DATA PROCESSING AGREEMENT (DPA)

Effective Date: [Date]

Between:

Data Processor: Action & Consequence AB
Product: STRAETCH
Registered Address: Sweden
Contact: compliance@straetch.com

And:

Data Controller: [Customer Company Name]
(hereinafter referred to as "Customer" or "Controller")

---

1. DEFINITIONS

1.1 **"Personal Data"** means any information relating to an identified or identifiable natural person.

1.2 **"Processing"** means any operation performed on Personal Data, whether automated or not.

1.3 **"Data Subject"** means the individual to whom Personal Data relates.

1.4 **"Subprocessor"** means any third party engaged by the Processor to process Personal Data.

1.5 **"GDPR"** means Regulation (EU) 2016/679 (General Data Protection Regulation).

---

2. SCOPE OF PROCESSING

2.1 **Nature and Purpose:** Provision of STRAETCH marketing strategy and AI content platform services.

2.2 **Categories of Data Subjects:**

- Customer employees and authorized users
- Marketing contacts and leads (as uploaded by Customer)
- Website visitors (analytics data)

2.3 **Types of Personal Data:**

- Contact information (names, email addresses, job titles)
- Authentication data (hashed passwords, session tokens)
- Usage data (platform interactions, preferences)
- Business data (marketing content, strategy documents)

2.4 **Duration:** Processing continues for the term of the service agreement plus 30 days for deletion.

3. OBLIGATIONS OF THE PROCESSOR

3.1 Action & Consequence AB shall:

a) Process Personal Data only on documented instructions from the Controller;

b) Ensure persons authorized to process Personal Data are bound by confidentiality;

c) Implement appropriate technical and organizational security measures;

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

e) Delete or return all Personal Data upon termination (at Controller's choice);

f) Make available all information necessary to demonstrate compliance.

4. SECURITY MEASURES

4.1 **Technical Measures:**

Measure	Implementation
Encryption in Transit	TLS 1.3 for all connections
Encryption at Rest	AES-256 for stored data
Access Control	Role-Based Access Control (RBAC)
Authentication	Multi-Factor Authentication (MFA) available
Audit Logging	Comprehensive activity logging
Data Anonymization	PII stripped from AI processing
Backup	Daily encrypted backups with 30-day retention

4.2 **Organizational Measures:**

- Security awareness training for all personnel
- Regular security assessments and penetration testing
- Incident response procedures
- Business continuity planning

5. DATA LOCATION

5.1 Primary data processing occurs in **AWS EU (Ireland)**.

5.2 All core data storage and processing is EU-based.

5.3 Limited US processing for specific subprocessors (see Annex B) with appropriate safeguards.

6. SUBPROCESSORS

6.1 Controller authorizes the use of subprocessors listed in Annex B.

6.2 Processor shall provide **30 days' notice** before adding new subprocessors.

6.3 Controller may object to new subprocessors within 14 days of notification.

6.4 Current subprocessors are listed in **Annex B** attached hereto.

---

7. DATA SUBJECT RIGHTS

7.1 Processor shall assist Controller in responding to requests from Data Subjects exercising their rights under GDPR:

- 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)

7.2 Response assistance shall be provided within **72 hours** of Controller's request.

---

8. DATA BREACH NOTIFICATION

8.1 In case of a Personal Data breach, Processor shall:

a) Notify Controller without undue delay and no later than **72 hours** after becoming aware;

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

8.2 Breach notifications shall be sent to Controller's designated security contact.

---

9. DATA RETENTION AND DELETION

9.1 Personal Data shall be retained only for the duration of the service agreement.

9.2 Upon termination:

- Controller may request data export within 30 days
- All Personal Data shall be deleted within 30 days of termination
- Processor shall provide written certification of deletion upon request

9.3 Backups containing Personal Data shall be deleted within 90 days of termination.

10. AUDIT RIGHTS

10.1 Controller has the right to:

a) Request annual compliance questionnaires/attestations;

b) Review third-party audit reports (SOC 2, ISO 27001 via infrastructure providers);

c) Conduct audits with reasonable notice (at Controller's expense).

10.2 Audit requests shall be submitted with at least 30 days' notice.

11. INTERNATIONAL TRANSFERS

11.1 For transfers outside the EU/EEA, Processor shall ensure:

a) Adequacy decision exists for the destination country; or

b) Standard Contractual Clauses (SCCs) are in place; or

c) Other appropriate safeguards under GDPR Article 46.

11.2 SCCs are incorporated by reference where applicable.

12. LIABILITY AND INDEMNIFICATION

12.1 Each party's liability for breaches of this DPA shall be governed by the main service agreement.

12.2 Processor shall indemnify Controller for direct damages arising from Processor's breach of this DPA or GDPR obligations.

13. TERM AND TERMINATION

13.1 This DPA shall remain in effect for the duration of the service agreement.

13.2 Obligations regarding data deletion and confidentiality survive termination.

14. GOVERNING LAW

14.1 This DPA shall be governed by the laws of **Sweden**.

14.2 Disputes shall be resolved in the courts of Stockholm, Sweden.

ANNEX A: TECHNICAL AND ORGANIZATIONAL MEASURES

A.1 Physical Security

- AWS data centers with SOC 2 Type II certification
- Biometric access controls
- 24/7 surveillance and monitoring

A.2 Network Security

- Firewall protection
- DDoS mitigation
- Network segmentation
- Regular vulnerability scanning

A.3 Application Security

- Secure development lifecycle (SDLC)
- Code reviews and security testing
- Input validation and output encoding
- CSRF and XSS protection

A.4 Access Control

- Principle of least privilege
- Regular access reviews
- Automatic session timeout
- Strong password policies

A.5 Data Protection

- Encryption (TLS 1.3, AES-256)
- Data anonymization for AI processing
- Secure key management
- Regular security audits

A.6 Incident Response

- Documented incident response plan
- 24-hour on-call security team
- Post-incident reviews and improvements

A.7 Business Continuity

- Daily encrypted backups
- Geographic redundancy
- 99% uptime SLA
- Disaster recovery procedures

ANNEX B: LIST OF SUBPROCESSORS

Subprocessor	Purpose	Data Processed	Location	DPA Link
Supabase / AWS	Database, Authentication, Edge Functions	All application data	EU (Ireland)	View
OpenAI	AI Content Verification & Analytics	Anonymized prompts (no PII transmitted)	US (EU data processing available)	View
Anthropic	AI Content Creation	Anonymized prompts (no PII transmitted)	US (EU data processing available)	View
Google Cloud (Search Console)	SEO Analytics Integration	Search performance metrics	EU	View
Stripe	Payment Processing	Billing information, payment details	EU	View
Resend	Transactional Email	Email addresses, notification content	US	View
DataForSEO	Keyword & Search Volume Data	Search queries (no PII)	EU	View
Firecrawl	Web Scraping for Social Listening	Public URLs only	US	View
Lovable	Application Hosting & Deployment	Application code, static assets	EU	View

---

ANNEX C: STANDARD CONTRACTUAL CLAUSES

For transfers to third countries without adequacy decisions, the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914) are incorporated by reference.

SIGNATURES

For Action & Consequence AB (Processor):

Name: _____
Title: _____
Date: ___
Signature: _____

For [Customer Company Name] (Controller):

Name: _____
Title: _____
Date: ___
Signature: _____

Version: 1.1
Last Updated: August 2026
Contact: compliance@straetch.com