BrandedAI
3rd Floor
86 - 90 Paul Street
London
EC2A 4NE
+44 7496 315485
scott@brandedai.net
www.brandedai.net

DATA PROCESSING AGREEMENT

GDPR Article 28 Compliant Data Processing Agreement

Data Controller: Chester Brethren Business Group (the "Controller")
Data Processor: SCEV Ltd t/a BrandedAI (Company Number: 10032640), 3rd Floor, 86-90 Paul Street, London, EC2A 4NE (the "Processor")
Date: 31st January 2026
Reference: This DPA supplements the Non-Disclosure Agreement dated 31st January 2026

---

1. Definitions

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person
Processing	Any operation performed on Personal Data (collection, storage, use, disclosure, deletion)
Data Subject	An individual whose Personal Data is processed
Sub-processor	Any third party engaged by the Processor to process Personal Data
Data Breach	A breach of security leading to accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of Personal Data

---

2. Scope of Processing

2.1 Subject Matter

The Processor shall process Personal Data solely for the purpose of providing the Chester Brethren Business Scorecard Platform, including:

- Collection and storage of business performance metrics
- Generation of aggregated reports and analysis
- Provision of AI-generated insights and recommendations
- Technical support and platform maintenance

2.2 Categories of Data Subjects

- Business owners and directors of participating Chester Brethren businesses
- Employees authorised to submit data on behalf of their businesses
- Chester Brethren representatives (Shane McEwan, Dylan Shaw)

2.3 Types of Personal Data

Category	Examples
Identity Data	Names, business names, job titles
Contact Data	Email addresses, telephone numbers
Business Data	EBITDA figures, sales data, targets, KPIs
Usage Data	Login timestamps, submission records

2.4 Duration of Processing

Processing shall continue for the duration of the service agreement and for 30 days thereafter to allow for data export and deletion, unless a longer retention period is required by law.

---

3. Processor Obligations

3.1 Processing Instructions

The Processor shall:

- Process Personal Data **only on documented instructions** from the Controller
- **Not process Personal Data** for any purpose other than providing the agreed services
- **Inform the Controller immediately** if any instruction appears to infringe data protection law
- **Not transfer Personal Data** outside the UK/EEA without prior written consent and appropriate safeguards

3.2 Confidentiality

The Processor shall:

- Ensure all personnel processing Personal Data are **bound by confidentiality obligations**
- **Limit access** to Personal Data to personnel who require it for service delivery
- **Not disclose** Personal Data to third parties except as permitted by this Agreement

3.3 Security Measures

The Processor implements and maintains the following technical and organisational measures:
Technical Measures:

- Encryption of Personal Data in transit (TLS 1.2+) and at rest (AES-256)
- Secure authentication with unique user credentials
- Database-level access controls (Row Level Security)
- Regular security updates and patch management
- Automated backup with encryption

Organisational Measures:

- Staff confidentiality agreements
- Access logging and audit trails
- Incident response procedures
- Minimal access principle (see NDA Section 7)

3.4 Sub-processors

Current Sub-processors:

Sub-processor	Purpose	Location
Supabase Inc.	Database hosting and authentication	EU (Frankfurt)
Vercel Inc.	Application hosting	EU
OpenAI / Anthropic	AI analysis generation	US (with SCCs)

The Processor shall:

- **Not engage additional sub-processors** without prior written consent from the Controller
- **Impose equivalent data protection obligations** on all sub-processors
- **Remain fully liable** for sub-processor compliance

3.5 Data Subject Rights

The Processor shall assist the Controller in responding to Data Subject requests including:

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

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

3.6 Data Breach Notification

In the event of a Data Breach, the Processor shall:

- **Notify the Controller without undue delay** and in any event within 24 hours of becoming aware
- Provide full details including: nature of breach, categories and numbers of Data Subjects affected, likely consequences, and measures taken
- **Cooperate fully** with the Controller's breach response and any regulatory notification
- **Document all breaches** including facts, effects, and remedial action

3.7 Data Protection Impact Assessments

The Processor shall provide reasonable assistance to the Controller for:

- Data Protection Impact Assessments (DPIAs) where required
- Prior consultation with the Information Commissioner's Office (ICO) where necessary

---

4. Controller Obligations

The Controller shall:

- Provide **clear, lawful instructions** for data processing
- Ensure a **valid legal basis** exists for all processing (legitimate interests for business benchmarking)
- **Inform Data Subjects** about data processing through appropriate privacy notices
- **Obtain any necessary consents** from participating businesses
- Respond to the Processor's requests for clarification in a timely manner

---

5. Audit Rights

5.1 Controller Audit Rights

The Controller has the right to:

- **Request evidence** of compliance with this Agreement and applicable data protection law
- **Conduct audits** (or appoint an independent auditor) with reasonable notice
- **Access audit logs** showing administrative access to Personal Data

5.2 Processor Cooperation

The Processor shall:

- Make available all information necessary to demonstrate compliance
- Allow and contribute to audits and inspections
- Immediately inform the Controller if an audit reveals non-compliance

---

6. Data Return and Deletion

6.1 Upon Termination

At the Controller's choice, the Processor shall:

- **Return all Personal Data** in a commonly-used, machine-readable format (CSV, JSON)
- **Delete all Personal Data** from all systems including backups within 30 days
- **Provide written certification** of deletion upon request

6.2 Exceptions

The Processor may retain Personal Data where required by applicable law, provided:

- The Controller is informed of the legal requirement
- Processing is limited to what is legally required
- Confidentiality obligations continue to apply

6.3 Individual Business Deletion

If an individual participating business requests deletion of their data:

- The Processor shall delete that business's data within 14 days of receiving instruction from the Controller
- The Controller shall confirm the deletion request in writing
- Historical aggregated data (which does not identify the business) may be retained

---

7. Liability and Indemnification

7.1 Processor Liability

The Processor shall be liable for damages caused by processing that:

- Does not comply with this Agreement
- Does not comply with applicable data protection law
- Is outside or contrary to the Controller's lawful instructions

7.2 Limitation

Liability under this Agreement is subject to the limitations set out in the main service agreement, except that neither party limits liability for:

- Wilful breach of data protection obligations
- Gross negligence or fraud
- Claims by Data Subjects or regulatory fines arising from the other party's breach

---

8. Term and Termination

8.1 Duration

This DPA shall remain in effect for the duration of the service relationship and for as long as the Processor retains any Personal Data.

8.2 Survival

Sections 3.2 (Confidentiality), 5 (Audit Rights), 6 (Data Return and Deletion), and 7 (Liability) shall survive termination.

---

9. Governing Law

This Agreement is governed by the laws of England and Wales. The courts of England and Wales have exclusive jurisdiction.

---

10. Amendments

This Agreement may only be amended in writing signed by both parties. The Processor shall notify the Controller of any changes to sub-processors or security measures.

Signature Section

SCEV Ltd t/a BrandedAI (Processor)

Signed: _____
Name: Scott Markham
Title: Director
Date: _____

Chester Brethren Business Group (Controller)

Signed: _____
Name: _____
Title: _____
Date: _____

Annex A: Technical and Organisational Measures

A.1 Platform Security Architecture

Layer	Measure
Application	React frontend with secure session management
API	HTTPS only, authentication required for all endpoints
Database	Supabase PostgreSQL with Row Level Security (RLS)
Storage	Encrypted at rest, access logged
Hosting	EU-based infrastructure, SOC 2 compliant providers

A.2 Access Control Model

Role	Access Level
Business User	Own business data only, aggregated reports
Chester Admin	All businesses' data, full reports, data export
BrandedAI Support	Database admin (for support only, logged)

A.3 Data Flow

Business User → Secure Form → Supabase DB → Aggregation Engine → Reports
All data encrypted at rest. AI Analysis uses anonymised data where possible.

A.4 Incident Response

1. **Detection:** Automated monitoring for unusual access patterns
2. **Containment:** Immediate access revocation if breach suspected
3. **Notification:** Controller notified within 24 hours
4. **Investigation:** Full root cause analysis
5. **Remediation:** Fix vulnerabilities, update procedures
6. **Documentation:** Full incident report retained for 5 years

---

This Agreement may be executed in counterparts. Electronic signatures are acceptable.