Data Processing Agreement (DPA)

Between:

Data Controller: [CLIENT NAME] ("Controller")
Data Processor: Omnera Data Group Ltd ("Processor")

Effective Date: the date both parties sign, or the date the Controller accepts Omnera's Terms of Service if earlier.

1. Definitions

- **Personal Data**: Any information relating to an identified or identifiable natural person as defined under UK GDPR.
- **Processing**: Any operation performed on Personal Data, including collection, storage, retrieval, and erasure.
- **Subprocessor**: Any third party engaged by the Processor to process Personal Data on behalf of the Controller.
- **Agreement**: Omnera's Terms of Service, together with any order form, quote or contract between the parties for the services.

2. Scope and Purpose

2.1 The Processor shall process Personal Data solely for the purpose of providing the Omnera market intelligence platform as described in the Agreement.

2.2 Categories of Personal Data processed:

- Business contact information (names, email addresses, phone numbers)
- Professional credentials (registry identification numbers)
- Business addresses and territory assignments
- User session data for security and audit purposes
- Platform usage data (search queries, export records)
- Company officer information (names, roles, appointment dates)

2.3 Categories of Data Subjects:

- Healthcare practitioners and clinic staff
- Sales representatives of the Controller
- Key Opinion Leaders (KOLs)
- Company directors and officers (sourced from public registries)
- Platform users (Controller's authorised team members)

3. Data Processing Obligations

3.1 Processor Obligations

The Processor shall:

a) Process Personal Data only on documented instructions from the Controller, unless required by UK law;

b) Ensure that persons authorised to process Personal Data have committed to confidentiality;

c) Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk (see Section 5);

d) Engage another processor only as set out in Section 9;

e) Assist the Controller in responding to Data Subject requests;

f) Delete or return all Personal Data upon termination of services, at the Controller's choice;

g) Make available all information necessary to demonstrate compliance and allow for audits.

3.2 Controller Obligations

The Controller shall:

a) Ensure lawful basis for processing under UK GDPR Article 6;

b) Provide documented instructions for data processing;

c) Notify the Processor of any Data Subject requests received directly.

4. Data Location and Transfers

4.1 Primary Data Location

All Personal Data is stored within the European Union.

Service	Provider	Data Location
Primary Database	Render PostgreSQL	Frankfurt, Germany (EU)
Application Hosting	Render	Frankfurt, Germany (EU)
Cache Layer	Render Redis	Frankfurt, Germany (EU)
File Storage	Cloudflare R2	European Union

Note: the EU is covered by the UK's adequacy regulations, so these transfers comply with UK GDPR without additional safeguards.

4.2 International Transfers

The Processor transfers Personal Data outside the UK/EEA to the following services, with appropriate safeguards in place:

Service	Purpose	Transfer Mechanism
Anthropic (Claude API)	AI analysis of public clinic website content	SCCs via Anthropic's Data Processing Addendum (part of its Commercial Terms) + Data minimisation
Google Generative AI (Gemini)	Search query parsing and fallback AI analysis	SCCs + Data minimisation
Sentry (only when error monitoring is enabled)	Application error monitoring	SCCs via Sentry's Data Processing Addendum
Resend	Email delivery	SCCs
Calendly	Meeting scheduling	SCCs
Stripe	Payments, subscriptions and invoices	SCCs via Stripe's Data Processing Agreement

For all international transfers:

a) Standard Contractual Clauses (SCCs) approved by the UK ICO are in place; AND

b) Additional technical measures are implemented including data minimisation and transient processing.

4.3 Subprocessor Transfers

Any Subprocessor engaged must maintain data within the UK/EEA or have appropriate transfer mechanisms in place. See Annex A: Subprocessor List.

5. Security Measures

The Processor implements the following technical and organisational measures:

5.1 Access Control

- Role-based access control (RBAC) with principle of least privilege
- Multi-factor authentication (MFA) for administrative access
- Strong password policies (minimum 12 characters, complexity requirements)
- Account lockout after failed authentication attempts

5.2 Encryption

- Data at rest: AES-256 encryption (Render platform managed)

- Data in transit: TLS 1.2+ for all communications
- Database connections: SSL/TLS enforced

5.3 Network Security

- Virtual Private Cloud (VPC) isolation
- Web Application Firewall (WAF)
- DDoS protection
- Rate limiting on API endpoints

5.4 Monitoring & Logging

- Comprehensive audit logging of data access
- Security event monitoring
- Automated alerting for anomalous activity

5.5 Backup & Recovery

- Continuous point-in-time recovery on the managed PostgreSQL database, with a rolling recovery window of at least 3 days
- On-demand logical backups (taken before bulk data changes), retained for 7 days
- Backups are stored with the primary database in Render's Frankfurt, Germany (EU) region
- Restores are made to a separate database instance and verified before cut-over

6. Data Breach Notification

6.1 Notification Timeline

In the event of a Personal Data breach, the Processor shall:

a) Notify the Controller **without undue delay** and in any event **within 24 hours** of becoming aware of the breach;

b) Provide the following information:
- Nature of the breach
- Categories and approximate number of Data Subjects affected
- Categories and approximate number of Personal Data records affected
- Likely consequences of the breach
- Measures taken or proposed to address the breach

6.2 Controller Notification to ICO

The Controller acknowledges responsibility for notifying the Information Commissioner's Office (ICO) within 72 hours where required under UK GDPR Article 33.

7. Data Subject Rights

The Processor shall assist the Controller in fulfilling obligations to respond to Data Subject requests including:

- Right of access (Article 15)
- Right to rectification (Article 16)
- Right to erasure (Article 17)
- Right to restriction of processing (Article 18)
- Right to data portability (Article 20)
- Right to object (Article 21)

Response time: The Processor shall respond to Controller requests within **5 business days**.

8. Audit Rights

8.1 The Controller may conduct audits of the Processor's data processing activities with **30 days written notice**.

8.2 Audits shall be conducted during normal business hours and shall not unreasonably interfere with the Processor's operations.

8.3 The Processor shall provide access to:

- Relevant documentation and records
- Personnel involved in data processing
- Systems and facilities where processing occurs

8.4 Audit costs shall be borne by the Controller unless the audit reveals material non-compliance.

9. Subprocessors

9.1 The Controller provides general authorisation for the Processor to engage Subprocessors listed in **Annex A**.

9.2 The Processor shall:

- Notify the Controller of any intended changes to Subprocessors with **30 days notice**
- Ensure Subprocessors are bound by equivalent data protection obligations
- Remain fully liable for Subprocessor compliance

9.3 The Controller may object to a new Subprocessor within **14 days** of notification.

10. Term and Termination

10.1 This DPA shall remain in effect for the duration of the Agreement.

10.2 Upon termination:

- The Processor shall cease all processing within **30 days**
- Personal Data shall be deleted or returned at Controller's instruction
- The Processor shall provide written certification of deletion

10.3 Obligations regarding confidentiality and data security survive termination.

11. Liability

11.1 Each party shall be liable for damages caused by processing that infringes UK GDPR.

11.2 The Processor shall indemnify the Controller for any fines, penalties, or damages arising from the Processor's breach of this DPA or UK GDPR.

11.3 Liability caps as specified in the Agreement shall apply.

12. Governing Law

This DPA shall be governed by the laws of **England and Wales**.

Disputes shall be subject to the exclusive jurisdiction of the courts of **England and Wales**.

Signatures

For the Controller:

Name: _____

Title: _____

Date: _____

Signature: _____

For the Processor (OMNERA DATA GROUP LTD):

Name: Sebastian Farrant

Title: Director

Date: _____

Signature: _____

Annex A: Subprocessor List

The current Subprocessor List is available on request from info@omnera.co.uk.

Annex B: Technical and Organisational Measures

The Security Overview is available on request from info@omnera.co.uk. Section 5 of this DPA summarises the measures in place.

Document Version: 1.2
Last Updated: October 2026