health information in correspondence.
Purpose	Account management, billing, client support, and the handling of data requests.
Lawful basis (Article 6)	Article 6(1)(b) contract; Article 6(1)(c) legal obligation for financial records.
Condition (Article 9)	Article 9(2)(a) explicit consent where health information is volunteered.
Retention	Financial records as required by law. Correspondence as per the 90-day rule.

5. PURPOSE D — GUARDIAN ACCESS FOR CLIENTS BELOW THE MINIMUM AGE

Field	Detail
Categories of data subject	Guardians of clients below the minimum age.
Categories of personal data	Guardian name and contact details; relationship to the client; access and deletion actions taken.
Purpose	Allowing a guardian to access and delete a minor's information.
Lawful basis (Article 6)	Article 6(1)(c) — legal obligation; Article 6(1)(f) — legitimate interests in safeguarding.
Condition (Article 9)	Article 9(2)(a) explicit consent, or Article 9(2)(c) vital interests where applicable.
Retention	As per the underlying client record.

6. PROCESSORS AND INTERNATIONAL TRANSFERS

Processor	Role	Location	Transfer mechanism	Status
Mistral AI — French company, reg. 952 418 325 , 15 rue des Halles, 75001 Paris	Language model inference	France (EU endpoint)	None required — EU processing, no third-country transfer	PAYG enabled; Organisation and billing both named Richard Flook Limited. Training verified OFF on both surfaces (API → Privacy toggle and subscription consent checkbox), Labs-models toggle also OFF. Screenshots filed. Zero Data Retention not enabled. Standard API logs retained 30 rolling days. EU endpoint pinning pending.
Gradium	Voice synthesis / transcription	France — Gradium SAS, Paris. ISO 27001:2022 certified. Control plane EU-hosted for all customers.	EU residency enrolment required — NOT YET ENABLED. Verified by live read-only probe, 7 Oct 2026: wss://eu.api.gradium.ai/api/speech/tts returns residency: "best-effort; zone=eu"; wss://api.gradium.ai/api/speech/tts returns residency: "none". Per Gradium's own documentation, best-effort on a region endpoint means residency has not been enabled on the plan. The default endpoint therefore carries no residency commitment and can process in the US. Enrolment request sent to support@gradium.ai 5 Oct 2026 (see 08-gradium-residency-request-SENT-2026-10-05.eml.md); no reply received as of 7 Oct 2026 across all five configured mailboxes. Open with the vendor: whether the entitlement follows the plan tier (M, credit-funded) or the billing state. Until granted, pin the integration to eu.api.gradium.ai and treat any response other than pinned; zone=eu as a configuration error.	Zero Data Retention — in force (retention disabled under My organisation → Privacy Settings, per Gradium FAQ). DPA — obtained and filed (ToS Exhibit 1, gradium-data-processing-agreement-v2026-07-22.pdf). Residency — pending; request sent 5 Oct 2026, no reply. DPA Appendix 1 §8 — verified verbatim, 7 Oct 2026: "The Processing is not designed to include sensitive data or special categories of data within the meaning of Applicable Privacy Laws. If such Personal Data are processed, they will only be collected and processed according to Client's instructions for providing the Services." Interpretation: this is not a refusal. It states the service is not designed for special category data and that such data, if processed, is processed on the Client's instructions — so the Article 9 safeguard rests on the Controller, not on Gradium. This is a documented residual risk with mitigation (controller-side Art.9(2)(a) explicit consent per the Article 9 memo; ZDR in force; EU residency pending; on-device Phonon route or

Processor	Role	Location	Transfer mechanism	Status
				self-hosted image as the fallback that removes Gradium from the client-data path entirely) — not a live fault . A question on what Gradium expects of a controller processing health data under §8 is drafted as Request (c) in the 5 Oct letter.
	Oracle Cloud Infrastructure	Application hosting and storage	France — eu-paris-1 (Paris)	None required — EU processing, no third-country transfer
	Namecheap Private Email	Client correspondence — sends as Eclipse eclipse@howcaniheal.org , the single client-facing address	United States — Los Angeles	UK Addendum to the EU SCCs NOT CONFIRMED IN WRITING — this is the live fault . Their DPA incorporates EU SCCs Module 2, but its UK clause cites the superseded 2010/87/EU clauses rather than the 2022 UK Addendum. Request sent to dpo@namecheap.com (6 asks, incl. this one — see 11-namecheap-dpa-confirmation.eml.md); no reply received as of 7 Oct 2026 across all five configured mailboxes. Client correspondence currently travels this US path with the transfer safeguard unconfirmed , and this is the path client email — including tester invitations — actually uses. Escalate or migrate the mailbox if no reply is received.

Out of scope. Development and experiment LLM lanes — DeepSeek, Gemini, Claude, and free-tier providers among them — are not processors under this record, because no client data flows through them. If that ever changes, each one becomes a processor and enters this table.

Action. Every row marked "to be confirmed" must be completed before that processor touches client data. An unconfirmed row is an unassessed transfer.

6A. CONTROLLER ESTABLISHMENT AND EU REPRESENTATION — UNDER REVIEW

Status: revised 1 October 2026, not settled. An earlier version of this section recorded, on the Controller's word, that "Richard Flook Limited is NOT established in the EU", and derived an Article 27 obligation from it. **That reasoning was incomplete.** It treated **incorporation** (UK) as though it settled **establishment** (a separate, fact-based test). The Controller has since disclosed facts that point the other way — see below. **Do not rely on this section until the solicitor has determined it.**

The establishment question — open, and it decides everything else

Establishment is not incorporation. Per Weltimmo and Google Spain, establishment means "any real and effective activity — even a minimal one — exercised through stable arrangements", and "the legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor."

The EDPB sets the threshold low:

"The threshold for 'stable arrangement' can actually be quite low... the presence of one single employee or agent of a non-EU entity in the Union may be sufficient to constitute a stable arrangement (amounting to an 'establishment' for the purposes of Art 3(1)) if that employee or agent acts with a sufficient degree of stability."

Article 3(1) does **not** require the EU establishment to carry out the processing itself — only that the processing be "in the context of the activities" of that establishment, read by Google Spain as "inextricably linked".

Facts now on record (disclosed by the Controller, 1 October 2026):

Fact	Status
The Ltd is incorporated in the UK (registered office, Bristol)	Settled
The Ltd currently does no trading — no clients, no client data, no processing	Settled
The Controller lives in France and is an EU resident, with a French address	Settled
The Controller directs the Ltd from France	Settled — and this is the operative fact
The Controller's auto-entrepreneur business is a separate undertaking , not the same activity	Settled — and it helps: it is not the Ltd's activity, so it does not make the Ltd EU-established through it
The Controller intends the whole Eclipse business to be run from the UK	Intention, not yet a fact

Two questions are separate, and only the second matters here: where the Ltd is incorporated (UK — settled), and where it is directed and operated from (France now; the UK is intended).

The question is currently DORMANT. Article 3 engages on processing, and the Ltd does no trading and processes no client data. Nothing needs fixing today; what is needed is a decision **before the first client's data is processed**, and substance built to match it.

The EDPB passage that decides it

Where a person is based in the EU but the processing relates to the controller's activities **outside** the EU, the mere presence of that person in the EU does **not** bring the processing into scope:

"When an employee is based in the EU but the processing is not being carried out in the context of the activities of the EU-based employee in the Union (i.e. the processing relates to activities of the controller outside the EU), the mere presence of an employee in the EU will not result in that processing falling within the scope of the GDPR."

So a director sitting in France directing a **genuinely UK business** is not automatically an establishment — but it depends on the processing actually relating to the UK activity, not the French one. Intent is not the test; facts at the time of processing are.

The trade-off the Controller should see clearly

Running Eclipse from the UK does not remove the Article 27 obligation — it creates it. Article 27 exists precisely for controllers outside the Union serving EU data subjects.

	Lead supervisory authority	EU representative
UK-operated (the stated intention)	ICO	Required for EU clients
EU-established	CNIL	Not required

To make UK operation real, not merely intended

At the moment the first client's data is processed, a regulator examines **facts**, not intentions. "I meant it to be UK-run" is not a defence. Build the substance:

- [] Hosting and processing anchored to the UK
- [] Banking, contracts, registered office and client-facing details all UK
- [] **The Ltd actually trading**
- [] Decisions documented as taken in the UK
- [] On that footing: **appoint an independent Article 27 representative before the first EU client**, and name them in the privacy notice

If a representative IS required — can the Controller act as its own?

Technically he meets the location test: Art. 4(17) defines a representative as a natural or legal person established in the Union, and he is one, in France.

But it is a weak arrangement and should not be relied on. The role exists to give EU data subjects and supervisory authorities a local counterparty — EDPB: "facilitating the liaison with and ensuring effective enforcement of the GDPR against controllers." If the representative is the Controller's own director, there is no separate party to address and the enforcement purpose is hollow.

The EDPB has already excluded overlapping roles on this reasoning — the **DPO** (independence) and the **processor for the same controller** ("given the possible conflict of obligation and interests in cases of enforcement proceedings"). Controller-as-representative is not expressly addressed but fails identically.

A representative can also **itself be subject to enforcement proceedings** — a real role with real exposure, not a mailbox.

Unless the solicitor holds otherwise: appoint an independent representative, and do not self-appoint.

If Article 27 does apply — the requirements

- Established in a **Member State where the EU data subjects are** (Art. 27(4)) — France, for a French EU client base.
- The **addressee for EU supervisory authorities and data subjects** (Art. 27(5)).
- **Named in the privacy notice.**
- **Transfers are a separate question.** UK adequacy covers EU→UK; no SCCs needed. Representation is not a transfer mechanism.

7. RETENTION SCHEDULE

Data	Retention	Then
Session records, transcripts, notes	90 days after last visit	Deleted
Backups containing the above	90 days + 10 days	Deleted
Client account and billing records	Duration of relationship + statutory period	Deleted
Data subject requests and their outcomes	3 years	Deleted

Clients may request earlier deletion at any time.

8. SECURITY MEASURES

- Encryption at rest: Oracle Cloud boot volume in eu-paris-1 encrypted with an Oracle-managed key (kms_key_id unset); no LUKS layer. Verified 6 October 2026.
- Encryption in transit: TLS for the application (Let's Encrypt via nginx); STARTTLS for mail.
- Access to client records restricted to named individuals with a role-based need.
- Transport encryption for all processor traffic.
- Processor DPAs held on file before data flows.
- Provider training opt-out recorded and evidenced.
- Deletion jobs verified, not assumed.

9. DOCUMENTATION OF THE ARTICLE 9 CONDITION

See the accompanying memo: Article 9 Condition — Legal Basis for Processing Health Data.

This is a working draft prepared to be reviewed and finalised by a qualified data protection solicitor before it is relied upon.

Richard Flook Limited · Record of Processing Activities · Confidential