

Eclipse — Legal and Data Protection Pack

Documents produced 1 October 2026 · 81 pages · 14 sections

Controller: **Richard Flook Limited** · Company number 12542030 ·
86 Shirehampton Road, Bristol BS9 2DR, United Kingdom · richard@richardflook.com

SECTION	STATUS	PAGE
01 Record of Processing Activities (Art. 30)	Internal — draft for legal review	2–6
02 Data Protection Impact Assessment (Art. 35)	Internal — draft for legal review	7–10
03 Processor Onboarding Checklist — Mistral AI	Internal — operational	11–16
04 Article 9 Condition — Health Data (memo to file)	Internal — draft for legal review	17–18
05 How We Handle Your Information (client notice)	Client-facing, version 1.0	19–20
06 Eclipse — Processing Chain and Data Flow	Internal architecture note	21–23
07 Processor Onboarding Checklist — Gadium (Voice)	Internal — operational	24–29
08 Email — Gadium Residency and DPA Request	Draft, ready to send	30–31
09 Eclipse — Terms of Service and Privacy Policy (web pages)	Draft for legal review — consumer terms	32–39
10 Evidence Index — Eclipse Data Protection Pack	Document register	40–42
11 Note to File — Mistral AI Account Holder	Awaiting director signature	43
12 Exhibit 1 — Gadium Data Processing Agreement (22 Jul 2026)	Vendor document, authenticated download	44–53
13 Exhibit 2 — Gadium Terms of Service (22 Jul 2026)	Vendor document, authenticated download	54–77
14 Exhibit 3 — Mistral console evidence (screenshots, 1 Oct 2026)	Captured from the live console	78–81

Contents. Sections 01–11 are our own documents; 12–13 are vendor contracts held as exhibits; 14 is console evidence. Sections 01, 02, 04, 05 and 09 are the ones put forward for legal review.

Provenance. Exhibits 12–13 were downloaded from the Gadium Trust Center after signing their non-disclosure agreement and carry the authenticated-download watermark. The ISO 27001:2022 certificate and report are view-only in the Trust Center and are recorded by link in section 10, not filed here.

Outstanding. Section 11 awaits the director's signature. The Gadium residency request in section 08 is drafted and not yet sent.

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 Human Design 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; Human Design 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	None outside the EEA on the sanctioned path. Mistral inference is served from the EU endpoint. Confirmed per processor in section 6.
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.
Gadium	Voice synthesis / transcription	France — Gadium SAS, Paris. ISO 27001:2022 certified. Control plane EU-hosted for all customers.	EU residency enrolment required. The default endpoint api.gadium.ai carries no residency commitment and can process in the US. Enrol (support@gadium.ai) and pin to eu.api.gadium.ai; assert pinned; zone=eu on every response.	Zero Data Retention — in force . DPA — obtained and filed (ToS Exhibit 1). Residency — request to send. Note: DPA Appendix 1 §8 states the processing is not designed for special category data.
Hosting provider	Application hosting and storage	To be confirmed	To be confirmed	—
Email provider	Client correspondence	To be confirmed	To be confirmed	—

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

- 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

Data Protection Impact Assessment

Article 35, UK GDPR and EU GDPR

Richard Flook Limited · Internal · Draft for legal review

Article 35, UK GDPR and EU GDPR

Controller	Richard Flook Limited (12542030)
Processing assessed	Eclipse voice sessions and the Quantum Turn analytical pipeline
Document version	1.0 — draft for legal review
Date	1 October 2026
Assessor	Richard Flook, with drafting support

1. WHY A DPIA IS REQUIRED

A DPIA is mandatory where processing is likely to result in a high risk to the rights and freedoms of individuals. This processing meets that threshold on three counts:

- 1. **Special category data.** The processing involves data concerning health (Article 9(1)).
- 2. **Large-scale processing of special category data.** Client records are processed systematically and continuously, not occasionally.
- 3. **Innovative technology.** Artificial intelligence is used to analyse personal data and to generate outputs about the individual.

Any one of these would call for an assessment. Taken together, the assessment is not optional.

2. SYSTEMATIC DESCRIPTION OF THE PROCESSING

The chain, in order:

- 1. A client speaks with Eclipse. Audio is captured.
- 2. Speech is transcribed to text (Gadium).
- 3. The transcript is passed to a language model for session support and analysis (Mistral AI, EU endpoint).
- 4. Session content and the client's chart are compiled into the analytical pipeline (Harmonic Fractal Mapping, Octon Map).
- 5. An evolutionary run produces a personalised clearing circuit (OpenEvolve).
- 6. A human practitioner reviews the output, authors the client-facing documents, and holds the clinical judgement.
- 7. Documents are delivered to the client. Records are retained for 90 days after the last visit.

Data involved: health and wellbeing information, birth data, session transcripts, chart data, and derived computational outputs.

Individuals affected: adult clients; guardians of clients below the minimum age.

3. NECESSITY AND PROPORTIONALITY

Question	Assessment
Is the processing necessary for the purpose?	The service cannot be delivered without analysing session content against the client's chart. The processing is the service.
Is it proportionate?	The client supplies the data knowingly for a paid, guided service. Nothing is collected beyond what the method requires.
Could it be done with less data?	Retention is capped at 90 days. Teaching and research use excludes personal and trauma content.
Is there a less intrusive method?	Not for this method. The analytical step is intrinsic to the product.

Question	Assessment
Are the individuals' expectations respected?	The privacy notice states plainly what is processed, by whom, and for how long.

Conclusion on necessity: the processing is necessary and proportionate to a service the client has chosen and paid for.

4. CONSULTATION

Where a DPIA identifies a high residual risk that cannot be mitigated, the supervisory authority must be consulted before processing begins. This draft proceeds on the basis that the mitigations in section 6 reduce residual risk to an acceptable level. **If, on legal review, that is not accepted, the ICO (UK) or the relevant EU authority must be consulted before the pipeline handles further client data.**

5. RISK ASSESSMENT

#	Risk	Likelihood	Severity	Inherent risk
R1	Health data reaches a processor that trains on it	Medium	High	High
R2	Health data is transferred outside the EEA without a safeguard	Medium	High	High
R3	A client is identifiable from material used for research or teaching	Medium	High	High
R4	Re-identification of a "mathematical" output by combination with other data	Low	High	Medium
R5	A subcontractor of a processor handles data outside the assessed region	Medium	Medium	Medium
R6	Retention runs past the stated 90 days because deletion is assumed rather than verified	Medium	Medium	Medium
R7	Automated output is treated as clinical advice without human review	Low	High	Medium
R8	Consent is not genuinely explicit, specific or freely given	Medium	Medium	Medium
R9	A client's data request is not answered within 30 days	Low	Medium	Low
R10	The processor's own DPA states its processing is not designed for special category data (Gadium, Appendix 1 §8), while our session content is health data	Medium	High	High
R11	EU establishment undetermined, and Article 27 follows from it. If the Ltd is not established in the Union, an EU representative is required and none is appointed; the Art. 27(2) exemption fails on health data processed systematically. If it is established, no representative is required but the lead supervisory authority changes	High	Medium	High

6. MEASURES TO ADDRESS THE RISKS

#	Risk	Measure	Residual risk
R1	Training on health data	Provider training opt-out set and evidenced. Zero-data-retention enabled where offered.	Low
R2	Third-country transfer	EU endpoint used for inference. Every processor's residency confirmed and recorded in the Article 30 record.	Low
R3	Identifiability in research	Personal, trauma and name-identifying content excluded before any teaching or research use. Re-identification risk assessment behind the exclusion.	Low
R4	Re-identification by combination	Publication is limited to methodology and mathematical structure, and is reviewed before release.	Low
R5	Unknown subprocessors	DPA requires notification of subprocessor changes. Subprocessor list reviewed on each change.	Low

#	Risk	Measure	Residual risk
R6	Retention overrun	Deletion job runs on schedule and is verified by query, not by assumption.	Low
R7	Output treated as advice	A human practitioner reviews and authors every client-facing output. Automated output is not delivered unreviewed.	Low
R8	Quality of consent	Explicit consent captured separately, specific to the purpose, informed by the privacy notice, and withdrawable.	Low
R9	Data requests	30-day internal deadline. Requests logged and tracked to completion.	Low
R10	Processor not designed for special category data	The responsibility is ours, not the processor's, so the Article 9 condition, the explicit consent capture and data minimisation are the load-bearing safeguards and are documented as such. Enrolling EU residency removes the cross-border element. Evaluating the on-device (Phonon) route would take session audio out of the processor's scope entirely. Raised with Gadium to confirm what they expect of a controller in this position.	Medium
R11	EU establishment undetermined	Determine establishment first — it decides the rest. The Controller is a French resident directing the business from France, which may constitute a stable arrangement and therefore an EU establishment (contractor's own activity counts; legal form is not decisive). If established: no Art. 27 appointment, but the lead supervisory authority becomes the CNIL. If not established: appoint an independent Art. 27 representative — the Controller should not self-appoint, as the role exists to be a counterparty distinct from the Controller.	High until determined

Processor security assurance — evidence held

Item	Position
Gadium Data Processing Agreement	Obtained and filed — standalone, 10 pages, authenticated Trust Center download
Gadium Terms of Service	Filed — the agreement incorporating the DPA as Exhibit 1
ISO 27001:2022 certification	Accepted on Gadium's public statement — certified, independently audited by A-LIGN. Certificate and report are view-only in the Trust Center and not downloadable; the access links are recorded in <code>legal/evidence/INDEX.md</code> , with the note that reaching the files requires signing Gadium's NDA. Requested by email as a fallback (email Request 3)
Zero Data Retention	In force on the account — data retention disabled in Privacy Settings
Subprocessors	Three, listed and assessed: Scaleway (Paris), AWS (Luxembourg), Clerk (San Francisco — identity only, recorded as a transfer to confirm)
Trust Center controls	Vendor-asserted controls published and reviewed, including "Data retention procedures established" and "Customer data deleted upon leaving"

Full document register: `legal/evidence/INDEX.md`.

7. THE HUMAN-IN-THE-LOOP SAFEGUARD

Article 22 restricts solely automated decision-making that produces legal or similarly significant effects. This processing does **not** qualify as solely automated, because a qualified human practitioner reviews the analytical output and authors the client-facing result. That human review is the safeguard, and it must remain genuine: if the pipeline output were ever delivered to a client without practitioner review, this assessment would no longer hold and would need to be redone.

8. OUTCOME

Residual risk after mitigations	Low to medium
---------------------------------	----------------------

Processing may proceed	Yes — subject to legal sign-off and completion of every "to be confirmed" processor row
Supervisory authority consultation required	Not on this assessment — unless legal review disagrees
Next review	On any change of processor, model, purpose or data category; otherwise annually

9. SIGN-OFF

Role	Name	Date	Signature
Controller	Richard Flook		
Legal reviewer			

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

Processor Onboarding Checklist — Mistral AI

Article 28 processor requirements

Richard Flook Limited · Internal · Operational

Applies to: all client data processed through Eclipse, The Study, the Quantum Turn, and the OpenEvolve pipeline.

Provider	Mistral AI
Role	Processor (Article 28)
Controller	Richard Flook Limited (12542030)
Document version	1.0
Date	1 October 2026

WHY THIS CHECKLIST EXISTS

A Data Processing Agreement is the instrument that makes sending personal data to a language model lawful. It is mandatory under Article 28 and it is the first thing a regulator asks for. But Mistral's DPA contains a clause that matters more than the signature line: **Mistral acts as Controller for AI model training unless the customer opts out.** The default is training on your data.

That means accepting the DPA alone is not enough. The opt-out must be set, and evidenced, before the first client record goes near the endpoint.

1A. ACCOUNT HOLDER — RESOLVED AT ORGANISATION LEVEL

Finding, 1 October 2026: the Mistral account was held under "**Richard Flook**" — the individual — not **Richard Flook Limited** (company 12542030), the Controller under this record.

What was done. The **Organisation name has been changed to Richard Flook Limited.**

This is the meaningful fix, and better than renaming the workspace would have been. In Mistral's model the **Organisation is the top-level entity** — billing, members, and every workspace sit beneath it, and the Data Processing Addendum is accepted at that level. So the entity that presents to Mistral as the customer is now Richard Flook Limited, which is the entity that holds the client data.

Level	Name	Significance
Organisation	Richard Flook Limited ✓	Top-level entity — billing, members, DPA acceptance
Workspace	(beneath the organisation)	Label only; isolates keys and usage

What the residual is now. Narrower than before. The account's login and the payment method remain personal to Richard Flook, a director of the company. The company's position is that the account is operated in his capacity as director and for the company's business.

Residual mitigation. The **Note to File** at evidence/mistral-account-holder-note-2026-10-01.md records that the account is operated by Richard Flook on behalf of Richard Flook Limited as Controller. It has been updated to reflect that the organisation now names the company, and addresses only the remaining personal-login point. **It requires the director's signature.**

The full fix, if ever needed. Mistral's **Team plan** provides organisation administration — member roles, SSO and an allowed-email-domain control. Not required: the organisation already carries the company name, and the remaining gap is the login and payment method, which the Note to File covers.

Remaining actions.

- [x] **Organisation renamed to Richard Flook Limited** — done 1 Oct 2026
- [] **Sign the Note to File** — evidence/mistral-account-holder-note-2026-10-01.md
- [] Confirm the **DPA is accepted against the organisation**, and therefore against the Ltd — check Settings → Organisation/Legal
- [] Check **Gradium** on the same point: its workspace reads "Richard Flook Heal Better" — establish whether that is a registered entity, a trading name, or a personal account, and whether its filed DPA names the Ltd

1B. PLAN POSITION — PAYG ENABLED, NO USAGE YET

Recorded 1 October 2026. Mistral's confirmation email states: "Pay-as-you-go has been enabled on your account for the organization Richard Flook Limited. You can now use the API beyond the included monthly usage, billed monthly or drawn from your credits."

Item	State
Plan	Pay-as-you-go — enabled
Payment method	VISA ····8118, marked Default
Billing name	Richard Flook Limited
Billing address	86 Shirehampton Road, Bristol BS9 2DR, GB
Credits	€0.00
Auto Recharge	Disabled
Usage / invoices	None — nothing has been run

Note on what "subscribed" means here. Mistral's API is **pay-as-you-go**, not a subscription product. There is no further step to take: enabling PAYG with a payment method on file makes the lane live. "Not subscribed" means simply that no usage has been incurred and no commitment has been made — which is the correct state during Beta.

The product is in Beta and has no users, so no client data is flowing through this lane.

Mistral AI's registered identity (from their own confirmation email, for the processor record):

Mistral AI — a French company incorporated in Paris, registration number **952 418 325**, registered office at **15 rue des Halles, 75001 Paris**, France.

The gate, in full. No client data touches Mistral until **all four** are true:

#	Condition	State
1	PAYG enabled with a payment method on file	✔ Done — confirmed 1 Oct 2026
2	DPA accepted against the Organisation	✔ Organisation named Richard Flook Limited — see §1a
3	Training opted out on BOTH surfaces — API → Privacy toggle AND subscription consent checkbox	✔ Verified 1 Oct 2026 — both OFF. Screenshots filed. Labs-models toggle also OFF — see §1c
4	EU endpoint pinned — api.eu.mistral.ai	⌚ Config not yet written

Until all four hold, the Mistral lane carries **no client data**.

1C. TRAINING OPT-OUT — BOTH SURFACES VERIFIED OFF

Verified 1 October 2026 by inspection of the account. There are **two independent controls**, and both are now confirmed in the protected state. Evidence filed as screenshots in legal/evidence/.

Surface 1 — API → Privacy ✔ **OFF**

Page: admin.mistral.ai/platform/privacy — "Manage your privacy settings for our API."

Toggle	State	Section
"Allow the use of your API calls to train Mistral's AI models."	OFF ✔	Data usage for improving our services
"Enable Labs models"	OFF ✔	Activation of Labs Models

The Labs toggle is the one that would have quietly undone everything else. Its own consent wording, verbatim: "I confirm that I am using Labs for professional testing and agree that my data may be used to train Mistral models, regardless of my subscription plan or opt-out settings, in accordance with the Commercial Terms of Service."

Had that been ON, the training toggle above it would have been academic. **It is OFF, and it must stay off.** This is the single most important state on that page.

No ZDR control appears on this page — consistent with Zero Data Retention being a Scale-plan feature requested separately, not a console toggle.

Surface 2 — PAYG subscription flow CLEAR

Presented as a **checkbox** on `admin.mistral.ai/subscription`:

"Allow the use of your API calls to train Mistral's AI models."

"By allowing us to train our models with your data, you help improve the performance of our models for you and for all our users. If you disable this option, your new interactions, or those of your users, will not be used to train our models. Learn more"

State observed: UNCHECKED — i.e. opted out. The control presents as an opt-in, so leaving it clear is the protected position.

Both controls exist — corrected a second time. The subscription-flow checkbox is **one** control. The admin sidebar also shows **API → Privacy** (alongside **Vibe → Privacy**), which is exactly where the documentation places the API training setting. An earlier note in this pack claimed the API Privacy page "is not the control on this account" — **that was wrong**. The sidebar confirms it exists, and Mistral's documentation is explicit that the surfaces are independent: opting out of one does not cover the other.

So: verify both. Do not assume the subscription checkbox covers the API Privacy page, or vice versa. Screenshot each.

Admin console map, as observed:

Section	Pages
Administration	Organization · Access · Trusted issuers · Members · Workspaces · Connectors
Subscription	Subscription · Billing
Vibe	Preferences · Privacy
API	API Keys · Usage · Limits · Privacy

Two separate Privacy pages, one per surface. That is the structure the documentation describes, and the sidebar is the confirmation.

Actions

- [] **Leave the checkbox UNCHECKED when subscribing.** Stated plainly because it is the whole exercise.
- [] **Screenshot the subscribed state**, with a date, and file it in `legal/evidence/`. The screenshot is the evidence, because it is the post-subscription state that governs.
- [] Re-verify on any plan change or terms update.

Two other observations from the same page

Billing name already reads Richard Flook Limited — the entity is correct at billing level as well as at organisation level. Good.

Billing address — resolved differently to how it was first framed. The billing address on file has been set to the company's registered office, **86 Shirehampton Road, Bristol BS9 2DR, GB**.

Correcting an earlier note in this pack. This section previously said the billing address and the registered office "should not disagree." That was wrong. They serve different purposes and routinely differ: a **billing address** is verified against the cardholder record as a fraud control (AVS), while the **registered office** is what identifies the Controller. If a payment method requires the French address to authorise, that is a payment detail with no bearing on the controller's identity. Bristol remains correct for the record.

EU establishment — REOPENED, not settled

Corrected 1 October 2026. An earlier version of this section recorded that "Richard Flook Limited is NOT established in the EU" and derived an Article 27 requirement from it. **That conflated incorporation with establishment.** Establishment is a separate, fact-based test, and facts later disclosed by the Controller point the other way. See §6a of the Record of Processing Activities for the full position. **Do not treat the Article 27 requirement as settled, in either direction.**

What is now on record: the Ltd is UK-incorporated; it **currently does no trading**; the Controller lives in France and **directs the Ltd from France**; and the Controller's **auto-entrepreneur business is a separate**

undertaking — which helps, because it is not the Ltd's activity and so does not make the Ltd EU-established through it. The Controller **intends** the whole Eclipse business to be run from the UK.

The question is currently dormant. Article 3 engages on processing, and there is none yet. What is needed is a decision before the first client's data is processed, and substance built to match it.

Why it matters more than the appointment: if the Ltd is established in the Union, Article 27 does not apply at all — and **the lead supervisory authority becomes the CNIL rather than the ICO**. That is the larger consequence.

But note the direction of travel. A UK-operated business is precisely what Article 27 exists for — so **running Eclipse from the UK does not remove the representation obligation, it creates it**. UK operation means ICO plus an independent representative for EU clients; EU establishment means CNIL and no representative. Choose deliberately, because the two are exclusive.

On self-appointment. The Controller technically meets Art. 4(17)'s location test, but the role exists to give authorities a counterparty distinct from the Controller. The EDPB has excluded overlapping roles (DPO, processor) on conflict grounds; controller-as-representative fails identically. **Appoint independently, and do not self-appoint.**

One point that is settled regardless: transfers EU → UK are not the issue. The UK holds an EU adequacy decision, so no SCCs are needed. Representation is not a transfer mechanism.

Two carve-outs that survive the opt-out

These apply on **every** plan and are the real traps:

1. Thumbs up / thumbs down feedback. From Mistral's own DPA:

"if Customer provides feedback to Mistral AI by using the in-app 'thumbs up' or 'thumbs down' features (the 'Feedback'), Mistral will use such Feedback as well as the associated Input and Output, as Controller, to train its artificial intelligence models..."

The main toggle **does not** protect rated content. Mistral steps out of the Processor role entirely for rated conversations.

Operational rule: never use the thumbs up/down controls on anything client-derived. Not in Vibe, not in Studio, not in a playground. It converts a processed record into a training record regardless of the setting.

2. Labs (experimental) models may train on data **regardless** of plan or opt-out. There is no setting for it.

Operational rule: never run client-derived content through a model marked Lab, experimental, or preview.

Also worth knowing

- **Not retroactive.** The opt-out does not recall data submitted before it was set.
- **Zero Data Retention is unavailable on this plan.** ZDR is **Scale-plan only**, and only for stateless API calls. On the free tier, standard API logs are retained **30 rolling days** for abuse monitoring.
- **No API exists to read the toggle state.** Mistral does not expose one — verification is visual in the Admin panel. That is why the screenshots are the evidence.

1D. BEFORE ANY CLIENT DATA FLOWS

- [] **Account created under Richard Flook Limited**, not a personal account.
- [] **DPA accepted and archived.** Mistral's Data Processing Addendum, effective 27 July 2026, forms part of the service agreement. Save the accepted copy with the date to ~/heal-better/legal/evidence/.
- [] **Training opt-out activated.** Confirm in the account/console settings that your data is excluded from model training. If the setting is unclear, contact Mistral support in writing and keep the reply.
- [] **Zero Data Retention enabled** if available on the plan. Without it, prompts may be retained for abuse monitoring.
- [] **EU endpoint confirmed.** Inference must be pinned to `api.eu.mistral.ai`. Never the default endpoint — the default carries no regional guarantee.
- [] **Subprocessor list reviewed** and saved with the date. Mistral publishes it on the Trust Center. Note any subprocessor outside the EEA.

- [] **Payment and billing confirmed** so the account does not lapse mid-processing.

2. CONFIGURATION TO SET IN THE PIPELINE

- [] Base URL set to `https://api.eu.mistral.ai/v1`
- [] Model set to the sanctioned model for the lane (`mistral/ministral-3` or `mistral/mistral-small-4`)
- [] Any environment variable or config file that could override the endpoint back to a default is checked and removed
- [] The API key in use is the Richard Flook Limited key, stored as a secret, not in a repository

3. EVIDENCE TO KEEP ON FILE

Evidence	Where it lives	Reviewed
Accepted DPA, with date	legal/evidence/	
Training opt-out confirmation	legal/evidence/	
Zero Data Retention confirmation (if applicable)	legal/evidence/	
Subprocessor list snapshot, with date	legal/evidence/	
EU endpoint confirmation (a successful request log showing <code>api.eu.mistral.ai</code>)	legal/evidence/	
Support correspondence	legal/evidence/	

4. ONGOING OBLIGATIONS

- [] Re-check the subprocessor list on every notified change, and record the review.
- [] Re-verify the training opt-out after any plan or terms change.
- [] Review this checklist annually, or on any change to the service.
- [] If Mistral cannot meet its Article 28 obligations, processing stops and the incident is recorded.

5. WHAT IS EXPLICITLY NOT PERMITTED

- Client data through the **default** Mistral endpoint, or any endpoint without a confirmed region.
- Client data through Mistral with the training opt-out unset.
- Client data through **any development or experiment lane** — DeepSeek, Gemini, Claude, free-tier providers. The rule is about the lane, not the provider name. See the note below.
- Client data through a gateway that forwards to an unassessed provider.

NOTE ON THE DEVELOPMENT LANES — LANE SEPARATION

Development and experiments use a range of models — DeepSeek, Gemini, Claude, and free-tier providers among them. **None of them is used for client data, and no client material flows through any of them.**

What matters is not the provider but the **lane**. Client data has exactly one route, and it is not these. That separation is the control, and it is recorded here so that it is a documented decision rather than an assumption.

For the record, and because this is why the lanes are kept apart: Italy's data protection authority prohibited DeepSeek's processing in January 2025, and thirteen European jurisdictions opened investigations. The grounds were a non-compliant privacy notice, storage of personal data in the People's Republic of China without an adequacy decision, and the absence of an Article 27 representative. Berlin's authority took the position that DeepSeek transfers personal data to Chinese processors without a Chapter V safeguard.

The same reasoning applies in principle to any provider whose residency, retention or training position is unconfirmed. Client data uses the Mistral EU lane only.

"Free" models — three different things, only one of them safe by default

What "free" means	Data position
Open weights, self-hosted	Best. The data never leaves our hardware. No training clause applies, because no third party processes it.
Free on a provider's own API	Follows that provider's plan terms — see §1b and §1c

What "free" means	Data position
A free slot on a routing service (e.g. an : free model variant)	Check the downstream provider. Free endpoints frequently exist precisely because the provider receives the data. One publisher's census of free tiers puts it plainly: turning training off contracts the free pool.

The middle and last cases are not equivalent, and the last one is the trap — a free model and a private model are often the same slot, and you get one of them.

Devstral Small 2505 — noted

Apache 2.0 open weights. Mistral released it "for free under an Apache 2.0 license for the community to build on" — free to **download and self-host**, from HuggingFace, Ollama, Kaggle, Unsloth or LM Studio.

On Mistral's own API it is not free: priced at \$0.10/M input and \$0.30/M output, the same as Mistral Small 3.1. So if it appeared free, it was either the self-hosted route or a third-party free slot — and those carry different data positions, per the table above.

Why this is a good fit regardless: Devstral is a **coding** model, so it belongs to the development lane by nature — the lane that carries no client data. Both routes are therefore safe for its intended use. But the **self-hosted route is the only one that is both free and data-sovereign**, and it matches the stated intent to keep proprietary work off third-party compute entirely. It is the local-AI answer, in the one place it can be adopted today without touching the client-data question.

Caveat on the line. Mistral's own documentation marks the later **Devstral Small 1.1 as deprecated** — "Use Mistral Small 4 for new integrations" — and Mistral Small 4 now unifies Instruct, Magistral and Devstral into a single model. Building new work on the Devstral Small line means building on a deprecating one. Fine for an experiment; worth knowing before it becomes load-bearing.

NOTE ON GRADIUM (VOICE)

Gadium is a separate processor with its own onboarding checklist at 07-gradium-onboarding-checklist.md, because the actions differ from Mistral's in one important way: **Zero Data Retention is self-serve, EU residency is not.** Gadium's endpoint is eu.api.gradium.ai (enrolment required), Mistral's is api.eu.mistral.ai (no enrolment — just call it, at +10%).

Status at 1 October 2026: Gadium DPA obtained and filed, ToS filed, NDA signed, Zero Data Retention in force, residency requested.

Draft prepared for review by a qualified data protection solicitor.

Article 9 Condition — Health Data

Legal basis memo to file

Richard Flook Limited · Internal · Draft for legal review

Memo to file

Controller	Richard Flook Limited (12542030)
Purpose	Processing of data concerning health in the delivery of Eclipse, The Study and the Quantum Turn
Version	1.0 — draft for legal review
Date	1 October 2026

1. THE RULE

Article 9(1) of the UK GDPR and EU GDPR prohibits the processing of special category data. Data concerning health is special category data. There are ten exceptions in Article 9(2), and processing is lawful only if one applies — on top of, not instead of, a lawful basis under Article 6.

Two things must therefore be established, separately:

1. A **lawful basis under Article 6**.
2. A **condition under Article 9(2)**.

Article 9(2) conditions are interpreted restrictively.

2. ARTICLE 6 — LAWFUL BASIS

Article 6(1)(b) — performance of a contract with the data subject.

The client pays for a guided service. Session content cannot be analysed without processing the client's information. The processing is the service, not a by-product of it. This is the correct basis for service delivery.

For research, teaching and product improvement, the basis is **Article 6(1)(a) consent**, because that use is not necessary to deliver the service.

3. ARTICLE 9 — CONDITION FOR HEALTH DATA

Primary condition: Article 9(2)(a) — explicit consent

This is the condition relied upon.

Explicit consent is the cleanest route, and it is the honest one: the client is told, in specific terms, that their health and session information will be processed to deliver the service and by which processors, and they agree explicitly. Consent under Article 9 must be:

- **Explicit** — a clear, affirmative statement, separately captured. Not a pre-ticked box, not buried in terms and conditions.
- **Specific** — given for the stated purposes, not for processing in general.
- **Informed** — given after reading the privacy notice naming the processors and the retention period.
- **Freely given** — refusable without losing access to something the client is entitled to.
- **Withdrawable** — and withdrawal must be as easy as giving it.

Secondary condition: Article 9(2)(h) — health or social care

Article 9(2)(h) permits processing necessary for the purposes of preventive or occupational medicine, medical diagnosis, the provision of health or social care or treatment, or the management of those systems. In the UK, it also requires an associated condition in Schedule 1, Part 1 of the Data Protection Act 2018 (condition 2), and it applies only where processing is carried out by, or under the responsibility of, a professional subject to an obligation of professional secrecy.

Legal flag. Whether Article 9(2)(h) is available depends on whether the practitioner and the service fall within the scope of that provision, which is a matter of professional status and of the regulatory

position of the service. Article 9(2)(a) explicit consent does not depend on that question. **This memo therefore relies on explicit consent as the primary condition, and records 9(2)(h) only as a possible secondary basis to be confirmed on advice.** Consent carries no such dependency, and where consent is available it removes the need to resolve the question at all.

4. WHAT THIS MEANS IN PRACTICE

Requirement	Implementation
Separate, explicit consent capture	A distinct consent step at onboarding, separate from the terms of service and separately recorded.
Purpose-specific wording	Names the processing: session analysis, chart computation, report generation.
Named processors	Mistral AI (EU) and Gadium, named in the consent text and the privacy notice.
Withdrawal route	A stated route — reply to any email, or write to frankie@richardflook.com. Withdrawal must be actioned, not just offered.
Evidence	Each client's consent recorded with its date, and produced on request.
Children and guardians	Where the client is below the minimum age, consent is captured through the guardian route, with the guardian able to access and delete.

5. AUTOMATED DECISION-MAKING — ARTICLE 22

Article 22 restricts decisions based **solely** on automated processing that produce legal or similarly significant effects, and it is stricter still where special category data is involved.

This processing does not fall within Article 22. A qualified human practitioner reviews the analytical output and authors every client-facing result. The human review is not a formality — it is the reason the restriction does not apply. If a client-facing output were ever produced without practitioner review, both the Article 22 position and the DPIA would need to be revisited.

6. CONCLUSION

Item	Position
Article 6 basis	6(1)(b) contract for service delivery; 6(1)(a) consent for research and teaching
Article 9 condition	9(2)(a) explicit consent
Secondary, to confirm on advice	9(2)(h) health or social care, with the UK Schedule 1 condition 2 requirement noted
Automated decision-making	Article 22 not engaged — human practitioner in the loop
Action required	Consent wording drafted, capture mechanism built, withdrawal route live, evidence retained

Draft prepared for review by a qualified data protection solicitor. The choice of Article 9 condition is a legal determination and should be confirmed before it is relied upon.

How We Handle Your Information

Eclipse — a plain-language notice for clients

Richard Flook Limited · Version 1.0

A plain-language notice for clients

This notice explains what we do with the information you give us. It is written to be read, not to be hidden behind.

WHO WE ARE

Richard Flook Limited, 86 Shirehampton Road, Bristol BS9 2DR, United Kingdom. We are the people responsible for your information. You can reach us about anything in this notice at **frankie@richardflook.com**.

WHAT WE HOLD

- Your name and contact details
- Your date, time and place of birth
- What you tell us about your health and how you are feeling
- A written record of your sessions, and our notes
- Your Human Design chart
- The analysis and reports we produce for you

Some of what you tell us is health information. The law treats that as especially sensitive, so we handle it with particular care.

WHY WE HOLD IT

To deliver the service you have asked for: to run your sessions, to analyse your information against your chart, and to produce the reports you receive.

We also use the **mathematical and structural** results of our work — never your personal or health details, and never your name — to improve our method and to teach it. You can say no to that use at any time without affecting your sessions.

YOUR PERMISSION

Before we analyse your health information, we ask for your clear permission, separately and in plain terms. You can withdraw that permission at any time. If you do, we will stop the analysis and discuss what you would like to happen to what we already hold.

WHO ELSE SEES IT

We use a small number of specialist services to run Eclipse. They act on our instructions and are bound by contract.

Service	What it does	Where it runs
Mistral AI	Understands language and helps compose responses	European Union (France)
Gadium	Converts speech to text and text to speech	European Union (France)
Our hosting and email providers	Stores the service and sends our correspondence	To be confirmed

We do not sell your information. We do not use it to advertise to you. It is not given to anyone else except these services, or where the law requires it.

YOUR VOICE

We do not clone your voice. There is no feature for it, and we are not building one.

Eclipse speaks with one of the provider's own ready-made voices. Nothing you say is recorded, therefore no synthetic copy of your voice and no sample of your voice is kept anywhere.

HOW LONG WE KEEP IT

90 days after your last session, and then it is deleted. Backups are cleared ten days later. If you would like it gone sooner, ask us and we will delete it sooner.

Your billing records are kept longer, because the law requires it.

IF YOU ARE UNDER 18

The minimum age for Eclipse is 18. Where a young person is under that age, a parent or guardian holds access, and can see the information and ask for the account to be deleted.

YOUR RIGHTS

You can ask us to:

- show you what we hold about you
- correct anything wrong
- delete it
- stop processing it
- give you a copy in a portable format

Just write to **frankie@richardflook.com**. We will respond within 30 days. If you are unhappy with how we have handled your information, you can complain to the Information Commissioner's Office (ico.org.uk).

A HUMAN BEING IS ALWAYS IN THE PICTURE

Every report and every analysis we send you is reviewed and written up by a person — Richard — before it reaches you. Nothing is generated and delivered to you by machine alone. The analysis supports the work; it does not replace the practitioner.

WHAT MAKES THIS LAWFUL

Two things, in plain terms: we process your information because you have bought a service from us and we cannot deliver it otherwise, and for the sensitive parts we ask for your clear permission first.

Version 1.0 — 1 October 2026.

Richard Flook Limited · How We Handle Your Information · Confidential

Eclipse — Processing Chain and Data Flow

Internal architecture note

Richard Flook Limited · Internal

Internal architecture note supporting the Article 30 record and the DPIA

Version	1.0
Date	1 October 2026

1. WHY THIS DOCUMENT EXISTS

The Article 30 record names processors in a table. This note shows where each one sits in the chain and what passes through it, so that the record can be checked against reality rather than against intention. Every processor in the chain is a point where client data leaves our control, and each one needs its own assessment.

2. THE CHAIN, STEP BY STEP

Step	What happens	Who touches client data	Data leaving our infrastructure
1	The client speaks with Eclipse	Our application	No
2	Speech is transcribed to text	Gadium (transcription)	Yes — audio, if transcription is cloud-side
3	The transcript informs the response	Mistral AI, EU endpoint	Yes — transcript text
4	Session content is compiled against the chart	Our pipeline, our infrastructure	No
5	The evolutionary run produces a clearing circuit	Our pipeline; the mutation model	Yes — whatever is in the prompt
6	A practitioner reviews and authors the output	Richard	No
7	Documents are delivered	Our email provider	Yes — the finished document

3. THE THREE SPEAKING ROLES, KEPT SEPARATE

There are three distinct jobs in the voice path, and conflating them is how assessments go wrong:

Role	Job	Provider
Speech driver	The language model that decides what to say and composes the response	Mistral AI (EU endpoint)
Speech rendering	Turning text into audible voice	Gadium
Transcription	Turning the client's speech into text	Gadium (confirm)

Mistral is the driver behind Eclipse — the reasoning and the language. Gadium renders the voice. They are separate processors and each is assessed separately.

No client voice is cloned. Eclipse speaks with a catalogue voice, or with Richard's own cloned voice, which is covered by his own consent. No recording of a client is used to build a synthetic version of their voice, so voice biometric data is not processed on the client path and Gadium's voice-cloning consent obligations are not engaged.

If that ever changes, the consent capture set out in the Gadium checklist (section 3) becomes mandatory **before** any upload — because Gadium requires consent contractually without enforcing it technically, which places the obligation squarely on us.

4. THE OPENEVOLVE PROMPT — THE POINT THAT NEEDS THE MOST CARE

The mutation call in an OpenEvolve run receives a **prompt**. Whatever is in that prompt reaches the model provider. If a prompt contains a client's chart, their locked octons, or their clinical narrative, then that material is being processed by the provider, and the provider's DPA and residency govern it.

Two things follow:

1. **The provider of the mutation lane is a processor** for that client's data, and must be named in the Article 30 record like any other.
2. **Data minimisation applies** (Article 5(1)(c)). Send what the run needs and no more. A run does not need a client's name; it needs the structural inputs. Those are different things, and the difference should be visible in the code.

Action. Enumerate every model endpoint the pipeline can reach — including any fallback lane — and list each one in the Article 30 record. A fallback lane that nobody wrote down is still a processor.

5. WHERE CLIENT DATA MUST NOT GO

- **Any development or experiment lane.** DeepSeek, Gemini, Claude, free-tier providers — none of them receives client data. The rule is about the lane, not the provider name.
- **The Gradium default endpoint** (`api.gradium.ai`) for client audio. It is not EU-pinned and can route to a US cluster. Client audio uses `eu.api.gradium.ai` once residency is enrolled — or the on-device / in-VPC option, which removes the cloud processor from the path.
- **Any endpoint without a confirmed region.**
- **Any gateway that forwards to a provider we have not assessed** — including a gateway used for convenience on a lane that was thought to be internal.
- **Any provider with a training opt-out that is unset.**

6. OPEN ITEMS BEFORE CLIENT DATA FLOWS

#	Item	Owner	State
1	Mistral DPA accepted and archived		Open
2	Mistral training opt-out set on both surfaces and evidenced		Done 1 Oct 2026 — screenshots filed
3	Mistral EU endpoint confirmed in config		Open — config to write
4	Gradium Zero Data Retention in force (data retention disabled in Studio); EU residency requested in implicit mode; pinned to <code>eu.api.gradium.ai</code> with pinned; <code>zone=eu</code> asserted in code; ToS Exhibit 1 DPA filed		ZDR done · residency request drafted · DPA obtainable now
5	Gradium on-device (Phonon) or in-VPC (SageMaker) option evaluated for the audio path		Open
6	Hosting and email provider residency confirmed		Open
7	Every OpenEvolve lane, including fallbacks, enumerated		Open
8	Development-lane separation documented: experiments use various LLMs (DeepSeek, Gemini, Claude, free tiers), none carrying client data		Open — position stated by controller
9	Explicit consent capture built and the withdrawal route live		Open
10	Deletion job verified to run at 90 days		Open
11	Gradium subprocessor Clerk (US) assessed — identity data, not session audio; confirm scope or an alternative		Open — transfer to record
12	Establishment decided and evidenced. The Ltd is UK-incorporated and currently non-trading , so the question is dormant until processing begins . Decide before the first client's data is processed, and build UK		Open — dormant; decide before the first client

#	Item	Owner	State
	operating substance (hosting, banking, contracts, actual trading, decisions documented) if UK operation is the intention		
13	Independent Article 27 representative appointed. Follows automatically from UK operation, because Article 27 exists for controllers outside the Union serving EU data subjects. Do not self-appoint		Open — required before the first EU client
14	Lead supervisory authority confirmed — ICO if UK-operated, CNIL if EU-established — and the privacy notice updated to match		Contingent on item 12

7. THE PRINCIPLE

Regional compliance is a property of **every step**, not of the chain as a whole. One unassessed processor anywhere in the path makes the whole path unassessed. The list above is short, and each line is an afternoon's work — but an item left open is an item a regulator will find.

Internal working document. Reviewed alongside the Article 30 record and the DPIA.

Richard Flook Limited · Eclipse — Processing Chain and Data Flow · Confidential

Processor Onboarding Checklist — Gadium (Voice)

Article 28 processor requirements

Richard Flook Limited · Internal · Operational

Applies to: all client audio, transcripts and voice data processed through Eclipse.

Provider	Gadium SAS, 151bis rue Saint-Honoré, 75001 Paris, France
Role	Processor (Article 28)
Controller	Richard Flook Limited (12542030)
Certification	ISO 27001:2022, independently audited by A-LIGN
Trust Center	https://trust.gadium.ai/
Document version	1.1
Date	1 October 2026

WHAT WAS ESTABLISHED BY CHECKING THE VENDOR DOCUMENTATION

1. **Gadium does not train models on our data.** Their data-use documentation states plainly: "We do not use feedback submitted through this form to train models." And where data retention is disabled, "nothing is collected through this feedback form." A materially better starting position than a provider that trains by default.
2. **Zero Data Retention is self-serve.** A toggle in Studio. Self-serve on paid plans since 2 September 2026.
3. **EU data residency is not self-serve.** It requires the Gadium team to enable it on the plan. The account currently reads "**Data residency: Not enforced.**"
4. **Compliance is verifiable, not just asserted.** Every response reports the residency that actually served it. We can assert it in code.
5. **Voice consent is a contractual obligation on us, not a platform gate on the voice owner.** See section 3. This one matters and does not work the way it is usually assumed to.

1. GATE — DO NOT PUBLISH THE CLIENT NOTICE UNTIL RESIDENCY CLOSES

The client privacy notice (05-client-privacy-notice.md) tells clients that Gadium processes in the **European Union (France)**. That is accurate for the control plane today, and for session inference **only once EU residency is enrolled**. The account currently shows residency **not enforced**, so session audio can still be processed in the US.

Publish the notice only after a response shows pinned; zone=eu.

2. ZERO DATA RETENTION — IN FORCE (CONFIRMED 1 OCTOBER 2026)

Gadium's FAQ gives the operative instruction, and it is the inverse of what the panel heading suggests: "To enable it, sign in to Gadium Studio, open the Profile dropdown in the top right, and select My organization. Under Privacy Settings, disable data retention. Once turned off, Gadium will no longer retain your request or response payloads."

The control is a data-retention toggle, and the compliant state is OFF. Retention on = payloads held for 90 days. Retention off = nothing retained.

- [x] **Data retention disabled** under **Privacy Settings** → Zero Data Retention is in force
- [] Screenshot the toggle in its off state and file it in legal/evidence/

Correction to the earlier reading of this pack. The supplied screenshot was first read here as "retention still active", on the basis of the section heading Zero data retention and the line Data retained for 90 days. That was wrong. The heading names the feature; the 90 days line describes the retained-on behaviour that the toggle exists to switch off. **The toggle is off, which is exactly what we want. The account is already compliant on this point.**

How to read this panel in future. Gradium's own wording — "disable data retention" — is the authority, so the compliant state is the toggle **off**, never on. If a panel is ever labelled Zero data retention rather than Data retention, read the resulting status line rather than the heading. A heading being present is not a setting being set.

What ZDR covers: the request and response payloads of speech sessions — the text and audio sent to TTS, STT and S2S, and the audio and transcripts returned. That is the client session content, which is the part that matters.

What ZDR does not cover: inputs to the voice creation tools — Voice Design written prompts, and the audio sample uploaded to create a custom voice (Instant or Pro clone). Extending ZDR to those requires an **Enterprise plan** and a custom privacy policy.

3. VOICE SAMPLING AND CONSENT — THE POSITION, AS IT ACTUALLY IS

Checked against Gradium's Terms of Service, FAQ, developer documentation and their own published guidance on cloning. The finding matters because the mechanism is not the one usually assumed.

What Gradium says

- FAQ, on Instant Voice Clone: "Please note that explicit consent from the voice owner is required."
- Their cloning guidance: "No voice should be cloned without explicit, informed consent from the person it belongs to, whether the audio comes from a recording session, a user upload, or any other source, and public availability (a podcast, a broadcast) is not consent. Gradium's terms require consent from the voice owner."
- Same guidance, on enforcement: "Responsible voice cloning APIs enforce consent requirements contractually and, where feasible, technically."
- Terms of Service prohibit using the Services "to impersonate another person or business without their explicit authorization."
- Voice cloning is described as processing **biometric data**, whichever jurisdiction applies (GDPR, CCPA, Illinois BIPA).

What Gradium does not do

There is no gate that makes the voice owner log in and agree.

- Our **clients are not Gradium users**. We hold the Gradium account; they never see it.
- The consent obligation is **contractual and sits on us**. Gradium's Terms place it under Client's Obligations: "Ensuring every Input submitted through the Services complies with Applicable Laws." And: "Client shall be responsible to prevent unauthorized access to or use of the Services."
- The voice-creation API takes an audio file and a name. There is **no consent attestation field, no owner-verification step, and no consent gate in the documented flow**. A sample can be uploaded by whoever holds the API key.
- So Gradium **cannot** stop a voice being sampled. The control is ours, not theirs.

What that means for us

We capture and file the consent ourselves. It is not something Gradium does for us, and it is not something we can point at Gradium for. If a client's voice were cloned without our own documented consent, Gradium's clause would be pointing back at us.

If a client voice is ever cloned, before upload:

- [] Explicit, specific, informed consent from the voice owner, recorded separately from the general terms
- [] Naming the purpose and the retention position
- [] A documented record kept on file, dated
- [] A withdrawal route stated and actioned

The cleaner route — avoid the question entirely

Gradium offer a way to sidestep it. From their own guidance, Voice Design "produces a voice from a text prompt... It sidesteps the consent and biometric-data questions, since no real person's voice is processed."

Eclipse does not need a client's voice in any case: the session voice is a **catalogue voice**, or Richard's own **cloned voice**, which is covered by his own consent. Proceeding on that basis means **no client voice is ever sampled and the biometric-consent question never arises**.

Recommendation: keep Eclipse on a catalogue or designed voice. Treat client voice cloning as a separate feature requiring its own consent instrument, its own DPIA entry, and — because standard ZDR does not cover voice samples — an Enterprise arrangement.

4. EU DATA RESIDENCY — WHAT IT IS, AND WHY IT NEEDS A REQUEST

What "data residency" means here

It is **not** your residency, and **not** the company's registered address. It is one thing only: **which country's servers physically process the audio.**

Gadium runs clusters in both the **European Union** and the **United States**. Every request goes to one endpoint, `api.gadium.ai`, and is routed to the nearest cluster.

- **By default there is no guarantee.** Gadium's own FAQ says that for customers in the EU, traffic "is routed to our EU cluster... your requests are processed there and your data stays in Europe" — but their data-residency documentation is explicit that the default endpoint carries "**no residency commitment.**" In practice it lands in the EU. In guarantee, it does not.
- **Enrolled EU residency is a contractual guarantee**, enforced per request, with no cross-region fallback, and a fail-closed rejection if a request is ever misrouted.

Why an email, and not a switch

Because there is no switch. Gadium's documentation: "Data residency is available on our paid plans. It is enabled on your plan by our team; there is no self-serve toggle yet." And their launch note says it "is enforced for our customers who request it."

Requesting it is the only route. There is nothing in the console to click.

Why it matters for us

A UK or EU client's health audio processed on a US server is a restricted international transfer, which carries extra legal machinery. With EU residency enrolled, **there is no transfer to analyse** — and the response header lets us prove it rather than assert it.

Actions

- [] Email `support@gadium.ai` asking for **EU data residency** in **Implicit** mode (whole organisation pinned, whichever endpoint is called). Draft at `08-gadium-residency-request.eml.md`.
- [] On confirmation, pin the integration to `eu.api.gadium.ai` (`wss://eu.api.gadium.ai/api` for WebSocket)
- [] Confirm the residency entitlement applies to the M plan while it is credit-funded — see the plan position below

Plan position — M tier, currently credit-funded

Corrected 1 October 2026. An earlier draft of this pack assumed the free tier. The account is on the **M plan** — the \$340/month tier — currently not being paid for, with a few months remaining on credits.

That changes the answer on both counts:

Requirement	Free	M — ours
Commercial use	No	Yes
Residency eligibility	Paid plans only	Yes — M is a paid plan
Instant voice clones	5	1,000 / month
Included credits	45k	9M

So **no upgrade is needed and there is no breach to worry about.** Commercial use is permitted and residency is available on request. The earlier "move to XS at \$13/mo" note in this pack was wrong and is withdrawn.

The one genuine question is entitlement versus payment. Gadium's documentation ties residency to "paid plans." Ours is a paid **tier** that is not currently being paid **for**. Whether the entitlement follows the tier or the billing state is the thing to confirm in the email — it is the difference between "enabled this week" and "the billing conversation comes first."

After the credits — what tier do we actually need?

Worth settling before the months run out, because **M at list is \$340/month** and Eclipse's top tier is \$100.

Text-to-Speech bills at 1 credit per character, and roughly 45,000 characters is an hour of speech:

- **M** — 9M credits ≈ **200 hours** a month
- **S** (\$43/mo) — 900k credits ≈ **20 hours**
- **XS** (\$13/mo) — 225k credits ≈ **5 hours**

One Eclipse session is perhaps 25–45 minutes of speech. Even a busy early month is unlikely to need more than **S**. **M is far more capacity than the early client base will consume**, so when the credits end the realistic choice is S or XS — not M. Decide on the numbers rather than defaulting to the tier we happen to be sitting on.

Subprocessors — the full list, and the one that sits outside the EU

From the Gadium Trust Center (<https://trust.gadium.ai/subprocessors>):

Subprocessor	Role	Location	EEA?
Scaleway	Cloud infrastructure	8 rue de la Ville-l'Évêque, 75008 Paris, France	✔ Yes
Amazon Web Services	Cloud infrastructure	38 avenue John F. Kennedy, L-1855 Luxembourg	✔ Yes (AWS EMEA)
Clerk	Identity provider	660 King Street, Unit 345, San Francisco, California, United States	⚠ No — United States

The Clerk flag. Clerk is a **US** subprocessor and it is not covered by EU inference residency. It handles **identity and authentication**, not session audio — so the client's voice and transcript stay in the EU under enrolment, but account and login data touch the United States. That is a transfer to record and, if required, to justify. Ask Gadium whether Clerk's processing can be scoped or whether identity can be handled without it.

Note: under **either** residency the control plane is EU-hosted for all customers, so account data, custom voices and pronunciation dictionaries sit in the EU regardless. Only session inference moves under US residency.

5. VERIFY THE GUARANTEE IN CODE — THE CONTROL THAT BITES

Gadium reports the residency each request **actually received**:

- **REST:** read the x-gadium-residency response header
- **WebSocket:** read the residency field of the ready message

Value	Meaning	Our action
pinned; zone=eu	Guarantee in force — EU, will not leave	Pass
best-effort; zone=eu	Landed in the EU but not enrolled — no commitment	Fail — treat as a configuration error
none	No region involved, not enrolled	Fail
pinned; zone=us	Pinned to the US	Fail — wrong region

- [] Add an assertion in the Eclipse voice client: anything other than pinned; zone=eu is a hard error, not a warning.

This turns "Gadium is compliant" from a belief into a check. Their own doc says it: "If you rely on the guarantee, assert pinned in your client and treat anything else as a configuration error."

6. DATA PROCESSING AGREEMENT — OBTAINED AND FILED

Status: acquired 1 October 2026. The **standalone DPA** is filed at evidence/gadium-data-processing-agreement-v2026-07-22.pdf — 10 pages, an authenticated Gadium Trust Center download obtained after signing the NDA. The **Terms of Service** it forms part of is filed alongside at evidence/gadium-terms-of-service-v2026-07-22.pdf (24 pages).

An earlier copy of the ToS — the public web render — has been removed after verification that it was the same document (identical title, page count and text, differing only by the Trust Center watermark). The authenticated download is the better artefact and replaces it. See evidence/INDEX.md.

The DPA is incorporated into the Terms of Service as Exhibit 1, and the Terms state: "The Agreement shall be considered signed and accepted by the Client by the subscription and/or use of the Services." It was already in force; we now hold the operative text rather than a claim that it exists.

Trust Center request also submitted (1 October 2026) for the DPA and the ISO 27001:2022 Certificate and Report.

Three clauses that matter, read from the filed DPA

1. The DPA says it is not designed for sensitive data — and ours is.

Appendix 1, Section 8 — Sensitive Data: "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."

Client session content is health data — special category. So we are processing special category data through a processor whose own DPA states the processing is **not designed for it**, and places the responsibility on our instructions.

That does not make it unlawful. It does mean **the safeguard is ours, not theirs** — and it belongs in the DPIA as a named risk. It also raises the value of the on-device (Phonon) route, which takes session audio out of the processor's scope entirely.

2. We currently authorise international transfers by default.

Section 6 — International Transfer of Client Personal Data: "Unless GRADIUM otherwise explicitly commits not to transfer any Client Personal Data to a Non-EEA Country, Client authorizes GRADIUM to transfer Client Personal Data directly or indirectly to any country deemed to have an adequate level of data protection..."

By default the DPA hands Gradium a blanket authorisation to transfer. **The "explicit commitment not to transfer" is precisely what the EU residency request obtains** — so that email is also the instrument that narrows this clause. Another reason to send it.

3. A right worth exercising — 30 days' notice of new subprocessors.

Section 5 — Use of Sub-Processors: "GRADIUM shall update the list of any Sub-Processor to be appointed at least thirty (30) days prior to the date on which the Sub-Processor shall commence the Processing of Client Personal Data."

That is a genuine notice right. **Subscribe to Trust Center subprocessor notifications** so a new subprocessor — possibly in a new country — arrives with 30 days to object rather than after the fact.

Actions

- [x] **DPA obtained and filed** — evidence/gradium-data-processing-agreement-v2026-07-22.pdf (standalone, 10 pages, authenticated download)
- [x] **Terms of Service filed** — evidence/gradium-terms-of-service-v2026-07-22.pdf (24 pages; supersedes the earlier public-web copy, verified identical)
- [x] **Trust Center access requested** (1 Oct 2026) for the DPA and ISO 27001:2022 Certificate and Report
- [x] **Gradium NDA signed** by Richard Flook for Richard Flook Limited, 1 October 2026
- [x] **ISO 27001:2022 Certificate and Report — POSITION SETTLED (Route C)**. Accepted on the strength of Gradium's public certification statement — **ISO 27001:2022, independently audited by A-LIGN** — with the Trust Center access links recorded in evidence/INDEX.md so an auditor can go and view them. Rationale: the DPA is filed, the certification is vendor-published, and the certificate is corroborative rather than foundational. Nothing is blocked by its absence.
- The links are an **access route, not a public copy**: the Trust Center is a Vanta page and the files remain gated behind Gradium's NDA. Recorded that way deliberately.
- If a future client, insurer or regulator requires the certificate itself, **Request 3** of the residency email is the route — send it and they will email the PDF
- [] Retain the **NDA signature confirmation** with the evidence file
- [] **Subscribe to Trust Center subprocessor notifications** — the 30-day notice right is only useful if we are watching

- [] Note **Appendix 3 (Security Measures)** points to the Trust Center
- [] Ask support@gradium.ai about the **Clerk** transfer (see section 4): can identity processing be scoped, or handled without a US subprocessor?
- [] Raise the **Appendix 1 §8 sensitive-data clause** with Gradium — confirm what they expect of a controller processing special category data through them

7. EVIDENCE TO KEEP ON FILE

Evidence	Where it lives	Reviewed
Zero Data Retention screenshot (showing the setting text, not just the heading)	legal/evidence/	
Residency enrolment confirmation	legal/evidence/	
A sample response showing pinned; zone=eu	legal/evidence/	
Standalone DPA — authenticated Trust Center download	legal/evidence/gradium-data-processing-agreement-v2026-07-22.pdf	✓ 1 Oct 2026
Terms of Service — authenticated Trust Center download	legal/evidence/gradium-terms-of-service-v2026-07-22.pdf	✓ 1 Oct 2026
Gradium NDA — signature confirmation	legal/evidence/	Signed 1 Oct 2026, confirmation to file
ISO 27001:2022 Certificate and Report	legal/evidence/	⌚ Outstanding — view-only, request individually
Subprocessor list	legal/evidence/	Captured in §4
Any client voice-consent record, if that feature is ever used	legal/evidence/	
Evidence index	legal/evidence/INDEX.md	✓ maintained

8. ALTERNATIVES THAT REMOVE THE CLOUD PROCESSOR ENTIRELY

Worth keeping on the table, because for spoken clinical sessions these are the strongest position available:

- **Gradium Phonon** — on-device TTS SDK. Audio never leaves the device.
- **SageMaker image / private cloud** — inference inside our own VPC.

Either removes Gradium from the client-data path completely, which would simplify the Article 30 record rather than complicate it.

Draft prepared for review by a qualified data protection solicitor.

Email — Gradium Residency and DPA Request

Ready to send from richard@richardflook.com

Richard Flook Limited · Draft for sending

To: support@gradium.ai From: Richard Flook richard@richardflook.com Subject: Gradium — EU residency enrolment, DPA confirmation, ISO certificate, and a sensitive-data question

Hello,

I run Richard Flook Limited (UK, company 12542030), and we are building a voice service on Gradium for a UK/EU clinical client base. Our client audio is health data, so we need the EU residency position confirmed before we put live traffic through.

Four requests, please.

Request 1 — EU data residency

Our organisation ("Richard Flook Heal Better") is on the M plan. We would like EU data residency enabled in IMPLICIT mode, so that all of our traffic is pinned to the EU whichever endpoint is called. We will pin our integration to eu.api.gradium.ai and assert the x-gradium-residency / residency field on every request.

One point to confirm, please: your documentation states that data residency is available "on our paid plans". Our M plan is currently funded by credits rather than billed, so please confirm that the entitlement follows the plan tier and is available to us now. If it depends on the billing state instead, please say so and tell us what is required.

Request 2 — Data Processing Agreement

We understand your DPA is incorporated in your Terms of Service as Exhibit 1, and accepted by use of the Services. Please confirm that Exhibit 1 in the current Terms is the operative DPA for our subscription, and send your current subprocessor list together with confirmation of where the control plane and any subprocessors sit.

On the subprocessors: your published list shows three — Scaleway (Paris), AWS (Luxembourg) and Clerk (San Francisco). We would like to understand the scope of the Clerk processing, since it is the only one outside the EEA. Our clients are not Gradium users, so we assume Clerk handles account and authentication data for your platform rather than client session audio — please confirm that, and let us know whether identity processing can be scoped or handled without a US subprocessor.

Request 3 — ISO 27001:2022 Certificate and Report

We have signed your NDA and can see both items in the Trust Center, but they are view-only and cannot be downloaded, and the bulk download does not include them. Could you send the ISO 27001:2022 Certificate and the ISO 27001:2022 Report as email attachments, so we can hold them with our compliance records alongside the DPA?

Request 4 — Sensitive data clause in your DPA

Appendix 1, section 8 of your Data Processing Agreement states that "the Processing is not designed to include sensitive data or special categories of data within the meaning of Applicable Privacy Laws."

Our client session content is health data, and therefore special category data under GDPR. We are not asking you to change your position — we would simply like to understand it clearly before we put clinical traffic through, specifically:

- What does Gradium expect of a controller who is processing special category data through you?
- Are there additional safeguards, settings, or contractual terms Gradium offers for that case?
- Does this affect the residency or retention position we have asked about above?

Zero Data Retention

We have disabled data retention in Privacy Settings under My organization, which per your FAQ puts Zero Data Retention in force. Please confirm that it is showing as active for our organisation.

Two further questions

- Voice cloning: our understanding is that cloned voice data is treated as biometric data under GDPR and therefore special category, and your terms require explicit consent from the voice owner. We will not be cloning client voices under the standard policy, since Zero Data Retention does not extend to voice samples. Could you confirm the position, and let us know what an Enterprise arrangement covering voice samples would involve?

- On-device and self-hosted: we would also like details of the Phonon SDK and the deployable SageMaker image, since keeping audio inside our own boundary may be the better long-term architecture for us.

Thank you — happy to jump on a call if that is quicker.

Best regards,

Richard Flook Richard Flook Limited 86 Shirehampton Road, Bristol BS9 2DR, United Kingdom Company number 12542030 frankie@richardflook.com

Richard Flook Limited · Email — Gradium Residency and DPA Request · Confidential

Eclipse — Terms of Service and Privacy Policy

The terms you agree to, and how we look after your information

Eclipse · Version 1.0 · Draft for review

DRAFT — for Richard Flook to read, correct and sign off. Not published. Not shown to any client until he approves it.

Drafted 15 September 2026, first pass, from the product's own code and configuration. Folded the same day with Richard's answers to all 28 open items, in his own words where he gave them. **Updated 16 September 2026** from his review of the Help page: a self-serve cancel that stops the next payment, a refund REQUEST that is reviewed by us and refunds nothing, the plainer billing sentence (section 6), the live download/delete wording, and the freeze on "there is no cancel button". The health and AI wording below is taken verbatim from disclaimer_copy.py (version 2026-09-10). Every place where a real answer is still needed is marked — 5 of them, and each one is a choice or a fact only you can supply.

PART ONE — TERMS OF SERVICE

1. WHO WE ARE

Eclipse is created and run by **Richard Flook Limited**, a company registered in the United Kingdom.

- Address: 86 Shirehampton Road, Bristol BS9 2DR, United Kingdom
- Company number: 12542030
- Contact: WhatsApp **+33664895058**
- Email: **frankie@richardflook.com** — live and monitored (the mailbox reads client mail today).

In these terms, "we", "us" and "our" mean Richard Flook Limited. "Eclipse" means the AI companion app and the voice sessions it guides. "You" means the person using it.

2. WHAT ECLIPSE IS — AND WHAT IT IS NOT

Eclipse is an **AI companion** that guides spoken, closed-eye clearing and self-reflection sessions. You speak. Eclipse guides.

Eclipse is **not a doctor**. It cannot diagnose or treat any medical or mental health condition, and it is not a substitute for professional medical or psychological advice. Nothing in a session is medical advice.

This is the exact wording you see and tick:

I understand that Eclipse is an AI companion for emotional clearing and self-reflection. It is not a doctor, cannot diagnose or treat any medical or mental health condition, and is not a substitute for professional medical or psychological advice. Nothing in this session should be taken as medical advice. I understand that this kind of work can bring old feelings or memories to the surface, and that this is a normal part of the process. I agree to discuss any changes I make to my health, wellbeing, or treatment with my own doctor, and to speak to my doctor if anything becomes difficult. If I am in crisis or emergency, I will contact emergency services or my doctor directly — Eclipse is not an emergency service.

If you're in crisis or think you may be experiencing a medical or mental health emergency, contact your local emergency services or your doctor immediately — Eclipse is not an emergency service and cannot help with emergencies.

Eclipse may say things that are inaccurate or that do not suit your situation. You can ask Eclipse to back up what it tells you with research papers, and you can always ask Richard to review your work.

What a session may bring up

Releasing energy can change how you feel. That is the work — and it is usually a relief — but it is worth knowing what to expect.

In the hours and days after a session, you may notice:

- **emotions moving through you** that you had not expected;
- **old memories, or old feelings, coming back to the surface;**
- feeling **tired, wired, or unusually light;**
- **physical sensations** — tightness easing, or briefly feeling stronger before it does.

This is normal. It usually settles, and it is part of letting something go rather than holding it.

If it gets challenging, go and see your doctor. If you feel unwell, if your mood drops and stays down, if what comes up frightens you, or if it feels like more than you can carry on your own — talk to your doctor. Eclipse is not a substitute for medical care and it is not an emergency service.

You can also simply stop, take a break, and come back to it later. Nothing is lost by waiting.

3. THE SPOKEN DISCLAIMER, AND THE TICK

Before your first session, Eclipse **says** this out loud:

Hi, I'm your AI companion for this clearing session. I'm not a doctor — I can't diagnose or treat anything — but I can walk with you through what you're feeling, and if anything needs a professional, I'll say so. One thing worth knowing before we start: this kind of work can bring old stuff up, sometimes in the days after. If it gets challenging, go and see your doctor. That's not me being cautious — that's just how it works. Sound good?

Only after Eclipse has spoken does the tick-box appear. You tick it, and that tick is our record that you understood. We keep the date, the version of the wording you agreed to, and where you agreed to it. If a tick arrives without the spoken words having come first, our system refuses it.

If we ever change that wording, you will be asked to agree to the new version the next time you come in.

4. WHO MAY USE ECLIPSE

You must be 18 or over to hold an account of your own.

Eclipse Junior, and guardians. A parent or guardian may hold an account for someone below that age. That young person's space is called **Eclipse Junior**, and it sits inside the guardian's own account. The guardian is recorded on the young person's record with us. The guardian can switch into the Eclipse Junior space and see the young person's conversations and transcripts, and can delete the account. The young person does not need a separate login of their own. This is a real, working part of the service.

This is the sentence a guardian is asked to agree to, in Richard's own words:

You affirm that you hold parental authority over the Minor and expressly grant permission, authorization, and consent for the Minor to establish a Eclipse Junior account

You use Eclipse for yourself. Keep your access to yourself, and do not let anyone else use your space. If someone below the minimum age is using an adult's account, that is the adult's responsibility.

5. YOUR FREE SESSIONS

Your first **two sessions are free**. Nothing is charged and no card is needed.

We offer these two sessions once to a person. We recognise a returning person by **date of birth, time of birth and place of birth — never by email address**. If we think you may have had the free sessions already, Eclipse will not accuse you of anything. It will simply ask — in Richard's own words:

I am just curious, have you used Eclipse before? I am unsure if you already had your two free sessions because your information corresponds to someone with similar details as you. Do let me know?

— and take it from there.

6. PAID PLANS AND PRICES

Prices are in **US dollars**. Payment is taken by **Stripe**, our payment provider. We never see or store your card number.

Plan	Price	What you get
Entry	\$20 , one payment	2 sessions
Standard	\$50 per month	6 sessions and ongoing support
Premium	\$100 per month	12–15 sessions, including a Quantum Turn run and one standard Computational biology report
Top-up	\$10 , one payment	1 more session

Entry and Top-up are single payments. Standard and Premium are monthly subscriptions. A Top-up is for when your plan sessions run out, or for a Premium client who has gone past the 15-session quota for the month.

The amount we charge is the US dollar price. You may be shown, and be able to pay in, your own currency. When that happens the conversion is done by Stripe at their exchange rate, so the exact figure in your currency is Stripe's, not ours, and it can vary. Whatever you pay is the amount Stripe debits and the amount a refund returns to you. **You pay in your own currency. Stripe shows you the exact amount before you pay, and that is the amount taken — no tax is added on top, and nothing else is charged.**

Tax. No tax is added at the moment, and we will show you exactly what you pay before you pay. These are the prices Richard has confirmed for publication. **We will give you 30 days' notice by email before any price change takes effect** — see section 14.

7. RENEWALS

Standard and Premium renew automatically each month until you change or stop them, and Stripe charges the card you paid with. Entry and Top-up do not renew — they are one payment for the sessions described.

If you stop a subscription, you keep everything you paid for until the end of the month you have already paid for.

8. OUR GUARANTEE, AND HOW TO CLAIM IT

In Richard's own words:

If Eclipse does not do what you hoped, tell us. We will refund you — no quibbles.

How it works:

- **Subscriptions** — we refund from the day you ask, pro rata.
- **Reports** — refunded in full if the report missed the brief.
- **Either way**, Stripe returns to you the exact amount you paid, in the currency you paid it.

To claim it, **press “Ask for a refund” under Your Plan in the app and tell us why** — that is the quickest route, and it reaches us directly. You can also reply to any email from Eclipse, or write to **frankie@richardflook.com**. Nothing is refunded automatically: see below.

A refund is not automatic. Richard and Frankie handle refunds themselves, on request and with their approval, because they want to understand what went wrong. Most requests mean either that the service was not used, or that it did not deliver what was expected — and either way we would rather hear it and put it right than have you sit with it. The button in the app records your request and your reason and puts it in front of them; it does not move money by itself.

9. CHANGING OR STOPPING A PLAN

You can change or stop your plan yourself, from your account page.

- **To stop a monthly plan** — under Your Plan, press **Stop my plan**, choose the reason that fits from the list, and confirm. **This stops your next payment.** It does not cut you off: your access carries on to the end of the month you have already paid for (section 7), and nothing further is charged. The app tells you the date your

access ends, from Stripe's own record of your period. If you press it twice, nothing else happens — no second cancellation, no double charge.

- **To ask for a refund** — under Your Plan, press **Ask for a refund**, choose a reason, and add anything you want in your own words. Your request goes straight to Richard and Frankie to read. Nothing is refunded automatically — a person decides, and they come back to you (section 8).
- **To change plan, or move up or down a tier** — reply to any email from Eclipse, or write to **frankie@richardflook.com**, and Richard will action it for you.
- **If you would rather not use the buttons**, the email route in section 8 always works.

We keep the reason you give with your account record, so we can see why clients leave and put right what we can. It is part of your record, and it goes when your record goes (section 6 and section 13).

10. USING ECLIPSE FAIRLY

Please do not:

- use Eclipse to harm yourself or anyone else, or to plan harm;
- use it as an emergency service, or in place of a doctor;
- try to break, overload, copy or reverse-engineer the service;
- share your access with other people, or sign up as someone else;
- upload anything unlawful, or anyone else's private information without their permission;
- use the sessions to give medical advice to other people;
- record a session and publish it, or share someone else's session, without their permission.

We may suspend or close an account that is being used to hurt someone or to break these rules. If we do, we will tell you why, and the guarantee in section 8 still applies.

11. WHO OWNS WHAT

Eclipse — the app, the voice, the prompts, the wording, the reports, the frameworks and the method — belongs to Richard Flook Limited. Your sessions, your words, your transcripts, your uploads and your reports are yours; we hold them on your behalf to run the service for you, as the Privacy Policy explains.

You give us permission to hold and use your session material for the purposes in the Privacy Policy and no others: keeping continuity between your sessions, producing your reports, and — where you have agreed to it — Richard reviewing your work as your practitioner.

Research, teaching and product improvement. Some of what Eclipse holds may be used for research, teaching and product improvement — **only where it cannot be traced back to an individual, never a name, and never personal or trauma content.** Section 5 of the Privacy Policy sets out exactly what may and may not be used.

12. THE LIMITS OF OUR RESPONSIBILITY

In plain English:

- Eclipse helps you reflect and clear. It does not treat or cure anything, and it does not replace your doctor, your medication or your treatment.
 - We are not responsible for decisions you make about your health after a session. Talk to your doctor before you change anything.
 - We do not promise that a session will work, or that Eclipse will always be available, accurate or free of interruption.
 - If something goes wrong on our side, our responsibility to you is limited to **the amount you have paid us in the last twelve months.**
 - Nothing in these terms removes rights you have as a consumer by law, or our responsibility for death or personal injury caused by our negligence, or for fraud.
-

13. WHICH LAW APPLIES

These terms are governed by the law of **England and Wales**, and any dispute is heard by the courts of **England and Wales**.

14. HOW THESE TERMS CAN CHANGE

We may update these terms as Eclipse changes. When we do, we will tell you by email, and the new version will apply from the date we say. If you keep using Eclipse after that date, you accept the new terms. If you do not accept them, tell us and we will stop your plan.

We will give you 30 days' notice by email before any change to these terms or to our prices takes effect.

PART TWO — PRIVACY POLICY

15/09/2026 · Version 2.0

1. THE SHORT VERSION

We collect what we need to run your Eclipse sessions, keep your continuity, make your reports and take your payment. We do not sell your information and we do not use it to advertise to you. Your session material is kept for **90 days after your last visit**, then deleted, and we email you before that happens. You can ask for a copy of everything, or ask us to delete it sooner, at any time. Eclipse is not a medical record.

2. WHAT WE COLLECT

- **Your account and contact details** — your name, your email address, and how to reach you.
- **Your birth details** — your date of birth, your time of birth (or a note that the time is not known) and your place of birth. These are used for your chart and for recognising you when you return.
- **Your sessions** — the transcript of what you said and what Eclipse said, so you can come back and carry on where you left off.
- **What you upload** — tongue photos, body photos, diagnostic letters, medical images and other documents you choose to send us. We can read text off letters and documents to help you.
- **Your notes, plans and reports** — daily practice, session notes, and any report we produce for you.
- **Payment records** — what you bought, when, and what you paid. **Card numbers are held by Stripe, never by us.**
- **Basic technical records** — that a session started and ended, and which parts of Eclipse you used, so we can keep the service working and spot abuse.

We do not ask for anything we do not need, and you are always free to leave out anything we have not asked for.

3. WHY WE HOLD IT

- To run your session and let Eclipse guide you.
 - To keep continuity, so you never have to start from the beginning again.
 - To produce your reports and your daily practice.
 - To take payment and to refund you when you ask.
 - To keep the service safe — stopping abuse, keeping the servers up, and keeping your account yours.
 - To email you about your own account and your own sessions.
-

4. THE LAWFUL BASES, IN PLAIN ENGLISH

- **Contract** — we hold what we need to deliver what you have paid for or signed up for: your account, your sessions, your reports, your payment records.
 - **Consent** — for the health-adjacent material: your birth details, the things you say about your body and your health in a session, the images and letters you upload, and the tick you give after hearing the spoken disclaimer. You can withdraw that consent at any time by asking us to delete — see section 7.
 - **Legitimate interest** — for keeping the service secure and working: rate limits, abuse prevention, and technical logs.
-

5. WHERE YOUR INFORMATION LIVES, AND WHO ELSE TOUCHES IT

Your information is held on our own server, and your uploaded files are held with it, kept under your client record with us. The companies below process it so that Eclipse can work:

Who	What they do
Stripe	Takes payments and manages subscriptions. They hold your card and payment details; we never see them.
Gadium	The voice. Turns your speech into text and Eclipse's reply into speech.
DeepSeek	The language model that writes Eclipse's words. What is said in a session is sent to it so Eclipse can answer.
Oracle Cloud Infrastructure	The server Eclipse runs on.
Google Drive	Our nightly backup. A copy of the client database — the records that hold your account and your sessions — is copied to Google Drive each night, so that we can restore everything if the server is lost.
Our email host	The company's mail host sends Eclipse's emails. Eclipse is the name you see on them, and a reply to them comes to frankie@richardflook.com .

We share your information with no one else, unless the law requires it, or unless it is necessary to protect someone from serious harm.

Research, teaching and product improvement

- **The mathematics may be used to develop Eclipse.** The Harmonic Fractal Mapper mathematics, the Quantum Mathematics and our other mathematical programmes are tools, not your information. They may be worked on and developed the same as any database is analysed for trends and anomalies.
- **Never a name, and never personal or trauma content.** Nothing that carries a name, and no personal content and no trauma content, is used for research, teaching or product improvement.
- **Embryonic-organ information, general disease issues, and the mathematics that drives Eclipse** may be used for research, teaching and product improvement **only where it cannot be traced back to an individual.**

6. HOW LONG WE KEEP IT

This is Richard's own client-facing wording, and it is the rule:

Your sessions, transcripts and notes are kept for 90 days after your last visit, so you can come back and carry on where you left off. We will email you before we delete anything, and you can download everything or ask us to delete it sooner, whenever you like.

We act on that with a reminder ladder by email:

- **Day 30 after your last visit** — a plain note that everything is safe and still here.
- **Days 80, 85 and 89** — three warnings that your material will be deleted, each with a link to download everything, and a link to delete it now instead.

Download everything, or delete everything. The account page gives you two choices: **Download everything** — one file with everything we hold about you, for your own records — or **Delete everything**. Deleting asks you first — **“Are you sure you want to delete everything?”** — and then confirms with a code sent to your email before it happens: a code will be sent to you, and nothing is deleted until you type it in. That way no one can end your account by accident and no one else can end it for you. Both buttons are live: you can do either yourself, at any time. If you would rather have us do it, reply to any email from Eclipse and we will send you everything, or delete everything, by hand.

Backups after you delete. If a copy of your record is still in a backup when you delete your account, it is kept a further ten days, just in case, and then it goes — once someone deletes an account we have no right to store their information any longer.

7. YOUR RIGHTS, AND HOW TO USE THEM

You can:

- **See and download everything we hold about you.**
- **Ask us to correct anything that is wrong.**
- **Ask us to delete everything** — your sessions, transcripts, notes, uploads and reports.
- **Withdraw your consent** to the health-adjacent material, by asking us to delete it.
- **Ask us to stop emailing you** about anything other than your own account.

How to ask today: reply to any email from Eclipse, or message us on WhatsApp at +33664895058, and say what you want. Richard actions it personally. We will confirm to you when it is done. **We answer a data request within 30 days.**

On the account page you can do both yourself — download everything we hold about you, and delete everything. Deleting asks you first — “Are you sure you want to delete everything?” — and confirms with a code sent to your email before it happens: a code will be sent to you, and nothing is deleted until you type it in. That way no one else can end your account. Both buttons are live; the routes above always work too.

Privacy requests go to **frankie@richardflook.com** (live and monitored), or the WhatsApp number.

8. SECURITY, IN PLAIN TERMS

- Your information sits on our own server, not in a public place.
- Your uploaded files are held separately from the app itself, under your client record.
- Your card details never reach us — Stripe holds them.
- Access to your space is tied to your own login, and a guardian's access is tied to the guardian recorded on your record.
- Session tokens are single-use and short-lived, so a link cannot be reused by someone else.
- We keep technical records of session activity so we can spot abuse.

No system is perfect. If anything ever goes wrong, we will tell you.

If you ever need to report a security problem, write to **frankie@richardflook.com**.

9. MINORS AND GUARDIANS

Where a young person uses Eclipse, their parent or guardian is recorded on their record and holds access to that young person's space, including their transcripts. The young person does not need a separate login. A young person's information is held under the same 90-day rule as anyone else's.

The minimum age is 18. Below that, the only way in is an Eclipse Junior account held by a parent or guardian. The free sessions for a young person are offered through their guardian, inside the guardian's own account. The wording a guardian agrees to is in section 4 of the Terms of Service, and the guardian can see everything in the young person's space and can delete the account.

10. HOW TO COMPLAIN

If you are unhappy with how we have handled your information, tell us first — reply to any email from Eclipse or message **+33664895058** and we will put it right.

You can also complain to the **UK Information Commissioner's Office (ICO)**, the authority that supervises data protection in the United Kingdom. You can go to them at any time; we would only ask that you let us try to put it right first.

11. WHAT ECLIPSE IS NOT

Eclipse is not a medical record, and it is not your doctor's file. It holds your words, your sessions and what you have chosen to send us, so that we can work with you. It is not a clinical record of care, it is not shared with your doctor, and it does not replace anything your doctor holds.

Some of what we hold is sensitive by nature: your birth date, time and place; what you say about your body, your feelings and your health; and the photos, letters and medical images you upload. We treat it that way, we use it

only for the purposes in section 3, and we delete it on the 90-day rule in section 6 unless you ask us to delete it sooner.

12. CHANGES TO THIS POLICY

If this policy changes, we will email you and say what changed and when it takes effect. The current version is always the one in the app.

This version: 15/09/2026 · Version 2.0.

End of draft. What is still marked is the short list of choices and facts still open; everything else is your own answer from 15 September 2026, written into the text.

Eclipse · Terms of Service and Privacy Policy

Evidence Index — Eclipse Data Protection Pack

Document register: what is held, from where, and what it evidences

Richard Flook Limited · Maintained alongside the Gadium checklist

Controller: Richard Flook Limited (12542030), 86 Shirehampton Road, Bristol BS9 2DR, United Kingdom

This folder holds the primary documents the Article 30 record and the DPIA rely on. An unindexed folder is not evidence, so everything held here is listed with its source and date.

HELD

#	Document	File	Pages	Source	Obtained	Evidences
1	Data Processing Agreement (standalone)	gradium-data-processing-agreement-v2026-07-22.pdf	10	Gradium Trust Center, authenticated download (after NDA signature)	1 Oct 2026	Article 28 processor terms — see clause notes below
2	Terms of Service	gradium-terms-of-service-v2026-07-22.pdf	24	Gradium Trust Center, authenticated download	1 Oct 2026	The agreement incorporating the DPA as Exhibit 1; also the contractual basis for the consent requirement
3	Note to File — Mistral account holder	mistral-account-holder-note-2026-10-01.md	1	Prepared by us	1 Oct 2026	Records that the Mistral account is operated by a director on behalf of Richard Flook Limited as Controller. The Organisation is named Richard Flook Limited and the DPA is accepted at that level; the note covers the remaining personal-login and payment-method point. Awaiting signature by the director.
4	Screenshot — Mistral API → Privacy: both toggles OFF	mistral-api-privacy-both-toggles-off-2026-10-01.png	—	Captured from the live console	1 Oct 2026	The primary evidence for the training position. Shows "Allow the use of your API calls to train Mistral's AI models" OFF and "Enable Labs models" OFF
5	Screenshot — PAYG		—		1 Oct 2026	The second training surface,

#	Document	File	Pages	Source	Obtained	Evidences
	subscription: training checkbox unchecked	mistral-payg-subscription-training-checkbox-unchecked-2026-10-01.png		Captured from the live console		clear at subscription time
6	Screenshot — PAYG enabled confirmation email	mistral-payg-enabled-confirmation-2026-10-01.png	—	Received from Mistral	1 Oct 2026	Confirms PAYG enabled for the organisation; also the source of Mistral AI's registered identity
7	Screenshot — Mistral billing page, Bristol address	mistral-billing-bristol-address-2026-10-01.png	—	Captured from the live console	1 Oct 2026	Billing entity Richard Flook Limited , registered office address; card on file as Default

Both files carry a Gadium Trust Center download watermark. The watermark obscures text extraction slightly but is the mark of an authenticated download — i.e. provenance we can point to, rather than a page copied from the public web.

Note on the superseded copy. An earlier copy of the Terms of Service (the public web render) was filed as gradium-terms-of-service-exhibit1-2026-07.pdf and has been removed. It was verified to be **the same document** — identical title (Terms of Service_Gradium_2026.07.22.docx), identical page count (24), identical text apart from the watermark. The authenticated download replaces it.

KEY CLAUSES RELIED UPON

Clause	Document	Effect
Exhibit 1 / standalone DPA	Both	The DPA — Gadium is Processor, Richard Flook Limited is Controller
Appendix 1 §8 — Sensitive Data	Both	"The Processing is not designed to include sensitive data or special categories of data..." — recorded as DPIA risk R10
§5 — Use of Sub-Processors	Both	General authorisation, but 30 days' notice before a new subprocessor begins processing
§6 — International Transfer	Both	We authorise transfers by default unless Gadium "explicitly commits not to transfer" — the EU residency request is the instrument that narrows this
Appendix 2 — Subprocessors	Both	Scaleway (Paris, EEA) · AWS (Luxembourg, EEA) · Clerk (San Francisco, US)
Appendix 3 — Security Measures	Both	Points to the Trust Center
ToS §28 — Signature	ToS	"The Agreement shall be considered signed and accepted by the Client by the subscription and/or use of the Services."

OUTSTANDING — ACCEPTED POSITION

#	Document	Position	Access route
3	ISO 27001:2022 Certificate	Accepted on the public certification statement. View-only in the Trust Center and confirmed not downloadable — tested; the shareable links do not bypass the gate. Not treated as a blocker, because the DPA is filed	https://trust.gradium.ai/resources?s=ayc6p1rqratf40qr8qnv2&name=iso-27001-:-2022-certificate

#	Document	Position	Access route
		and the certification is vendor-published	
4	ISO 27001:2022 Report	Same	https://trust.gradium.ai/resources?s=131o88jnxv7fcpiwnyxu8&name=iso-27001-:-2022-report
5	Gradium NDA (signed copy)	Signed by Richard Flook, 1 Oct 2026. Retain the confirmation email	—

Read the access route precisely. These links are recorded so an auditor, solicitor or successor can **go and view** the certification. They are **not** public copies. The Trust Center is a Vanta page and the resources remain gated: reaching the files requires signing Gradium's non-disclosure agreement. Anyone relying on these links should expect to sign the NDA first.

The public statement of certification — **ISO 27001:2022, independently audited by A-LIGN** — is made by Gradium at <https://trust.gradium.ai/> and requires no access at all.

Trust Center — general

Resource	URL
Trust Center home	https://trust.gradium.ai/
Resources (DPA, ToS, ISO items)	https://trust.gradium.ai/resources
Subprocessor list	https://trust.gradium.ai/subprocessors
Controls	https://trust.gradium.ai/controls

ALSO ON RECORD (NOT FILED HERE)

- **Gradium subprocessor list** — captured from <https://trust.gradium.ai/subprocessors>, reproduced in the Gradium checklist §4
- **Gradium Trust Center controls** — 5 control groups listed (Infrastructure, Organizational, Product, Internal procedures, Data and privacy), including "Data retention procedures established" and "Customer data deleted upon leaving"
- **Zero Data Retention** — in force; data retention disabled in Studio under My organization → Privacy Settings
- **Gradium residency position** — account currently reads "Data residency: Not enforced"; enrolment requested

Maintained alongside 07-gradium-onboarding-checklist.md. Update this index whenever a document is added or superseded.

Note to File — Mistral AI Account Holder

Basis on which the Mistral AI account is held

Richard Flook Limited · Awaiting director signature

Date: 1 October 2026 **Controller:** Richard Flook Limited, company 12542030, 86 Shirehampton Road, Bristol BS9 2DR, United Kingdom **Subject:** Basis on which the Mistral AI account is held

THE POSITION

The Mistral AI account used to process personal data on behalf of Richard Flook Limited is administered by **Richard Flook**, a director of the company.

The Organisation is named Richard Flook Limited. In Mistral's model the Organisation is the top-level entity: billing, membership and every workspace sit beneath it, and Mistral's Data Processing Addendum is accepted at that level. The entity presenting to Mistral as the customer is therefore the company.

What remains personal is narrower: the **account login** and the **payment method** are held in Richard Flook's own name.

WHY THIS NOTE EXISTS

Article 28 requires processing of personal data by a processor to be governed by a contract between the controller and the processor. The Organisation names the company and the DPA is accepted at Organisation level, so the contracting chain now matches the data flow at the level that matters.

Two details remain personal to a director. This note records, on the date stated, that the account is **operated by Richard Flook in his capacity as a director and on behalf of Richard Flook Limited, which is the Controller for all personal data processed through it** — so the position is documented rather than inferred.

WHAT IS RELIED UPON

1. **The Organisation is named Richard Flook Limited** — the company is the entity presented to Mistral.
2. **The DPA is accepted at Organisation level**, binding Mistral as Processor to the Organisation.
3. **The account is used exclusively for the company's business.** No personal or unrelated use is made of it.
4. **Richard Flook is a director of the company**, and operates the account in that capacity.
5. **The company's Record of Processing** (01-record-of-processing-activities.md) names Richard Flook Limited as Controller and Mistral AI as Processor for the relevant purposes.

RESIDUAL RISK ACKNOWLEDGED

The login and the payment method sit with an individual. If the account were closed, transferred or disputed, the company's access to the client-data lane could be affected. The residual is one of continuity, not of contractual form — the Organisation and the DPA both name the company.

REMEDY, IF REQUIRED

Mistral's **Team plan** provides organisation administration — member roles, SSO and an allowed-email-domain control — which would move administration away from a single personal login. Recorded as an available option, not a current action.

SIGNED

Richard Flook, Director — Richard Flook Limited

Date: _____

Filed with the Eclipse data protection evidence. See INDEX.md.

Richard Flook Limited · Note to File — Mistral AI Account Holder · Confidential

DATA PROCESSING AGREEMENT

This Data Processing Agreement governs the Processing of Personal Data carried out by GRADIUM as part of its provision of the Services to Client, as Data Processor.

1. DEFINITIONS

All capitalized terms used in this Data Processing Agreement will have the following meanings.

- Client Personal Data means any Personal Data Processed by GRADIUM as a Data Processor on behalf of Client or Third-Party Controller.
- Data Controller, Data Processor, Data Security Breach, Data Subject, Personal Data, Processing, and Supervisory Authority shall have the meaning given to them under European Data Protection Laws.
- Data Processing Agreement means this document.
- European Data Protection Laws means the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), their national implementations in the EEA, including the European Union, and all other data protection laws of the EEA, the United Kingdom ("UK"), and Switzerland, each as applicable, and as may be amended or replaced from time to time.
- International Data Transfer means any transfer of Personal Data to a Restricted Country.
- Non-EEA Country means any country located outside of the European Economic Area (EEA), regardless of whether it benefits from an adequacy decision from the European Commission.
- Restricted Country means any country located outside of the European Economic Area (EEA) and that does not benefit from an adequacy decision from the European Commission.
- SCC means the clauses annexed to the European Commission Implementing Decision 2021/914 of June 4th, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR.
- Sub-Processor means any Data Processor appointed by GRADIUM.
- Third-Party Controller means a Data Controller for which Client is a Data Processor.
- UK Addendum means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).
- The terms "Share", and "Shared" shall have the same meaning given to them under the CCPA. The terms "Sell" and "Selling" shall have the meaning defined in Applicable Privacy Laws in the U.S.

All capitalized terms not defined herein shall have the meaning ascribed to them in the Terms of Service.

2. ROLE OF THE PARTIES AND PURPOSE OF THE PROCESSING

Client is the Data Controller and GRADIUM is the Data Processor with respect to the Processing detailed in Appendix 1. GRADIUM processes Client Personal Data on behalf of Client when Client uses the Services, as set out in Appendix 1.

If Client is a Data Processor on behalf of a Third-Party Controller, then Client shall act (i) as the single point of contact for GRADIUM; (ii) obtain all necessary authorizations from such Third-Party Controller; (iii) ensure that the Third Party Controller provided notice and obtained any consents necessary for Processing by Service Provider as set forth in this Data Processing Agreement; and (iv) undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.

3. MUTUAL OBLIGATIONS

Each Party shall comply with their respective obligations under the Applicable Privacy Laws and shall not, by any act or omission, cause the other to be in breach of any such obligations under the Applicable Privacy Laws.

4. OBLIGATIONS OF DATA PROCESSOR

The Parties agree that the subject matter, nature, purpose and duration of Processing performed by GRADIUM under this Data Processing Agreement as Data Processor, the type of Personal Data, and categories of Data Subjects, are as described in this Agreement and in Appendix 1.

When providing the Services, GRADIUM makes the following commitments as Data Processor:

- a) GRADIUM shall process Client Personal Data only on Client's documented lawful instructions as set out in this Data Processing Agreement or as otherwise necessary to provide the Services. In this regard, such instructions may be provided by Client via the use of the Services and via this Data Processing Agreement. GRADIUM shall process Client Personal Data for no purpose other than as authorized under this Data Processing Agreement, unless required to do so by applicable laws. In such a case, GRADIUM shall promptly inform Client of such legal requirement, unless prohibited to do so by applicable laws.
- b) GRADIUM shall ensure that GRADIUM's staff members have committed themselves to confidentiality of Client Personal Data, that staff members Processing Client have a need to know the relevant Client Personal Data for the provision of the Services and that Sub-Processors are under confidentiality obligations substantially similar to the confidentiality obligations imposed on GRADIUM pursuant to the Data Processing Agreement.
- c) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, GRADIUM shall implement and maintain the Security Measures to protect Client Personal Data from any Data Security Breach. The Security Measures implemented by GRADIUM under this Data Processing Agreement are listed in Appendix 3. Client acknowledges that

such Security Measures are subject to technical progress and development and that GRADIUM may update them from time to time, provided that such updates do not materially decrease the overall security of the Processing governed by this Data Processing Agreement. GRADIUM shall provide Client with reasonable and timely assistance to allow Client to comply with its obligations under Article 32 of the GDPR.

- d) Taking into account the nature of the Processing and the information available to GRADIUM, GRADIUM shall notify Client without undue delay and not later than forty-eight (48) hours after having become aware of a Data Security Breach affecting Client Personal Data. GRADIUM shall cooperate with Client, and if requested by Client, GRADIUM shall (i) provide Client with reasonable information about the Data Breach in its possession such as the nature of the personal data affected, or the cause and origin of the Data Security Breach, and (ii) provide reasonable assistance to Client to mitigate or remediate the Data Security Breach.

GRADIUM has no obligation to assess Client Personal Data in order to identify if they are subject to any specific legal requirements.

Upon Client's written request, taking into account the nature of the Processing and the information available to GRADIUM, this latter shall provide Client with commercially reasonable assistance to conduct a data protection impact assessment and to conduct a prior consultation with a Supervisory Authority when required by Applicable Privacy Laws and reasonably requested by Client, solely with respect to the Processing and Client Personal Data.

Taking into account the nature of the Processing, GRADIUM shall provide Client with commercially reasonable assistance (by appropriate technical and organizational measures) with respect to the fulfilment of Client's obligation to respond to requests from Data Subjects to exercise their rights under the Applicable Privacy Laws (a "Data Subject Request"). In the event GRADIUM receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by applicable laws) promptly notify Client of such Data Subject Request, and direct the Data Subject to Client. Client will be responsible for responding to any such Data Subject Request.

GRADIUM shall immediately inform Client if, in its opinion, Client's Processing instruction infringes the Applicable Privacy Laws. In such event, GRADIUM is entitled to refuse to perform the Processing of Client Personal Data that it believes to be in violation of the Applicable Privacy Laws.

5. USE OF SUB-PROCESSORS

Client hereby provides a prior and general authorization allowing GRADIUM to appoint any Sub-Processors to assist GRADIUM in the provision of the Services and in the Client Personal Data Processing described in Appendix 1, in accordance with the terms provided in this Data Processing Agreement.

GRADIUM commits that Sub-Processors (i) are to fulfil obligations at least equivalent to those set out in this Data Processing Agreement with respect to Personal Data protection; (ii) provide guarantees regarding Personal Data protection at least equivalent to those

presented by the measures implemented by GRADIUM. GRADIUM remains liable to Client for the fulfilment by the Sub-Processors of their contractual obligations towards GRADIUM.

Client hereby agrees that GRADIUM may appoint Sub-Processors from the list of Sub-Processors in Appendix 2 of this Data Processing Agreement. GRADIUM shall update the list of any Sub-Processor to be appointed at least thirty (30) days prior to the date on which the Sub-Processor shall commence the Processing of Client Personal Data.

Client may object in writing to GRADIUM's appointment of a new Sub-Processor within fifteen (15) days of such notice, provided that such objection is based on reasonable and substantiated grounds relating to compliance with Applicable Privacy Laws. If Client provides observations during this fifteen (15) days period, GRADIUM and Client will consult and negotiate in good faith to find a mutually acceptable resolution to address any objections raised by Client. If GRADIUM chooses to retain the Sub-Processor, GRADIUM shall inform Client at least thirty (30) days before authorizing the Sub-Processor to Process Client Personal Data, and either party may immediately discontinue providing or using the relevant parts of the Services, as applicable, and may terminate the relevant parts of the Services within thirty (30) days.

6. INTERNATIONAL TRANSFER OF CLIENT PERSONAL DATA

Unless GRADIUM otherwise explicitly commits not to transfer any Client Personal Data to a Non-EEA Country, Client authorizes GRADIUM to transfer Client Personal Data directly or indirectly to any country deemed to have an adequate level of data protection by the European Commission. Client also authorizes GRADIUM to perform International Data Transfers directly or indirectly to a Restricted Country (a) on the basis of adequate safeguards in accordance with Applicable Privacy Laws, including but not limited to the EU-US Data Privacy Framework, or (b) pursuant to the SCCs, as the case may be the UK Addendum if applicable, or any other transfer mechanism allowed pursuant to Applicable Privacy Laws.

This Section only applies if Client is located in a Restricted Country. By accepting this Data Processing Agreement, GRADIUM and Client conclude Module 4 (Processor-to-Controller) of the SCCs where Client is a Data Controller, and Module 3 (Processor-to-Processor) of the SCCs to the extent Client is a Data Processor on behalf of a Third-Party Controller, which are hereby incorporated and completed as follows and apply to any International Data Transfer conducted by GRADIUM acting as a Data Processor:

1. The "data exporter" is GRADIUM and the "data importer" is Client.
2. The optional docking clause in Clause 7 is not implemented.
3. Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 5 above.
4. The optional redress clause in Clause 11(a) is struck.
5. Option 2 in Clause 17 is implemented and the governing law in Clause 17 is the law of France.
6. The courts in Clause 18 are the Courts of France.
7. Annex I and II to the Modules 3 and 4 of the SCCs are Appendices 1 and 3 to this Data Processing Agreement respectively.

If GRADIUM has explicitly committed not to transfer any Client Personal Data to a Non-EEA Country, the aforementioned parts of this Section shall not apply and GRADIUM undertakes not to transfer any Client Personal Data to a Non-EEA Country.

7. AUDIT

Documentary audit. Upon Client's written request, GRADIUM will make available all documents and information to demonstrate that the Processing carried out by GRADIUM as Data Processor complies with this Data Processing Agreement in a timely manner, to the extent that is commercially reasonable and required by the Applicable Privacy Laws, subject to confidentiality and trade secrets. Documentary audits can be requested maximum once per year.

Onsite audit. For this Section, "Auditor" will have the meaning of either Client or the third-party auditor mandated by Client under this Section to conduct an audit or inspection as set out in this Section solely with respect to the Processing and compliance with this Data Processing Agreement. Only to the extent Client cannot reasonably be satisfied with GRADIUM's compliance with this Data Processing Agreement through the exercise of the documentary audit set out in this Section, Auditor may conduct up to one (1) onsite audit per year to verify GRADIUM's compliance with this Data Processing Agreement, under the conditions defined below:

1. Client demonstrates that Auditor is subject to strict confidentiality obligations.
2. Client demonstrates that Auditor is independent, impartial and with expertise in data protection, and is not a competitor of GRADIUM.
3. The procedure described below is followed:
 1. Client gives GRADIUM a thirty (30)-days prior written notice of such audit or inspection (hereafter "Audit").
 2. During this thirty (30)-days period, Client and GRADIUM mutually agree in writing upon the scope (which must be limited to Processing operations related to the provision of Services to Client), timing and duration and starting date of the Audit.
 3. Client ensures that the Audit will not impact GRADIUM's organization or GRADIUM's activities, and is carried out during regular business hours.
 4. GRADIUM will not give access to its premises for the purposes of the Audit:
 1. To an Auditor's employee who does not provide GRADIUM with reasonable evidence of identity and authority.
 2. To any Auditor's employee who requests access to GRADIUM's premises outside regular business hours.
 5. GRADIUM will not give access to premises other than its corporate site; for example, GRADIUM will not provide access to Sub-Processors' premises.
 6. The Audit is conducted by the Auditor in a reasonable manner and in good faith, an identical copy of the Audit report shall be given to both Parties following the completion of the Audit. Each Party may make observations regarding the Audit report.
 7. All costs relative to the Audit will be at the charge of Client unless the Audit reveals a breach by GRADIUM of this Data Processing Agreement or Applicable Privacy Laws.

8. OBLIGATIONS OF DATA CONTROLLER

Client agrees and commits to the following:

1. Client is responsible for compliance with the requirements of Applicable Privacy Laws applicable to Data Controllers. In particular, Client guarantees that the Processing is compliant with the Applicable Privacy Laws and in particular that the Data Subjects are informed of the Processing via an appropriate information notice and have given their consent as necessary to comply with Applicable Privacy Laws, in particular where the Processing described in Appendix 1 includes sensitive data or special categories of data within the meaning of Applicable Privacy Laws.
2. Client is solely responsible for the accuracy and appropriateness of Personal Data and the means by which such Personal Data is acquired in compliance with the Applicable Privacy Laws. Client is solely responsible for providing GRADIUM with instructions that comply with this Data Processing Agreement and the Applicable Privacy Laws.
3. Client undertakes to document in writing any additional instructions regarding the Processing by GRADIUM.

9. RETURN AND DESTRUCTION OF PERSONAL DATA

Upon the termination of Client's access to and use of the Services, GRADIUM will, up to forty-five (45) days following such termination, delete or return to Client, at Client's choice, all Client Personal Data detained by GRADIUM except as otherwise authorized under the Terms of Service. Client acknowledges and accepts that Client Personal Data will no longer be accessible upon the expiry of the forty-five (45) day period.

Without prejudice of any Zero Data Retention feature implemented as applicable, GRADIUM may retain Client Personal Data to the extent required by applicable law but only to the extent and for such period as required by such law and always provided that GRADIUM shall ensure the confidentiality of all such Client Personal Data.

10. California Provisions

These CCPA Terms apply when the California Consumer Privacy Act of 2018, Cal. Civ. Code §§1798.100–1798.199.100, as amended, and the CCPA regulations, Cal. Code Regs. §§7000–7304 (together, the "CCPA") applies to Client's use of the Services to process the Personal Information contained in Client Personal Data and Account Data.

Where the CCPA applies, GRADIUM acknowledges that it does not receive Personal Data as consideration for any Services provided to Client. GRADIUM: (i) is responsible for compliance with its obligations under this Data Processing Agreement, (ii) is responsible for compliance with its obligations as a service provider under the CCPA, and (iii) shall provide the same level of privacy protection as required by the CCPA. GRADIUM shall notify Client if it reasonably determines that it cannot meet its obligations under the CCPA, and in such circumstances, and upon provision of notice to GRADIUM, Client shall be entitled to take reasonable and appropriate steps to remediate unauthorized use of Personal Data. GRADIUM must not process the Personal Data for any purpose other than for the purpose of performance of the Agreement, except where and to the extent permitted by the CCPA.

GRADIUM shall not: (i) Sell or Share Client Personal Data; (ii) retain, use, or disclose Client Personal Data for any purpose other than for the purpose of performance of the Services except as expressly permitted under the CCPA; (iii) retain, use, or disclose Client Personal Data with Personal Data obtained from, or on behalf of, sources other than Client, except as expressly permitted under the CCPA; or (iv) process Client Personal Data for targeted and/or cross context behavioral advertising. GRADIUM certifies that it understands the restrictions set out in this Section and will comply with them. Solely for the purpose of the CCPA, GRADIUM shall promptly notify Client if it determines that it can no longer meet its obligations under the CCPA.

11. PROCESSING OF GRADIUM AS DATA CONTROLLER

GRADIUM processes Personal Data as Data Controller for the purposes set forth in GRADIUM's Privacy Policy available at the following link and any succeeding link: <https://gradium.ai/privacy>.

Unless the Zero Data Retention feature is applicable or Client objected to the Processing, Client also authorizes GRADIUM and its Affiliates, and any party replacing GRADIUM to the Agreement, to reuse Client Personal Data for the purpose of improving current and future Services, and training any AI model or product as an independent Data Controller.

GRADIUM undertakes to comply with the Applicable Privacy Laws in relation to all Processing for which it is classified as Data Controller. The information related to such Processing are set forth in Gradium's Privacy Policy and Client undertakes to direct all its users of the Services to this Privacy Policy.

12. DURATION

This Agreement will remain in force as long as Client uses the Services.

13. JURISDICTION AND GOVERNING LAW

Any dispute arising from this Data Processing Agreement will be resolved by the competent courts of Paris, France in accordance with the Terms of Service.

This Data Processing Agreement is governed by the laws of France

Appendix 1

Detail of Processing

1. PARTIES

Client as Data Controller or Data Processor of a Third-Party Controller, and data importer for the purposes of SCCs as applicable.

GRADIUM as Data Processor and data exporter for the purposes of SCCs as applicable.

2. DURATION OF PROCESSING

If the Zero Data Retention feature is not activated, GRADIUM shall store Client Personal Data as Data Processor solely for the duration of the Services.

If the Zero Data Retention feature is applicable, GRADIUM shall not store any Input and Output after their respective ingestion and generation for a duration longer than necessary to the generation of Output and shall not be retained further. Notwithstanding the foregoing, GRADIUM may retain Voice Sample recordings that are (i) explicitly and separately provided by Client for the sole purpose of Voice Reproduction, and (ii) reasonably necessary to deliver the Voice Reproduction pursuant to the Services.

3. SUBJECT-MATTER AND NATURE OF PROCESSING

Generation of Output and Voice Reproduction based on Client's Input at Client's request.

4. FREQUENCY OF THE PROCESSING

On a continuous basis.

5. PURPOSE OF PROCESSING

The purpose of the Processing of Client Personal Data is provision of the Services.

6. DATA SUBJECTS

Data subjects whose characteristics, such as their voice, are present in Client's Input and, as applicable, reproduced in Output.

7. CATEGORIES OF PERSONAL DATA

Voice input, voice recordings, text input, or other content included in Client's Input, and text or voice Output generated by GRADIUM based on Input provided by Client.

8. SENSITIVE DATA

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.

Appendix 2

List of Subprocessors (at the date of signature of the Agreement)

#	Corporate denomination	Address	Country of establishment	Data Storage location	Subcontracted Processing operations	Transfers Tool (SCC, BCR...)
1	Scaleway	8 rue de la Ville l'Evêque, 75008, Paris, France	France	EU	Cloud infrastructure	N/A
2	Amazon Web Services EMEA SARL	38 avenue John F. Kennedy, L-1855, Luxembourg	Luxembourg	Frankfurt, Germany	Hosting / Compute for model inference	Data region locked to the EU (Frankfurt); SCCs
3	Clerk, Inc	660 King Street, Unit 345, SF, California, United States	USA	USA	Provision of the authentication service and management of studio user accounts	Certification under the EU-US Data Privacy Framework (DPF).

Appendix 3

Security Measures

GRADIUM implements the following Security Measures:

- Real-time monitoring systems are implemented across the organization's IT infrastructure to detect, log, and alert on suspicious or unauthorized activity. Alerts generated by the monitoring tools are reviewed promptly by the IT security team to ensure rapid response and incident containment.
- All internal and external web traffic is encrypted using HTTPS with Transport Layer Security (TLS), ensuring that data transmitted between clients, servers, and third-party services remains confidential and protected against interception or tampering. This encryption protocol provides robust authentication and integrity assurance, preventing man-in-the-middle attacks and safeguarding personal and business-critical information in transit.
- GRADIUM uses a virtual private cloud (VPC) which isolates GRADIUM's cloud and traffic from the open web and whose entry points are controlled by GRADIUM via API to further strengthen access control and protect internal systems from external exposure.

As GRADIUM develops and expands, more organisational and technical measures will be implemented. Together, these measures form a cohesive security framework designed to

maintain the confidentiality, integrity, and availability of data while supporting GDPR compliance.

All the security measures are listed at trust.gradium.ai.

Downloaded at Thu, 01 Oct 2026 13:54:41 GMT
Downloaded by advancedclearingenergetics@gmail.com

Terms of Service

Version: July 2026

Between Gradium, a French limited joint-stock company (*société par actions simplifiée*), registered at the trade register of Paris, under number 989 284 955 having its registered office at 151bis rue Saint-Honoré, 75001 Paris, France, ("**GRADIUM**"), and customer subscribing to GRADIUM's Services (as defined hereafter) ("**Client**").

These Terms of Service are made by and between GRADIUM and Client and entered into as of the Effective Date (as defined below) for the purpose of granting Client a limited subscription to use GRADIUM's artificial intelligence models (the "**Models**").

1. Definitions

Affiliate means any entity (a) that a Party Controls; (b) that a Party is Controlled by; or (c) with which a Party is under common Control, where "**Control**" means direct or indirect control within the meaning of Article L233-3 of the French Commercial Code.

Agreement means these Terms of Service, and any document and policy referenced therein including but not limited to the Documentation.

API means the Application Programming Interface provided by GRADIUM to Client to allow Client to use the Models.

Applicable Laws means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern the provision and/or use of Services, the Client Service and any part thereof such as Input collection, use and provision.

Applicable Privacy Laws means any applicable privacy or data protection legislation or regulations, governing personal data protection and voice processing, including but not limited to European Data Protection Laws, and the California Consumer Privacy Act, as amended by the California Privacy Rights Act and its implementing regulations as amended or superseded from time to time ("CCPA") as well as similar laws adopted in other states. European Data Protection laws shall have the meaning ascribed to them in the Data Processing Agreement.

Beta Services has the meaning set forth in Section 2.12 (Beta Services).

Client Environment means the systems, platforms, services, devices, software, AI models and systems, servers, sites and/or networks that Client uses for the operation of Client Service to the exclusion of the Services.

Client Data means the data that are submitted to the Services, including Input, by Client or on its behalf, the Voice Sample, the Voice Reproduction and the Output.

Client Personal Data means Personal Data contained in Client Data.

Client Service means as applicable the service provided by Client to its customers, which integrates the Services.

Confidential Information has the meaning set forth in Section 12.1 (Confidential Information).

Disclosing Party means a Party to the Agreement when the Party is providing or disclosing Confidential Information to the other Party.

Documentation means the usage manuals and instructional materials for the Services that are made available by GRADIUM to Client at the following link and any succeeding link: <https://gradium-ai.github.io/gradium-api/documentation/docs.html>.

Data Processing Agreement means the document available in Exhibit 1.

Effective Date means the date of subscription of the Services.

Fees means all the applicable amounts owed by Client to GRADIUM for the Services, which includes the Service Plan Fees, the Usage Overage Fees, and the Zero Data Retention fees and any fees associated to GRADIUM's commitment not to transfer Personal Data outside the EU, where applicable.

Feedback means suggestions, feedback, or comments from Client or users for improvement of the Services.

Force Majeure Event means an unforeseen event outside a party's reasonable control where the affected party took reasonable measures to avoid or mitigate the impacts of the event, and which prevents a party from performing its obligations (except payment of Fees) as per Article 1218 of the French Civil Code. Examples of these kinds of events include unpredicted natural disasters like a major earthquake, war, pandemic, riot, act of terrorism, or public utility or internet failure.

GRADIUM Covered Claim has the meaning set forth in Section 9.1 (Indemnification by Client).

Individual means any individual who interacts with, receives, or is otherwise exposed to the Models and/or their Output, whether through a telephone call, a live or recorded audio or video exchange, translated or dubbed content, or any other means, and whether or not as part of Client Service.

Input means any voice recording, audio, text, image, video, prompt, description, or other content submitted by Client or on its behalf to GRADIUM for the provision of the Services, including but not limited to the Voice Sample and any voice or text content to be processed by the Models to generate an Output, whether in the form of a transcription, translation, conversion, synthesis, or any other transformation thereof.

Intellectual Property Rights means any right or protection existing from time to time in any jurisdiction, whether registered or not, under any patent law or other invention or discovery law, copyright law, trademark law, performance or moral rights law, trade-secret law, confidential information law, integrated circuit topography law, semi-conductor chip protection law, data law, database law, trade-mark law, unfair competition law or other similar intellectual property laws and includes related legislation by competent governmental authorities and related judicial decisions under common law or equity.

Malicious Code means code, files, scripts, agents, or programs intended to do harm, including viruses, worms, time bombs, and Trojan horses.

Models means the AI Models available by GRADIUM as part of the Services, including without limitation any speech-to-text (STT), text-to-speech (TTS), speech-to-text translation (STT Translation), speech-to-speech translation (S2S Translation) model, or any other

artificial intelligence model developed, offered, or made available by GRADIUM from time to time, whether now existing or hereafter introduced, under any current or future name, version, or denomination.

Output means any text, synthetic audio recording, or other content generated by the Models based on the Input provided by Client, including without limitation any transcription, translation, conversion, or synthesis of such Input, whether or not based on a Voice Reproduction. For the avoidance of doubt, Output does not include the Models, the API, any voice embedding and any other artificial intelligence models or systems owned by GRADIUM or powering the Models and their related components.

Party, Parties means either Client or GRADIUM or collectively Client and GRADIUM.

Personal Data has the meaning(s) set forth in the Applicable Privacy Laws for personal information, personal data, personally identifiable information, or other similar term.

Recipient means a Party to the Agreement when the Party receives Confidential Information from the other Party.

Services means the provision of the Models and associated services, together with our website as further described in Client's subscription and the Documentation, and which includes the Models and as applicable the API, whether for free or in consideration of the Fees, and whether provided by API or via GRADIUM's website.

Service Plan means the level of Services selected and subscribed to by Client, which determines the scope of features, usage limits, support entitlements, and other included benefits or limits. Service Plans are described at the time of subscription.

Service Plan Fees means the price associated to each Service Plan as described at the time of finalization of the subscription, and as updated afterwards.

Security Measures means GRADIUM's security measures described in Appendix 3 to the Data Processing Agreement.

Taxes has the meaning set forth in Section 5.6 (Taxes).

Term means the duration of the Agreement as set forth in Section 4.1 (Term).

Territory means the whole world, except as provided under the Agreement.

Usage Overage Fees means the price associated to any Service Plan overuse if activated by the Client.

Voice Reproduction means the model used to generate voice Output in the form of synthetic audio sounding like the Voice Sample provided by Client and based on the Voice Sample.

Voice Sample means the voice recording provided by Client to GRADIUM to create a Voice Reproduction as part of the provision of the Services.

Zero Data Retention means the feature of deletion of Input and Output as described in Section 2.7 (Zero Data Retention).

2. GRADIUM's Obligations

- 2.1. **Services.** GRADIUM will provide the Services part of the subscription to Client.
- 2.2. **Professional use.** The Services are specifically designed for professional and business use. The Services are not intended for personal, consumer, or non-professional use. By accessing or using the Services, Client represents and warrants that any user using the Services is acting on behalf of a business, organization, or professional entity. Where Clients are natural persons, they must be at the age of legal majority where Clients live.
- 2.3. **Documentation.** GRADIUM will make Documentation available to Client.
- 2.4. **Client Data.** GRADIUM will process Client Data submitted to the Services by or on behalf of Client and generated by the Services only according to the Agreement, the Documentation and GRADIUM's Privacy Policy.
- 2.5. **Security Measures.** GRADIUM will maintain Security Measures to protect Client Data from accidental loss and from unauthorized access, use, alteration, or disclosure. Subject to Section 8.3 (GRADIUM Warranties), GRADIUM may modify the Security Measures from time to time.
- 2.6. **Personal Data.** Where Client is deemed data controller under Applicable Privacy Laws, GRADIUM shall process any Client Personal Data on behalf of Client, as data processor, pursuant to the terms of the Data Processing Addendum, and the Parties agree to comply with such terms. GRADIUM processing of Personal Data as data controller, whether Client is deemed data controller, are set forth in GRADIUM's Privacy Policy available at the following link and any succeeding link: <https://gradium.ai/privacy>
- 2.7. **Zero Data Retention.** If the Zero Data Retention is activated, Client acknowledges and agrees that GRADIUM will not store any Client Data and will immediately delete Client Data after the generation and provision of Output. By exception to the foregoing, GRADIUM may retain Voice Sample and Voice Reproduction solely for the purpose of providing the Services. Zero Data Retention may be subject to additional Fees.
- 2.8. **Overuse.** The Services are subject to usage limitations described in the applicable Service Plan. GRADIUM shall notify Client by email when its use of the Services reaches both 80% and 100% of the Services use limitation. If not already activated, Client can decide to activate Usage Overage Fees to continue using the Services beyond the Services use limitations for the applicable subscription period. If Usage Overage Fees are not activated, GRADIUM shall block the use of the Services above 100% of the Services use limitation for the current subscription period, without any liability for GRADIUM.
- 2.9. **Services and Service Plan Updates and Modifications.** Subject to Section 8.3 (GRADIUM Warranties), GRADIUM may from time to time and in its discretion provide updates, modifications or upgrades to the Services and Service Plans, but is under no obligation to do so. All references herein to the Services and Service Plans shall include updates and modifications thereto. The Agreement shall govern any update that replaces or supplements the original Services and Service Plan, unless the update is accompanied by separate supplemental terms which will govern the revision. If a modification to Service Plans introduces new or additional Services limitations to Client, Client's current Service Plan shall remain in force for the duration of the current subscription period. After that subscription period ends or at

the date indicated by GRADIUM, Client's subscription will automatically switch to the modified Service Plan at the time of renewal and for the same duration as the initial subscription term, unless Client terminates the Agreement in accordance with Section 4.1 (Term) and at least ten (10) days before the change of Service Plan takes effect.

2.10. Upgrade of Service Plan. Subject to GRADIUM's approval, Client may request to upgrade its Service Plan. The new Service Plan will then replace the previous Service Plan for the same Term, unless otherwise specified in the applicable Service Plan description, and Client shall pay the applicable Service Plan Fees.

2.11. Maintenance. Access and use of the Services may be interrupted from time to time for maintenance of the Services carried out by GRADIUM. Except for emergency maintenance, GRADIUM shall take commercially reasonable measures to carry out maintenance during French continental non-business hours and to provide reasonable prior notice to Client.

2.12. Beta Services. From time to time, GRADIUM may offer services identified as beta, pilot, developer preview, non-production, evaluation or by a description of similar import ("**Beta Services**"). Client may accept or decline Beta Services. If Client accepts Beta Services, Beta Services: (i) are provided only for evaluation purposes; (ii) may not be relied on by Client for production use; (iii) may not be supported; and (iv) may be subject to additional terms. Unless otherwise stated, any Beta Services trial period will expire on the date that a version of the Beta Services becomes generally available or is discontinued. GRADIUM may discontinue Beta Services at any time in its sole discretion and may never make Beta Services generally available.

ALL BETA SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE" WITHOUT ANY WARRANTY OF ANY KIND. BETA SERVICES MAY BE TERMINATED AT ANY TIME. GRADIUM DISCLAIMS ALL OBLIGATION AND LIABILITY UNDER THE AGREEMENT FOR ANY HARM OR DAMAGE ARISING OUT OF OR IN CONNECTION WITH A BETA SERVICE, INCLUDING ANY OBLIGATION OR LIABILITY WITH RESPECT TO CLIENT DATA. ANY CLIENT DATA ENTERED INTO BETA SERVICES MADE TO BETA SERVICES BY OR FOR CLIENT, MAY BE PERMANENTLY LOST IF THE BETA SERVICES ARE SUSPENDED, TERMINATED, OR DISCONTINUED.

3. Client's Obligations

3.1. Client's responsibilities. Client agrees and acknowledges that Client is responsible:

- a. For the provision, use and maintenance of Client Environment and Client Service, including but not limited to any telecom service allowing voice exchanges between Individuals and Output and any applicable rerouting of Individuals to third parties, any AI system processing Individual's speech or other content where the corresponding Model is not provided by GRADIUM, and any AI system inferring responses to be provided to Individuals and transmitted to the Services as Input to produce corresponding Output.
- b. To inform Individuals that they are interacting with an AI system in accordance with Applicable Laws.
- c. For properly configuring Client Environment with the Services in accordance with the Documentation as applicable.
- d. For providing all equipment, systems, assets, access, and ancillary goods and services needed to access and use the Services, and for ensuring their compatibility with the Services.

- e. For interactions of Individuals with Client Service and any consequence resulting from such interactions.
- f. For storing and making backup of all Individuals' interactions, and relating Input and Output, in accordance with the state of the art. For the avoidance of doubt, this paragraph shall not constitute an obligation upon Client to carry out such backup if it is not necessary for Client, being reminded that GRADIUM shall in any case not be responsible for such task.

3.2. Input and Output. Client is responsible, in particular with respect to compliance with Applicable Laws and Applicable Privacy Laws for:

- a. Input provided to the Services.
- b. Output transcribing faithfully reflecting the content of the Input, whether in the form of a transcription, translation, conversion, or synthesis thereof.
- c. Providing appropriate and required notices and information to Individuals and any individual whose data is processed as Input, Output and/or Voice Reproduction.
- d. Obtaining consents where applicable, including but not limited to the collection, recording and processing of Individual's speech, Individual's interaction with an artificial intelligence system and any individual's voice processed as Input, Output and/or Voice Reproduction. Client shall obtain and maintain any required consents necessary to permit the processing of Client Data by GRADIUM under the Agreement including but not limited to any individual consent required to record Individuals, provide Voice Sample to produce Voice Reproduction, provide Input to produce Output, or with respect to any content included into Input such as Intellectual Property Rights.
- e. Ensuring every Input submitted through the Services complies with Applicable Laws and are accurate and appropriate for their purpose.

3.3. Personnel, Users and Performance. As applicable, Client shall be responsible for the performance of its personnel (including employees and contractors) and users' use of the Services in compliance with the Agreement and Applicable Laws. Client enters into the Agreement on behalf of the users that make use of the Services under its subscription. Client shall ensure that users comply with the terms of the Agreement and any act, omission, breach, or negligence committed by users will be deemed an act, omission, breach or negligence of Client for all purposes under the Agreement, and Client shall be jointly and severally liable for any such act, omission, breach, or negligence committed by users.

3.4. Usage Restrictions. Client shall not:

- a. Use the Services in a way that is not compliant with the Agreement and/or Applicable Laws.
- b. Direct the Services to generate any Output in violation of any applicable Intellectual Property Right, contractual restriction, privacy or publicity right of any other person, or otherwise violate any Applicable Law.
- c. Upload, submit, create, transmit, display, perform, post, store, or otherwise make available through the Services any content, including Input and Output, that is unlawful, threatening, defamatory, obscene, excessively violent, deceptive, fraudulent, libelous, unethical, invasive of privacy or publicity rights, harassing, abusive, hateful, discriminatory, violent, or cruel, or otherwise use the Services in a manner that is obscene, excessively violent, harassing, hateful, cruel, abusive, inciting, organizing, promoting or facilitating violence or criminal activities.
- d. Direct and/or use the Services to impersonate another person or business without their explicit authorization.
- e. Direct and/or use the Services to create, provide, disseminate disinformation, misleading, inaccurate or false content or information, promote unlawful activities or for political reasons (e.g. campaigning, lobbying, fundraising, solicitation etc).

- f. Direct and/or use the Services to provide medical, legal or financial advice without the necessary qualifications.
- g. Use the Services to access GRADIUM's Intellectual Property Rights except as permitted under the Agreement.
- h. Use the Services to store, transmit or display Malicious Code.
- i. Modify or try to modify the Services and Documentation.
- j. Interfere with or disrupt the integrity or performance of the Services.
- k. Attempt to gain unauthorized access to any of GRADIUM's data centers, systems, models or networks.
- l. Permit direct or indirect access to or use the Services in a way that circumvents a usage or capacity limit of the Services, or for a purpose that is not authorized under the Agreement.
- m. Sell, resell, license, sublicense, distribute, redistribute, rent, make publicly available or lease the Services.
- n. Copy, modify, improve the Services or create a derivative work of the Services or any part, feature, function, or user interface thereof.
- o. Access, use, modify, copy, analyze any part of the Services, including Output and Voice Reproduction, or the Documentation to develop a competitive AI model, AI system, product, software or service.
- p. Access, duplicate, reverse engineer, decompile, translate, disassemble, decode or otherwise attempt to extract any or all of the source code, algorithm, object code, underlying structure, sequence, organization, file formats, non-public APIs, or ideas of any part of the Services for any purpose, even to correct errors, this ability being exclusively reserved to GRADIUM.
- q. Alter, remove or obscure any copyright, trademark or other proprietary notices or confidentiality legend on the Services.
- r. Frame or mirror the Services without GRADIUM's express prior written consent or use any robot, spider, site search/retrieval application or other manual or automatic device to retrieve, index, "scrape," "data mine," or in any way gather any messages, text, files, images, photos, video, sounds, profiles, works of authorship, or any other content from the Services or reproduce or circumvent the navigational structure or presentation of the Services without GRADIUM's express prior written consent.
- s. Use the Services in any situation of medical and drugs advice, emergency healthcare and emergency services, healthcare diagnostic, assessment and prescription, aircraft or other modes of human mass transportation or nuclear or chemical facilities.
- t. Circumvent, disable or otherwise interfere with security-related features of the Services that prevent or restrict use or copying of any content or that enforce limitations on use of the Services.

Client shall be solely responsible for any consequence resulting from its violation of this Section. In the event GRADIUM reasonably believes a violation of this Section has occurred, GRADIUM will have the right, but not the obligation, to investigate the suspected violation and suspend access from the Services for so long as reasonably necessary to address the potential violation. GRADIUM will notify Client by email of any such suspension and work with Client in good faith to resolve the potential violation. Such suspension notice will be provided in advance, unless GRADIUM reasonably believes the suspected violation creates an urgent or emergency situation where a failure to take immediate action may put GRADIUM, Client, or other GRADIUM clients at risk of imminent harm. If Client materially fails to comply with Client's obligations under this Section (Usage Restrictions), GRADIUM may terminate the Agreement immediately for cause pursuant to Section 4.2 (Termination for Cause).

3.5. **Moderation.** GRADIUM does not undertake to review all Client Data and disclaims any duty or obligation to undertake any monitoring or review of any Client Data. Without prejudice to the foregoing, GRADIUM may delete or remove Client Data or refuse to generate any Output if such Client Data violates the Agreement and/or Applicable Laws.

3.6. **Client Login Information.** Client must protect the confidentiality of Services login credentials provided by GRADIUM. Login credentials and any Client's account are personal and cannot be shared. Client shall be responsible to prevent unauthorized access to or use of the Services and shall accordingly be liable for any breach of the Agreement caused by any unauthorized use of the Services. Client shall promptly notify GRADIUM if it suspects or knows of (i) any fraudulent activity with its accounts, passwords, or credentials, (ii) if they are lost or become compromised, and/or (iii) in case of unauthorized access or use of the Services via Client's login credentials.

4. Term and Termination

4.1. **Term.** The Agreement duration shall be based on Client's subscription, which may either be a monthly subscription (based on calendar months) or an annual subscription (based on the Effective Date). Client's subscription shall be tacitly and automatically renewed at the end of each current term for an additional month or year as the case may be, unless either Party gives notification to the other Party of its intent not to renew the Agreement with a ten (10) day prior notice for monthly subscriptions and sixty (60) days prior notice for annual subscriptions before the end of the subsequent term (the initial subscription term and any subsequent terms being together the "**Term**").

4.2. **Termination for Cause.** Client or GRADIUM may terminate the Agreement for cause (i) upon fifteen (15) days' written notice to the other Party in the event of a material breach, including but not limited to the representations and warranties set forth in Section 8 (Warranties), if the material breach remains uncured at the expiration of the notice period, (ii) immediately in case of material breach if such material breach cannot be cured, or (iii) if the other Party (x) becomes the subject of a proceeding relating to insolvency, receivership, liquidation or assignment for the benefit of creditors to the extent permitted by Applicable Laws, (y) goes out of business or (z) ceases its operations.

4.3. **Effect of Termination.** Upon any expiration or termination of the Agreement, (i) Client will no longer have any right to use the Services; (ii) each Recipient will return or destroy Disclosing Party's Confidential Information in its possession or control without undue delay, including but not limited to Voice Sample and Voice Reproduction, except for Client Data licensed pursuant to Section 6.1 (Client Data) for Services improvement and AI model training; and (iii) the Parties will make any payments required under Section 4.4 (Refund or Payment upon Termination).

4.4. **Refund or Payment upon Termination.** If Client terminates the Agreement in accordance with Section 4.2 (Termination for Cause), Section 2.9 (Services and Service Plan Updates and Modifications), Section 5.2 (Fees Revision) or Section 23 (Modifications), GRADIUM will refund any prepaid Fees covering the remainder of the Term after the effective date of termination. If the Agreement is terminated by GRADIUM in accordance with Section 4.2 (Termination for Cause), Client will pay any unpaid Fees covering the remainder of the current Term. In no event will termination relieve Client of its obligation to pay any Fees payable for the period prior to the effective date of termination. If Client terminates the Agreement without cause prior to the end of the then current Term, Client shall be immediately liable for the

balance of the Fees for the remainder of the current Term and there shall be no refund for partially used subscription periods.

5. Fees and Payment

- 5.1. **Fees.** Client will pay all Fees to GRADIUM. Fees details are described during the subscription process, and Client will receive a summary of the applicable Fees once its subscription is complete. If Client agrees to Usage Overage Fees, and in the event Client's usage exceeds the volume provided under its Service Plan, Client shall be charged the applicable Usage Overage Fees as described by the Usage Overage Fees financial conditions and failure to pay Usage Overage Fees may result in the suspension of use of the Services as described therein.
- 5.2. **Fees Revision.** GRADIUM may change the Fees, including Usage Overage Fees, charged for the Services at any time by notifying updated pricing through the Services; provided, however, that the Fees for Client's ongoing subscription shall remain in force for the duration of the current subscription period. After that subscription period ends, Client's use of the Services shall be charged at the then-current subscription Fees or at the date indicated by GRADIUM. If Client does not agree to this Fees revision, Client must terminate the Agreement in accordance with Section 4.1 (Term) and at least ten (10) days before the change of Fees takes effect. In absence of such termination, Client's subscription will automatically switch to the then-current Fees at the time of renewal or the date indicated by GRADIUM.
- 5.3. **Payment methods.** Client shall pay the Fees through the payment method set forth in the subscription process. Client represents and warrants that it has the right to use any payment method that is submitted in connection with a payment and that all payment information provided is true and correct. Client is responsible for any payment charge associated with its payment method. By submitting its payment information, Client hereby authorizes GRADIUM to collect and store Client's payment information and charge Client for the Fees (including Usage Overage Fees) with no further action required from Client in accordance with the Agreement. Client is responsible for any payment fee associated to the payment method used for the payment of the Fees.
- 5.4. **Invoicing Terms.** Client will pay correct and undisputed invoices within seven (7) days from issuance of such invoice. Client shall pay upfront Fees on the day of subscription for the ongoing subscription period, and each subsequent Fees on an upfront basis on the subsequent subscription anniversary date(s) whether for monthly or yearly subscription periods (for illustration purpose, for a monthly subscription started on May 7th, the next payment date shall be June 7th).
- 5.5. **Late payment.** If Client fails to pay undisputed Fees within five (5) days of the payment due date, GRADIUM reserves the right to suspend the provision of the Services after providing Client with a two (2) days' prior notice of non-payment by email to Client. Suspension of the Services does not relieve Client of its obligation to pay all outstanding amounts and will last until full payment of the Fees due. Without prejudice of GRADIUM's right to suspend the Services in accordance with this Section, and to terminate the Agreement for material breach in accordance with Section 4.2 (Termination for Cause), in the event of late payment, Client shall pay to GRADIUM an interest on the overdue amount accrued at the rate of ten (10) percentage points above the European Central Bank's reference rate, from the due date until full payment is made, and recovery costs which may not be lower than (40)

euros. This late payment compensation and interest are due automatically without the need for a formal reminder.

5.6. **Taxes.** Fees for Services do not include any taxes, levies, duties, or similar governmental assessments of any nature, including, for example, value-added, sales, use, or withholding taxes assessable by any jurisdiction whatsoever and applicable to the provision of the Services (collectively, "**Taxes**"). Client is responsible for paying all Taxes associated with the Fees. If GRADIUM is obligated by law to pay or collect Taxes for which Client is responsible, GRADIUM will invoice Client and Client will pay that amount unless Client can provide a valid tax exemption certificate authorized by the appropriate taxing authority. Client will provide GRADIUM any information GRADIUM reasonably requests to determine whether GRADIUM is obligated to collect Taxes. Each Party is solely responsible for taxes assessable against its income, property, and employees in accordance with Applicable Laws.

6. Licenses and Intellectual Proprietary Rights

6.1. **Client Data.** As between the Parties and to the extent Client Data is protected by Intellectual Property Rights, Client shall own and retain all Intellectual Property Rights in Client Data. Client hereby grants GRADIUM and its Affiliates for the Term, a worldwide, nonexclusive, irrevocable, non-transferable (except as permitted in Section 10 (Assignment)), non-sublicensable (except to GRADIUM's service providers for the below purposes), royalty-free, and limited license to use, store, copy, modify, transmit, display, publish, distribute, reproduce Client Data, and create derivative works thereof as necessary for GRADIUM to provide, manage, maintain and optimize the Services, which includes debugging, assessing, reviewing and correcting the performance of the Services in accordance with the Agreement, and exercise its rights under the Agreement. Except in case of activation of the Zero Data Retention, Client hereby grants GRADIUM and its Affiliates a worldwide, nonexclusive, irrevocable, non-transferable (except as permitted in Section 10 (Assignment)), non-sublicensable (except to GRADIUM's service providers for the below purposes), royalty-free, and limited license to use, store, copy, modify, transmit, display, publish, distribute, reproduce Client Data, and create derivative works thereof as necessary for GRADIUM to analyse and improve the current and future Services, and train and develop any underlying AI model, including but not limited to the Models, for the greater of the duration necessary to achieve the intended purposes or the duration of the legal protection of any Intellectual Property Rights contained in Client Data. Except otherwise expressly provided in this Agreement, GRADIUM acquires no right, title, or interest from Client under the Agreement in or to Client Data. Client acknowledges that due to the nature of generative AI tools, Outputs may not be unique, and users of the Services may receive their own Output that is similar or the same as Client's Output. Client hereby waives and releases GRADIUM and any of its Affiliates from any claim that another user's Output is the same as, or reproduces, any of Client's Output.

6.2. **Services and Models.** As between GRADIUM and Client, GRADIUM shall own and retain all Intellectual Property Rights in (a) the Services including but not limited to the Models, the API, the Documentation, text, graphics, images, photographs, videos, illustrations, its website and other content contained therein, and all improvements, enhancements or modifications thereto; and (b) any software, applications, inventions or other technology developed in connection with the Services, its website or support. Client shall not take any action inconsistent with GRADIUM's Intellectual Property Rights. In consideration of the Fees, GRADIUM grants Client for the Term and Territory a personal, limited, non-exclusive, non-transferable, non-sublicensable license to use the Services in accordance with the Agreement and solely for the provision of Client Service. Where the Service Plan

subscribed is a free plan, the license is only given for Client's internal and non-commercial purposes. No rights are granted to Client except as expressly set forth in the Agreement

6.3. **Feedback.** Client may, but is not required to, give GRADIUM Feedback, in which case Client gives Feedback "AS IS". Client acknowledges and expressly agrees that any contribution of Feedback does not and will not give or grant Client any right, title or interest in the Services or in any such Feedback. All Feedback becomes the sole and exclusive property of GRADIUM, and GRADIUM may use, transfer, sub-license and disclose Feedback in any manner and for any purpose whatsoever, including AI model training and current and future Services improvement, without further notice or compensation to Client and without retention by Client of any proprietary or other right or claim, for the whole world and for the greater of the duration necessary to achieve the intended purposes or the duration of the legal protection of any Intellectual Property Rights contained in the Feedback if any.

7. Liability

7.1. **Limitation of Liability.** UNLESS EXPLICITLY STATED OTHERWISE IN THE AGREEMENT, IN NO EVENT WILL GRADIUM'S (TOGETHER WITH ALL OF ITS AFFILIATES) AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THE AGREEMENT (REGARDLESS OF THE NUMBER OF INDIVIDUAL INCIDENTS GIVING RISE TO LIABILITY) EXCEED ONE HUNDRED PERCENT (100%) OF THE TOTAL AMOUNT PAID BY CLIENT HEREUNDER FOR THE SERVICES GIVING RISE TO THE LIABILITY IN THE SIX (6) MONTHS PRECEDING THE FIRST INCIDENT OUT OF WHICH THE LIABILITY AROSE OR ONE-HUNDRED (100) EUROS, WHICHEVER THE GREATER. THE ABOVE LIMITATIONS WILL APPLY WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY. HOWEVER, THE ABOVE LIMITATIONS WILL NOT LIMIT CLIENT'S PAYMENT OBLIGATIONS UNDER SECTION 5 (FEES AND PAYMENT) OR CLAIMS FOR WHICH LIABILITY CANNOT BE LIMITED UNDER APPLICABLE LAWS.

7.2. **Exclusion of Consequential and Related Damages.** IN NO EVENT WILL GRADIUM HAVE ANY LIABILITY TO CLIENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS, FOR ANY INDIRECT DAMAGES INCLUDING LOST PROFITS, LOST MARGIN, LOST OPPORTUNITIES, INTERRUPTION OF BUSINESS, LOSS OF DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, COVER, OR PUNITIVE DAMAGES, WHETHER AN ACTION IS IN CONTRACT OR TORT AND REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF GRADIUM HAS BEEN ADVISED OF THE POSSIBILITY OF THESE TYPES OF DAMAGES OR A GRADIUM'S REMEDY OTHERWISE FAILS OF ITS ESSENTIAL PURPOSE. THE FOREGOING DISCLAIMER WILL NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAWS.

8. Warranties

- 8.1. **Mutual Warranties.** Each Party represents and warrants to the other Party that:
- Any individual signing on behalf of each Party has the legal power and authority to enter into the Agreement on behalf of said Party.
 - Is duly organized, validly existing, and in good standing under the Applicable Laws of the jurisdiction of its origin.
- 8.2. **Client Warranty.** Client represents and warrants that:
- It always has all the rights, licenses, consents, authorizations, permissions, power and/or authority necessary to provide to GRADIUM any Input and create

any Output or Voice Reproduction based on Client's Input, and to grant the rights necessary to GRADIUM on Client Data pursuant to the Agreement.

- b. Client Data do not and will not infringe any third party right, including Intellectual Property Rights, data protection or privacy rights.
- c. Client and users shall use the Services in accordance with the Agreement and Applicable Laws.
- d. The warranties given to a Client's customer pursuant to the Client Service and covering the subcontracted Services do not go beyond the ones given in the Agreement; any such warranty, promises or commitments given or made by Client are not binding for GRADIUM and are at the sole responsibility of Client.

8.3. GRADIUM Warranties. GRADIUM represents and warrants to Client that during the Term, GRADIUM:

- a. will not materially reduce the general functionality of the Services and the overall effectiveness of the Security Measures.
- b. Takes industry standard steps to help ensure when used in accordance with the Agreement, the Services do not include Malicious Code.

GRADIUM shall not be liable for any breach of the warranties set forth in this Section if such non-compliance results from:

- a. Services degradation or suspension as a result of Client exceeding any applicable limits set forth under the Agreement.
- b. Client's breach of the Agreement or use of the Services not in compliance with the Agreement or Documentation.
- c. Client's failure to configure the Services, and Client Environment in accordance with the Documentation.
- d. Failures of, or issues with, Client Environment and Client Service.
- e. Force Majeure Events.
- f. Unavailability of the Services that result from equipment and/or software of third parties where such equipment and/or software is not within the control or responsibility of GRADIUM.
- g. GRADIUM's suspension or termination of the Services pursuant to the Agreement.

Without limiting GRADIUM's obligations pursuant to Section 2 (GRADIUM's Obligations), Client's exclusive remedies for a breach of a warranty in this Section (GRADIUM Warranties) shall be to exercise the express rights described in Sections 4.2 (Termination for Cause) and 4.4 (Refund or Payment upon Termination).

8.4. Disclaimers. EXCEPT AS EXPRESSLY PROVIDED IN THIS SECTION OR IN THE AGREEMENT, THE SERVICES ARE PROVIDED "AS IS" AND GRADIUM MAKES NO WARRANTY OR GUARANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, OR OTHERWISE, AND GRADIUM SPECIFICALLY DISCLAIMS ALL WARRANTIES, WHETHER IMPLIED, EXPRESS, OR STATUTORY, INCLUDING ANY IMPLIED WARRANTY OF TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAWS. EXCEPT AS OTHERWISE INDICATED IN THE AGREEMENT, GRADIUM DISCLAIMS ANY WARRANTY THAT THE OPERATION OF THE GRADIUM SOFTWARE OR THE SERVICES WILL BE ERROR-FREE, ACCURATE OR UNINTERRUPTED.

9. Indemnification

- 9.1. Indemnification by Client.** Client will indemnify and defend GRADIUM against any and all third party claims (subject that such claims are not initiated by GRADIUM's Affiliates), suits or proceedings (each a "**GRADIUM Covered Claim**") and all

resulting judgments, liabilities, awards, damages, and costs, including reasonable attorneys' fees and expenses, finally awarded by a court of competent jurisdiction, or included as part of a final settlement payable to a third party based on a claim arising out of or in connection with:

- a. Input.
- b. Client's violation of its warranties set forth in Section 8.2 (Client Warranties).
- c. Client's use of the Services in breach of the Agreement and/or Applicable Laws.

Provided GRADIUM (x) promptly gives Client written notice of the GRADIUM Covered Claim; (y) gives Client sole control of the defense and settlement of the GRADIUM Covered Claim (except that Client may not settle any GRADIUM Covered Claim unless it unconditionally releases GRADIUM of all liability related to the GRADIUM Covered Claim); and (z) give Client all reasonable assistance in connection with the defense or settlement of such GRADIUM Covered Claim, at Client's expense. The above defense and indemnification obligations do not apply to the extent a GRADIUM Covered Claim arises from GRADIUM's breach of the Agreement.

9.2. **Additional Indemnities.** For purposes of this Section 9 (Indemnification), a GRADIUM Covered Claim shall include a claim against GRADIUM, GRADIUM's Affiliates, and GRADIUM's or its Affiliates' officers, directors, and employees.

10. **Assignment.** Neither Party may assign any of its rights or obligations under the Agreement, whether by operation of law or otherwise, without the other Party's prior written consent (not to be unreasonably withheld) provided, however, GRADIUM may assign the Agreement in its entirety, without Client's consent (a) to its Affiliates or (b) in connection with a merger, acquisition, corporate reorganization, or sale of all or substantially all of its assets. The Agreement will bind and inure to the benefit of the Parties, their respective successors, and permitted assigns.

11. Manner of Giving Notice

11.1. **Updates.** All updates to any cross-referenced document or policy will be posted online to its designated address. Updates to the Documentation and Security Measures will be effective upon notification.

11.2. **Notices.** Any notice, request, or approval about the Agreement must be in writing and sent to the notice address set out in the preamble or the subscription process, unless explicitly provided otherwise in the Agreement. Notices will be deemed given (i) upon confirmed delivery if by email, registered or certified mail, or personal delivery; or (ii) two days after mailing if by overnight commercial delivery.

12. Confidentiality

12.1. **Confidential Information.** "Confidential Information" means all information disclosed by a Party ("**Disclosing Party**") to the other party ("**Recipient**"), whether orally or in writing, that is designated as confidential or, given the nature of the information and the circumstances of disclosure, should be understood to be confidential. Client's Confidential Information includes but is not limited to Client Data and Output. GRADIUM's Confidential Information includes but is not limited to the Services, the Models, the API and the Documentation. Confidential Information of each Party includes but is not limited to the non-public terms and conditions of the Agreement, pricing, business and marketing plans, technology and technical information, developments, product plans and designs, and business processes disclosed by each Party in connection with the Agreement and more generally any information exchanged pursuant to the Agreement. Confidential Information does not include information that: (i) is at the time of disclosure, or later becomes, generally

known to the public through no fault of Recipient; (ii) was known to the Recipient with no obligation of confidentiality prior to disclosure by Disclosing Party, as proven by records of Recipient; (iii) is disclosed to Recipient by a third party who did not directly or indirectly obtain the information subject to any confidentiality obligation; or (iv) is at any time independently developed by Recipient without use of Disclosing Party's Confidential Information as proven by records of Recipient.

12.2. Protection of Confidential Information. Except as provided in Section 12.3 (Compelled Disclosure) Recipient shall not disclose or otherwise make available any Confidential Information of Disclosing Party to anyone except those of its employees, directors, attorneys, agents and consultants who: (i) need to know the Confidential Information in connection with the purpose of the Agreement and (ii) who have previously agreed to be bound by confidentiality obligations no less stringent than those in the Agreement. Each Party shall (i) safeguard all Confidential Information of the other Party with at least the same degree of care (but no less than reasonable care) as it uses to safeguard its own Confidential Information and (ii) not use any Confidential Information of the other Party for any purpose outside the scope of the Agreement.

12.3. Compelled Disclosure. If Recipient is compelled by law to disclose Confidential Information of Disclosing Party, then to the extent legally permitted, Recipient shall provide Disclosing Party with prior notice of the compelled disclosure and reasonable assistance, at Disclosing Party's cost, if Disclosing Party wishes to contest the compelled disclosure. Any compelled disclosure shall be limited to the extent required and shall be subject to confidentiality protections to the extent practicable. If Recipient is compelled by law to disclose Disclosing Party's Confidential Information as part of a proceeding to which Disclosing Party is a party, and Disclosing Party is not contesting the disclosure, Disclosing Party will reimburse Recipient for its reasonable cost of compiling and providing secure access to that Confidential Information.

12.4. Duration of confidentiality obligations. Confidentiality obligations set forth under this Section shall apply for five (5) years after the end of the Agreement.

13. Export regulations. Client acknowledges and expressly agrees that the Services provided by GRADIUM may be subject to applicable export control and sanctions laws and regulations, including but not limited to those imposed by the European Union, the United States, the UK, France and other jurisdictions. By accessing or using the Services, Client represents and warrants that:

- it is not located in, organized under the laws of, or a resident of a country or territory subject to comprehensive sanctions or embargoes, including but not limited to Cuba, Iran, North Korea, Syria, or the Crimea, Donetsk, and Luhansk regions of Ukraine;
- it is not identified on any government-issued list of prohibited or restricted parties;
- it shall not, directly or indirectly, use, export, re-export, transfer, divert, or disclose any portion of the Services or related technology:
 1. to or for the benefit of any entity or individual prohibited under applicable export control or sanctions laws;
 2. to or for the benefit of any entity or individual located in, organized under the laws of, or a resident of a country or territory subject to comprehensive sanctions or embargoes, including but not limited to Cuba, Iran, North Korea, Syria, or the Crimea, Donetsk, and Luhansk regions of Ukraine; or
 3. in any manner that would cause GRADIUM or its Affiliates to be in violation of applicable export control or sanctions laws.

14. **Anti-corruption.** Client shall not take any action that would be a violation of any Applicable Laws that prohibit the offering, giving, promising to offer or give, or receiving, directly or indirectly, money or anything of value to any third party to assist GRADIUM or Client in retaining or obtaining business. Examples of these kinds of laws include the U.S. Foreign Corrupt Practices Act, the French Act Sapin 2 and the UK Bribery Act 2010.

15. **Right violation notification.** If anyone believes that any content on the Services infringe any Intellectual Property Right, or privacy right that they own or control, they may notify GRADIUM as follows:

By Certified Mail:

GRADIUM

151bis, rue Saint-Honoré, 75001 Paris, France

By Email: legal@gradium.ai

Please see Section 512(c)(3) of the Digital Millennium Copyright Act (DMCA) for the requirements of a proper notification. Failure to comply with all of the requirements of Section 512(c)(3) of the DMCA may result in the notice not being effective. Any knowingly material misrepresentation that any activity or material on the Services is infringing may give rise to liability and right for GRADIUM to claim damages.

16. **Governing Law and Jurisdiction.** The Agreement shall be governed by and construed in accordance with the laws of France excluding rules governing conflict of law and choice of law. The civil courts in Paris, France shall have exclusive jurisdiction to adjudicate any dispute arising out of the Agreement. The Parties agree that the UN Convention on Contracts for the International Sale of Goods (Vienna, 1980) and the Uniform Computer Information Transaction Act or similar federal or state laws or regulations shall not apply to the Agreement nor to any dispute or transaction arising out of the Agreement.

17. **Subcontracting.** Subject to the Data Processing Agreement, Client authorizes GRADIUM to subcontract part or all the Services, provided that GRADIUM shall remain liable for the performance of the Services in accordance with the Agreement and for any breach of the Agreement caused by its subcontractors.

18. **Publicity.** If explicitly indicated and authorized by Client, GRADIUM may use Client's name and logo and general description of Client's relationship with GRADIUM in press releases and other marketing materials and appearances.

19. **Force Majeure.** Neither Party will be liable for a delay or failure to perform its obligations of this Agreement if caused by a Force Majeure Event. However, this Section does not excuse Client's obligations to pay Fees.

20. **Relationship of the Parties.** The parties are independent contractors. The Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship between the Parties.

21. **Third-Party Beneficiaries.** There are no third-party beneficiaries under the Agreement.

22. **Entire Agreement.** The Agreement supersedes all prior and contemporaneous agreements, proposals, or representations, written or oral, concerning its subject

matter. In the event of any conflict or inconsistency among the following, the order of precedence shall be: (i) the Terms of Service and the Data Processing Agreement, and (ii) the Documentation and any document or policy cross-referenced in the Agreement. Any term or condition stated in a Client's purchase order or other Client order documents is void.

23. **Modification.** To the extent permitted by Applicable Laws, GRADIUM may update the Terms of Service from time to time, including but not limited to changes to reflect changes of the Services, including to introduce new features or functionality or improve Services quality, changes to Applicable Laws or security or safety reasons. GRADIUM will give Client at least thirty (30) days advance notice of changes to these Terms of Service that materially adversely impact Client via email. When Client's subscription is on yearly basis, the revised Terms of Service will apply, as indicated in GRADIUM's notification, either at the renewal of the next subscription period, or after a thirty (30) day prior notice. Client may oppose the notified changes to the Terms of Service in such delay and terminate the Agreement within this period. All other changes will be effective as soon as GRADIUM notify them to Clients.
24. **Waiver.** No failure or delay by either Party in exercising any right under the Agreement will constitute a waiver of that right.
25. **Severability.** If any provision of the Agreement is held by a court of competent jurisdiction to be contrary to law, the provision will be deemed null and void, and the remaining provisions of the Agreement will remain in effect.
26. **Interpretation.** All reference in the Agreement to "including" means "including but not limited to". All references to hours, days, months or years refer to calendar hours, days, months or years unless explicitly stated otherwise.
27. **Survival.** Any term or condition that by its nature is clearly intended to survive the expiration or termination of the Agreement, shall survive any expiration or termination of the Agreement, including but not limited to Sections 3.4 (Usage Restrictions), 4.3 (Effect of Termination), 4.4 (Refund or Payment upon Termination), 5 (Fees and Payment), 6 (Licenses and Intellectual Property Rights), 7 (Liability), 9 (Indemnification), 12 (Confidentiality), and 16 (Governing Law and Jurisdiction).
28. **Signature.** The Agreement shall be considered signed and accepted by the Client by the subscription and/or use of the Services.

Exhibit 1 - Data Processing Agreement

This Data Processing Agreement governs the Processing of Personal Data carried out by GRADIUM as part of its provision of the Services to Client, as Data Processor.

1. DEFINITIONS

All capitalized terms used in this Data Processing Agreement will have the following meanings.

- Client Personal Data means any Personal Data Processed by GRADIUM as a Data Processor on behalf of Client or Third-Party Controller.
- Data Controller, Data Processor, Data Security Breach, Data Subject, Personal Data, Processing, and Supervisory Authority shall have the meaning given to them under European Data Protection Laws.
- Data Processing Agreement means this document.
- European Data Protection Laws means the General Data Protection Regulation (EU) 2016/679 ("GDPR") and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC), their national implementations in the EEA, including the European Union, and all other data protection laws of the EEA, the United Kingdom ("UK"), and Switzerland, each as applicable, and as may be amended or replaced from time to time.
- International Data Transfer means any transfer of Personal Data to a Restricted Country.
- Non-EEA Country means any country located outside of the European Economic Area (EEA), regardless of whether it benefits from an adequacy decision from the European Commission.
- Restricted Country means any country located outside of the European Economic Area (EEA) and that does not benefit from an adequacy decision from the European Commission.
- SCC means the clauses annexed to the European Commission Implementing Decision 2021/914 of June 4th, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to the GDPR.
- Sub-Processor means any Data Processor appointed by GRADIUM.
- Third-Party Controller means a Data Controller for which Client is a Data Processor.
- UK Addendum means the addendum to the SCCs issued by the UK Information Commissioner under Section 119A(1) of the UK Data Protection Act 2018 (version B1.0, in force March 21, 2022).
- The terms "Share", and "Shared" shall have the same meaning given to them under the CCPA. The terms "Sell" and "Selling" shall have the meaning defined in Applicable Privacy Laws in the U.S.

All capitalized terms not defined herein shall have the meaning ascribed to them in the Terms of Service.

2. ROLE OF THE PARTIES AND PURPOSE OF THE PROCESSING

Client is the Data Controller and GRADIUM is the Data Processor with respect to the Processing detailed in Appendix 1. GRADIUM processes Client Personal Data on behalf of Client when Client uses the Services, as set out in Appendix 1.

If Client is a Data Processor on behalf of a Third-Party Controller, then Client shall act (i) as the single point of contact for GRADIUM; (ii) obtain all necessary authorizations from such Third-Party Controller; (iii) ensure that the Third Party Controller provided notice and obtained any consents necessary for Processing by Service Provider as set forth in this Data

Processing Agreement; and (iv) undertakes to issue all instructions and exercise all rights on behalf of such other Third-Party Controller.

3. MUTUAL OBLIGATIONS

Each Party shall comply with their respective obligations under the Applicable Privacy Laws and shall not, by any act or omission, cause the other to be in breach of any such obligations under the Applicable Privacy Laws.

4. OBLIGATIONS OF DATA PROCESSOR

The Parties agree that the subject matter, nature, purpose and duration of Processing performed by GRADIUM under this Data Processing Agreement as Data Processor, the type of Personal Data, and categories of Data Subjects, are as described in this Agreement and in Appendix 1.

When providing the Services, GRADIUM makes the following commitments as Data Processor:

- a) GRADIUM shall process Client Personal Data only on Client's documented lawful instructions as set out in this Data Processing Agreement or as otherwise necessary to provide the Services. In this regard, such instructions may be provided by Client via the use of the Services and via this Data Processing Agreement. GRADIUM shall process Client Personal Data for no purpose other than as authorized under this Data Processing Agreement, unless required to do so by applicable laws. In such a case, GRADIUM shall promptly inform Client of such legal requirement, unless prohibited to do so by applicable laws.
- b) GRADIUM shall ensure that GRADIUM's staff members have committed themselves to confidentiality of Client Personal Data, that staff members Processing Client have a need to know the relevant Client Personal Data for the provision of the Services and that Sub-Processors are under confidentiality obligations substantially similar to the confidentiality obligations imposed on GRADIUM pursuant to the Data Processing Agreement.
- c) Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, GRADIUM shall implement and maintain the Security Measures to protect Client Personal Data from any Data Security Breach. The Security Measures implemented by GRADIUM under this Data Processing Agreement are listed in Appendix 3. Client acknowledges that such Security Measures are subject to technical progress and development and that GRADIUM may update them from time to time, provided that such updates do not materially decrease the overall security of the Processing governed by this Data Processing Agreement. GRADIUM shall provide Client with reasonable and timely assistance to allow Client to comply with its obligations under Article 32 of the GDPR.
- d) Taking into account the nature of the Processing and the information available to GRADIUM, GRADIUM shall notify Client without undue delay and not later than forty-eight (48) hours after having become aware of a Data Security Breach affecting Client Personal Data. GRADIUM shall cooperate with Client, and if requested by Client, GRADIUM shall (i) provide Client with reasonable information about the Data Breach in its possession such as the nature of the personal data affected, or the cause and origin of the Data Security Breach, and (ii) provide reasonable assistance to Client to mitigate or remediate the Data Security Breach.

GRADIUM has no obligation to assess Client Personal Data in order to identify if they are subject to any specific legal requirements.

Upon Client's written request, taking into account the nature of the Processing and the information available to GRADIUM, this latter shall provide Client with commercially reasonable assistance to conduct a data protection impact assessment and to conduct a prior consultation with a Supervisory Authority when required by Applicable Privacy Laws and reasonably requested by Client, solely with respect to the Processing and Client Personal Data.

Taking into account the nature of the Processing, GRADIUM shall provide Client with commercially reasonable assistance (by appropriate technical and organizational measures) with respect to the fulfilment of Client's obligation to respond to requests from Data Subjects to exercise their rights under the Applicable Privacy Laws (a "Data Subject Request"). In the event GRADIUM receives a Data Subject Request directly from a Data Subject, it shall (unless prohibited by applicable laws) promptly notify Client of such Data Subject Request, and direct the Data Subject to Client. Client will be responsible for responding to any such Data Subject Request.

GRADIUM shall immediately inform Client if, in its opinion, Client's Processing instruction infringes the Applicable Privacy Laws. In such event, GRADIUM is entitled to refuse to perform the Processing of Client Personal Data that it believes to be in violation of the Applicable Privacy Laws.

5. USE OF SUB-PROCESSORS

Client hereby provides a prior and general authorization allowing GRADIUM to appoint any Sub-Processors to assist GRADIUM in the provision of the Services and in the Client Personal Data Processing described in Appendix 1, in accordance with the terms provided in this Data Processing Agreement.

GRADIUM commits that Sub-Processors (i) are to fulfil obligations at least equivalent to those set out in this Data Processing Agreement with respect to Personal Data protection; (ii) provide guarantees regarding Personal Data protection at least equivalent to those presented by the measures implemented by GRADIUM. GRADIUM remains liable to Client for the fulfilment by the Sub-Processors of their contractual obligations towards GRADIUM.

Client hereby agrees that GRADIUM may appoint Sub-Processors from the list of Sub-Processors in Appendix 2 of this Data Processing Agreement. GRADIUM shall update the list of any Sub-Processor to be appointed at least thirty (30) days prior to the date on which the Sub-Processor shall commence the Processing of Client Personal Data.

Client may object in writing to GRADIUM's appointment of a new Sub-Processor within fifteen (15) days of such notice, provided that such objection is based on reasonable and substantiated grounds relating to compliance with Applicable Privacy Laws. If Client provides observations during this fifteen (15) days period, GRADIUM and Client will consult and negotiate in good faith to find a mutually acceptable resolution to address any objections raised by Client. If GRADIUM chooses to retain the Sub-Processor, GRADIUM shall inform Client at least thirty (30) days before authorizing the Sub-Processor to Process Client Personal Data, and either party may immediately discontinue providing or using the relevant parts of the Services, as applicable, and may terminate the relevant parts of the Services within thirty (30) days.

6. INTERNATIONAL TRANSFER OF CLIENT PERSONAL DATA

Unless GRADIUM otherwise explicitly commits not to transfer any Client Personal Data to a Non-EEA Country, Client authorizes GRADIUM to transfer Client Personal Data directly or indirectly to any country deemed to have an adequate level of data protection by the European Commission. Client also authorizes GRADIUM to perform International Data Transfers directly or indirectly to a Restricted Country (a) on the basis of adequate safeguards in accordance with Applicable Privacy Laws, including but not limited to the EU-US Data Privacy Framework, or (b) pursuant to the SCCs, as the case may be the UK Addendum if applicable, or any other transfer mechanism allowed pursuant to Applicable Privacy Laws.

This Section only applies if Client is located in a Restricted Country. By accepting this Data Processing Agreement, GRADIUM and Client conclude Module 4 (Processor-to-Controller) of the SCCs where Client is a Data Controller, and Module 3 (Processor-to-Processor) of the SCCs to the extent Client is a Data Processor on behalf of a Third-Party Controller, which are hereby incorporated and completed as follows and apply to any International Data Transfer conducted by GRADIUM acting as a Data Processor:

- The “data exporter” is GRADIUM and the “data importer” is Client.
- The optional docking clause in Clause 7 is not implemented
- Option 2 of Clause 9(a) is implemented and the time period therein is specified in Section 5 above.
- The optional redress clause in Clause 11(a) is struck.
- Option 2 in Clause 17 is implemented and the governing law in Clause 17 is the law of France.
- The courts in Clause 18 are the Courts of France.
- Annex I and II to the Modules 3 and 4 of the SCCs are Appendices 1 and 3 to this Data Processing Agreement respectively.

If GRADIUM has explicitly committed not to transfer any Client Personal Data to a Non-EEA Country, the aforementioned parts of this Section shall not apply and GRADIUM undertakes not to transfer any Client Personal Data to a Non-EEA Country.

7. AUDIT

Documentary audit. Upon Client's written request, GRADIUM will make available all documents and information to demonstrate that the Processing carried out by GRADIUM as Data Processor complies with this Data Processing Agreement in a timely manner, to the extent that is commercially reasonable and required by the Applicable Privacy Laws, subject to confidentiality and trade secrets. Documentary audits can be requested maximum once per year.

Onsite audit. For this Section, “Auditor” will have the meaning of either Client or the third-party auditor mandated by Client under this Section to conduct an audit or inspection as set out in this Section solely with respect to the Processing and compliance with this Data Processing Agreement. Only to the extent Client cannot reasonably be satisfied with GRADIUM's compliance with this Data Processing Agreement through the exercise of the documentary audit set out in this Section, Auditor may conduct up to one (1) onsite audit per year to verify GRADIUM's compliance with this Data Processing Agreement, under the conditions defined below:

1. Client demonstrates that Auditor is subject to strict confidentiality obligations.
2. Client demonstrates that Auditor is independent, impartial and with expertise in data protection, and is not a competitor of GRADIUM.

3. The procedure described below is followed:
 1. Client gives GRADIUM a thirty (90)-days prior written notice of such audit or inspection (hereafter "Audit").
 2. During this thirty (90)-days period, Client and GRADIUM mutually agree in writing upon the scope (which must be limited to Processing operations related to the provision of Services to Client), timing and duration and starting date of the Audit.
 3. Client ensures that the Audit will not impact GRADIUM's organization or GRADIUM's activities, and is carried out during regular business hours.
 4. GRADIUM will not give access to its premises for the purposes of the Audit:
 1. To an Auditor's employee who does not provide GRADIUM with reasonable evidence of identity and authority.
 2. To any Auditor's employee who requests access to GRADIUM's premises outside regular business hours.
 5. GRADIUM will not give access to premises other than its corporate site; for example, GRADIUM will not provide access to Sub-Processors' premises.
 6. The Audit is conducted by the Auditor in a reasonable manner and in good faith, an identical copy of the Audit report shall be given to both Parties following the completion of the Audit. Each Party may make observations regarding the Audit report.
 7. All costs relative to the Audit will be at the charge of Client unless the Audit reveals a breach by GRADIUM of this Data Processing Agreement or Applicable Privacy Laws.

8. OBLIGATIONS OF DATA CONTROLLER

Client agrees and commits to the following:

- Client is responsible for compliance with the requirements of Applicable Privacy Laws applicable to Data Controllers. In particular, Client guarantees that the Processing is compliant with the Applicable Privacy Laws and in particular that the Data Subjects are informed of the Processing via an appropriate information notice and have given their consent as necessary to comply with Applicable Privacy Laws, in particular where the Processing described in Appendix 1 includes sensitive data or special categories of data within the meaning of Applicable Privacy Laws.
- Client is solely responsible for the accuracy and appropriateness of Personal Data and the means by which such Personal Data is acquired in compliance with the Applicable Privacy Laws. Client is solely responsible for providing GRADIUM with instructions that comply with this Data Processing Agreement and the Applicable Privacy Laws.
- Client undertakes to document in writing any additional instructions regarding the Processing by GRADIUM.

9. RETURN AND DESTRUCTION OF PERSONAL DATA

Upon the termination of Client's access to and use of the Services, GRADIUM will, up to forty-five (45) days following such termination, delete or return to Client, at Client's choice, all Client Personal Data detained by GRADIUM except as otherwise authorized under the Terms of Service. Client acknowledges and accepts that Client Personal Data will no longer be accessible upon the expiry of the forty-five (45) day period.

Without prejudice of any Zero Data Retention feature implemented as applicable, GRADIUM may retain Client Personal Data to the extent required by applicable law but only to the

extent and for such period as required by such law and always provided that GRADIUM shall ensure the confidentiality of all such Client Personal Data.

10. California Provisions

These CCPA Terms apply when the California Consumer Privacy Act of 2018, Cal. Civ. Code §§1798.100–1798.199.100, as amended, and the CCPA regulations, Cal. Code Regs. §§7000–7304 (together, the “CCPA”) applies to Client’s use of the Services to process the Personal Information contained in Client Personal Data and Account Data.

Where the CCPA applies, GRADIUM acknowledges that it does not receive Personal Data as consideration for any Services provided to Client. GRADIUM: (i) is responsible for compliance with its obligations under this Data Processing Agreement, (ii) is responsible for compliance with its obligations as a service provider under the CCPA, and (iii) shall provide the same level of privacy protection as required by the CCPA. GRADIUM shall notify Client if it reasonably determines that it cannot meet its obligations under the CCPA, and in such circumstances, and upon provision of notice to GRADIUM, Client shall be entitled to take reasonable and appropriate steps to remediate unauthorized use of Personal Data. GRADIUM must not process the Personal Data for any purpose other than for the purpose of performance of the Agreement, except where and to the extent permitted by the CCPA.

GRADIUM shall not: (i) Sell or Share Client Personal Data; (ii) retain, use, or disclose Client Personal Data for any purpose other than for the purpose of performance of the Services except as expressly permitted under the CCPA; (iii) retain, use, or disclose Client Personal Data with Personal Data obtained from, or on behalf of, sources other than Client, except as expressly permitted under the CCPA; or (iv) process Client Personal Data for targeted and/or cross context behavioral advertising. GRADIUM certifies that it understands the restrictions set out in this Section and will comply with them. Solely for the purpose of the CCPA, GRADIUM shall promptly notify Client if it determines that it can no longer meet its obligations under the CCPA.

11. PROCESSING OF GRADIUM AS DATA CONTROLLER

GRADIUM processes Personal Data as Data Controller for the purposes set forth in GRADIUM’s Privacy Policy available at the following link and any succeeding link: dpo@gradium.ai.

Unless the Zero Data Retention feature is applicable or Client objected to the Processing, Client also authorizes GRADIUM and its Affiliates, and any party replacing GRADIUM to the Agreement, to reuse Client Personal Data for the purpose of improving current and future Services, and training any AI model or product as an independent Data Controller.

GRADIUM undertakes to comply with the Applicable Privacy Laws in relation to all Processing for which it is classified as Data Controller. The information related to such Processing are set forth in Gradium’s Privacy Policy and Client undertakes to direct all its users of the Services to this Privacy Policy.

12. DURATION

This Agreement will remain in force as long as the Client uses the Services.

13. JURISDICTION AND GOVERNING LAW

Any dispute arising from this Data Processing Agreement will be resolved by the competent courts of Paris, France in accordance with the Terms of Service.

This Data Processing Agreement is governed by the laws of France

Appendix 1

Detail of Processing

1. PARTIES

Client as Data Controller or Data Processor of a Third-Party Controller, and data importer for the purposes of SCCs as applicable.

GRADIUM as Data Processor and data exporter for the purposes of SCCs as applicable.

2. DURATION OF PROCESSING

If the Zero Data Retention feature is not activated, GRADIUM shall store Client Personal Data as Data Processor solely for the duration of the Services.

If the Zero Data Retention feature is applicable, GRADIUM shall not store any Input and Output after their respective ingestion and generation for a duration longer than necessary to the generation of Output and shall not be retained further. Notwithstanding the foregoing, GRADIUM may retain Voice Sample recordings that are (i) explicitly and separately provided by Client for the sole purpose of Voice Reproduction, and (ii) reasonably necessary to deliver the Voice Reproduction pursuant to the Services.

3. SUBJECT-MATTER AND NATURE OF PROCESSING

Generation of Output and Voice Reproduction based on Client's Input at Client's request.

4. FREQUENCY OF THE PROCESSING

On a continuous basis.

5. PURPOSE OF PROCESSING

The purpose of the Processing of Client Personal Data is provision of the Services.

6. DATA SUBJECTS

Data subjects whose characteristics, such as their voice, are present in Client's Input and, as applicable, reproduced in Output.

7. CATEGORIES OF PERSONAL DATA

Voice input, voice recordings, text input, or other content included in Client's Input, and text or voice Output generated by GRADIUM based on Input provided by Client.

8. SENSITIVE DATA

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.

Appendix 2

List of Subprocessors

The list of Sub-Processors is available on our website <https://gradium.ai/>

Appendix 3

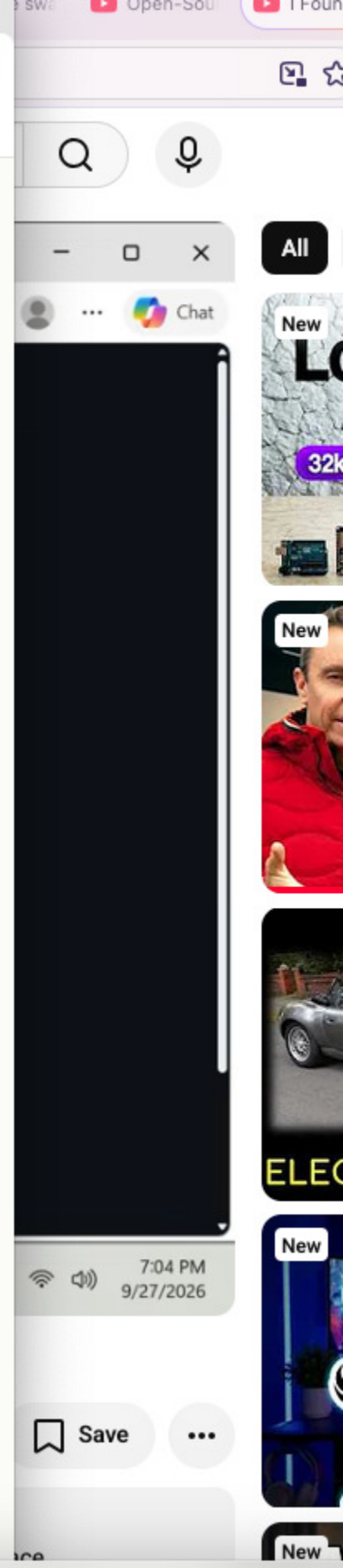
Security Measures

GRADIUM implements the following Security Measures:

- Real-time monitoring systems are implemented across the organization's IT infrastructure to detect, log, and alert on suspicious or unauthorized activity. Alerts generated by the monitoring tools are reviewed promptly by the IT security team to ensure rapid response and incident containment.
- All internal and external web traffic is encrypted using HTTPS with Transport Layer Security (TLS), ensuring that data transmitted between clients, servers, and third-party services remains confidential and protected against interception or tampering. This encryption protocol provides robust authentication and integrity assurance, preventing man-in-the-middle attacks and safeguarding personal and business-critical information in transit.
- GRADIUM uses a virtual private cloud (VPC) which isolates GRADIUM's cloud and traffic from the open web and whose entry points are controlled by GRADIUM via API to further strengthen access control and protect internal systems from external exposure.

As GRADIUM develops and expands, more organisational and technical measures will be implemented. Together, these measures form a cohesive security framework designed to maintain the confidentiality, integrity, and availability of data while supporting GDPR compliance.

All the security measures are listed at trust.gradium.ai.



Enable PAYG

advancedclearingenergetics@gmail.com

PAYG

Pay for what you use. Billed monthly or drawn from your credits.

Price

Pay-As-You-Go

The next invoice will be triggered after €10 of usage.

Billing information

Edit

Richard Flook Limited
29 Chemin du Bout des Pres
Issigeac 24560
FR

Payment methods

Add payment method



Card Payment
****-8118

Gift code (optional)

☐ Allow the use of your API calls to train Mistral's AI models.
By allowing us to train our models with your data, you help improve the performance of our models for you and for all our users. If you disable this option, your new interactions, or those of your users, will not be used to train our models. [Learn more](#)

☒ I accept the Mistral AI [Terms of Service](#) and [Privacy Policy](#).

Subscribe

Screenshot



Mistral AI

Pay-as-you-go is now enabled on your account

To: Richard Flook



Richard Flook Limited - Pay-as-you-go is now enabled on your account

Hello Richard,

Pay-as-you-go has been enabled on your account for the organization Richard Flook Limited. You can now use the API beyond the included monthly usage, billed monthly or drawn from your credits.

Happy coding!

[Access Studio](#)

Right of withdrawal: You acknowledge that Services will be provided to you before the expiration of the legal withdrawal period of fourteen days from your subscription. By subscribing to our services, you expressly waive your right of withdrawal.

Thanks,
The Mistral AI Team

Need help?

Check the [Help Center](#) for answers to your most common questions. You can also reach out to the Support team directly from [Studio](#).



Mistral AI is a French company incorporated in Paris, under number 952 418 325, having its registered offices at 15 rue des Halles, 75001 Paris ("We", "Us" or "Mistral AI").

© 2026 Mistral AI | [Privacy policy](#)

