INNERMEDIA

25

YEARS · 2001–2026

DATA PROCESSING AGREEMENT

TERMS, CONDITIONS & POLICIES

VERSION 4.0 · MAY 2026

INNER MEDIA LIMITED · COMPANY NO. 04818830
SOPERS HOUSE, SOPERS RD, CUFFLEY, POTTERS BAR EN6 4RY
01707 875 721 · INNERMEDIA.CO.UK

UK GDPR Article 28 — Processor Agreement

This Data Processing Agreement (DPA) is incorporated into and forms part of the Master Terms & Conditions between InnerMedia Limited (Processor) and the Client (Controller). It applies wherever the Supplier processes Personal Data on behalf of the Client in connection with any Service.

This DPA is entered into between:

PARTY	DETAILS
Data Controller (“Controller”)	The Client as named in the relevant Schedule.
Data Processor (“Processor”)	Inner Media Limited, Company No. 04818830, Enterprise Centre, Cranborne Road, Potters Bar, Hertfordshire EN6 3DQ. ICO Registration: ICO:00010252104.

1. DEFINITIONS

1.1 In this DPA, the following terms have the meanings given in the UK GDPR and the Data Protection Act 2018: ‘Controller’, ‘Data Subject’, ‘Personal Data’, ‘Personal Data Breach’, ‘Processing’, ‘Processor’, ‘Special Category Data’, ‘Supervisory Authority’.

1.2 ‘Services’ means the services described in the applicable Schedule to the Master Terms.

1.3 ‘Sub-Processor’ means any third party engaged by the Processor to carry out Processing activities on behalf of the Controller.

2. SCOPE AND PURPOSE OF PROCESSING

PROCESSING DETAIL	DESCRIPTION
Subject matter	Personal Data provided by the Client in connection with the Services, including website visitor data, enquiry data, staff data, and AI interaction data.
Duration	For the term of the Agreement and as required by applicable law.

PROCESSING DETAIL	DESCRIPTION
Nature of processing	Collection, storage, structuring, retrieval, use, transmission, deletion and destruction of Personal Data as necessary to deliver the Services.
Purpose of processing	To enable the Processor to deliver the Services as described in the Schedules, including website hosting, content management, AI product operation, and related technical services.
Type of Personal Data	Names, email addresses, telephone numbers, IP addresses, website interaction data, enquiry content, conversation logs, and any other data provided by or on behalf of the Client.
Categories of Data Subjects	Website visitors, prospective clients/pupils/parents, existing clients/pupils/parents, staff members, and End-Users of AI Products.
Special Category Data	Not anticipated. The Client must notify the Processor in writing before providing any Special Category Data.

3. CONTROLLER OBLIGATIONS

3.1 The Controller warrants and undertakes that:

- It has a valid lawful basis under UK GDPR for each Processing activity;
- It has provided Data Subjects with all required privacy notices;
- It is entitled to transfer Personal Data to the Processor for Processing under this DPA;
- Where required, it has obtained valid consent from Data Subjects (including parents/guardians of children under 13);
- It will ensure that any instructions given to the Processor comply with UK GDPR.

4. PROCESSOR OBLIGATIONS

The Processor shall, in relation to any Personal Data processed on behalf of the Controller:

4.1 Process Only on Instructions

Process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law (in which case the Processor shall notify the Controller unless prohibited by law).

4.2 Confidentiality

Ensure that all personnel authorised to process Personal Data are subject to binding confidentiality obligations and have received appropriate data protection training.

4.3 Security

Implement and maintain appropriate technical and organisational measures to protect Personal Data against unauthorised or unlawful Processing and against accidental loss, destruction, damage, alteration or disclosure, including:

- AES-256 encryption of Personal Data at rest;
- TLS 1.2 or higher encryption of Personal Data in transit;
- Role-based access controls and least-privilege principles;
- Multi-factor authentication (MFA) for all systems accessing Personal Data;
- Regular security testing and review of AI infrastructure;
- Physical security controls at all data centre locations (managed by AWS).

4.4 Sub-Processors

4.4.1 The Controller provides general written authorisation to use the Sub-Processors listed in Schedule D Appendix 1 (the Approved Sub-Processor List).

4.4.2 The Processor shall: (a) give at least thirty (30) days' written notice before engaging any new Sub-Processor or replacing an existing one; (b) impose data protection obligations on each Sub-Processor equivalent to those in this DPA; and (c) remain fully liable to the Controller for the acts and omissions of each Sub-Processor.

4.4.3 The Controller may object to a new Sub-Processor within fourteen (14) days of notice. If the parties cannot resolve the objection, the Controller may terminate the affected Service on thirty (30) days' notice without penalty.

4.5 Data Subject Rights

Without undue delay, and in any case within seventy-two (72) hours, assist the Controller in responding to Data Subject requests (access, rectification, erasure, restriction, portability, objection) by providing all information the Controller reasonably requires. Such assistance shall be at the Processor's cost where it relates to a security or processing failure by the Processor, and at the Controller's cost otherwise.

4.6 Data Protection Impact Assessments (DPIAs)

Assist the Controller with any Data Protection Impact Assessment required by Article 35 UK GDPR and with any consultation with the ICO.

4.7 Personal Data Breach Notification

Notify the Controller without undue delay (and in any event within 72 hours) of becoming aware of a Personal Data Breach affecting Controller Personal Data. Such notification shall include:

- A description of the nature of the breach;
- The categories and approximate number of Data Subjects and Personal Data records affected;
- The name and contact details of the Data Protection contact;
- The likely consequences of the breach;
- Measures taken or proposed to address the breach.

Where it is not possible to provide all information within 72 hours, the Processor shall provide information in phases without undue further delay.

4.8 Audit

Make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA, and allow for and contribute to audits and inspections by the Controller or a mandated auditor, at the Controller's cost, on not less than thirty (30) days' written notice. The Processor may refuse unreasonable audit requests or impose reasonable conditions to protect third-party confidentiality.

4.9 No Training on Client Data

The Processor shall not use Personal Data or any other Client Data to
train, fine-tune, benchmark or otherwise develop or improve any AI
model, whether proprietary or third-party. This obligation survives
termination of the Agreement.

4.10 International Transfers

The Processor shall not transfer Personal Data outside the United Kingdom or the European Economic Area without the prior written consent of the Controller, except where a valid transfer mechanism under UK GDPR exists (such as adequacy regulations or Standard Contractual Clauses).

The use of AWS UK/EU regions and Anthropic Claude accessed exclusively via AWS Bedrock ensures that AI processing does not constitute an international transfer of Personal Data.

4.11 Deletion and Return

On termination of the Agreement or on written request by the Controller: (a) return all Personal Data in a structured, machine-readable format; and (b) securely delete all Personal Data from Supplier systems within thirty (30) days, unless retention is required by applicable law. The Processor shall confirm deletion in writing.

5. DATA RETENTION

DATA TYPE	RETENTION PERIOD
AI Interaction Data (conversation logs)	360 days from session end (or shorter if instructed by Controller)
Children's Interaction Data (under 18)	360 days maximum (automatic deletion)
Website analytics data	As configured in the analytics platform (typically 26 months — GA4 default)
Client business information (for AI configuration)	Duration of Agreement + 30 days post-termination
Billing and financial records	7 years (UK statutory requirement)
Security logs and access records	12 months

6. GOVERNING LAW

This DPA is governed by the laws of England and Wales. Any dispute arising under this DPA shall be subject to the exclusive jurisdiction of the courts of England and Wales.