INNERMEDIA

25

YEARS · 2001–2026

DATA PROTECTION POLICY

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

POLICY DETAIL	INFORMATION
Policy Owner	Board of Directors
Approved By	Board of Directors
Review Cycle	Annual (or following material regulatory or business change)
Applies To	All InnerMedia staff, contractors and sub-processors with access to personal data
Associated Documents	Privacy Policy | AI & Data Transparency Statement | Information Security Policy | Data Processing Agreement
Regulatory Framework	UK GDPR (retained EU law) | Data Protection Act 2018 | Privacy and Electronic Communications Regulations 2003

1. INTRODUCTION AND PURPOSE

1.1 Inner Media Limited ('InnerMedia') collects and processes personal data about clients, prospective clients, staff, website visitors, and end-users of our AI products. We are committed to handling all personal data lawfully, transparently and securely.

1.2 This policy sets out the framework for how InnerMedia complies with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. It applies to all personal data processed by InnerMedia, whether in digital or physical form.

1.3 Compliance with this policy is mandatory for all staff, contractors and any third party granted access to InnerMedia systems or client data.

Failure to comply with this policy may result in disciplinary action,
up to and including dismissal, and may also expose individual staff to
personal liability under data protection law.

2. ROLES AND RESPONSIBILITIES

2.1 Data Controller

InnerMedia acts as a Data Controller for personal data it collects about its own contacts, prospects and staff. InnerMedia acts as a Data Processor for personal data provided by clients. In both cases, the obligations in this policy apply.

2.2 Board of Directors

- Hold ultimate accountability for data protection compliance;
- Ensure adequate resources are allocated for data protection;
- Approve this policy and any material amendments;
- Receive and act on reports of data breaches or significant compliance issues.

2.3 Data Protection Lead

InnerMedia has designated a Data Protection Lead (currently the Managing Director) who is responsible for:

- Day-to-day oversight of data protection compliance;
- Maintaining the Record of Processing Activities (ROPA);
- Managing data subject requests and breach notifications;
- Liaising with the ICO when required;
- Keeping staff training up to date;
- Reviewing and updating this policy annually.

2.4 All Staff

- Complete data protection induction training before handling personal data;
- Complete annual refresher training;
- Handle personal data only as required for their role and in accordance with this policy;
- Report any suspected data breach or security incident immediately to the Data Protection Lead;
- Not access, share or use personal data for any purpose outside their role;
- Follow the clean desk and screen lock policies in the Information Security Policy.

3. DATA PROTECTION PRINCIPLES

InnerMedia shall ensure that all personal data is:

PRINCIPLE	WHAT THIS MEANS IN PRACTICE
Lawfully, fairly and transparently processed	We identify a legal basis before processing. We are clear with individuals about how we use their data (via our Privacy Policy).
Collected for specified, explicit and legitimate purposes	We do not use data for purposes incompatible with why it was collected. AI products do not use client data for model training.
Adequate, relevant and limited to what is necessary	We collect only the data we need. We do not request unnecessary information in AI interactions.
Accurate and kept up to date	We take reasonable steps to keep data accurate. Clients can request corrections at any time.
Not kept longer than necessary	We apply the retention periods set out in the Privacy Policy and DPA. Automated deletion is in place for AI interaction data.
Processed securely	We apply the technical and organisational measures set out in the Information Security Policy and DPA.
Accountability	We maintain records of our processing activities and can demonstrate compliance on request.

4. LAWFUL BASES FOR PROCESSING

4.1 Before processing any personal data, the relevant team member must confirm that a valid lawful basis exists. InnerMedia's primary lawful bases are:

- Contract (Article 6(1)(b)): processing necessary to deliver services to clients;
- Legitimate Interests (Article 6(1)(f)): managing client relationships, marketing to business contacts, improving our services — subject to a Legitimate Interests Assessment (LIA) where required;
- Legal Obligation (Article 6(1)(c)): compliance with accounting, employment and regulatory requirements;
- Consent (Article 6(1)(a)): newsletter sign-ups, non-essential cookies, certain marketing activities.

4.2 For Special Category Data (health, race, religion, biometric data, etc.), an additional condition under Article 9 UK GDPR must be identified. InnerMedia does not ordinarily process Special Category Data. If a client scenario requires this, the Data Protection Lead must be consulted before any processing begins.

4.3 For children's data, the Data Protection Lead must review the relevant processing activity before it begins to ensure compliance with the ICO's Age Appropriate Design Code and any applicable sector guidance.

5. RECORD OF PROCESSING ACTIVITIES (ROPA)

5.1 InnerMedia maintains a Record of Processing Activities (ROPA) as required by Article 30 UK GDPR. The ROPA is maintained by the Data Protection Lead and reviewed annually.

5.2 The ROPA covers: all categories of personal data processed; the purposes of processing; lawful bases; data subjects; retention periods; recipients and sub-processors; and international transfers.

5.3 Any new processing activity (including new AI product features, new sub-processors or new client sectors) must be notified to the Data Protection Lead before launch so the ROPA can be updated.

6. DATA SUBJECT RIGHTS

6.1 InnerMedia is committed to honouring all Data Subject rights requests within the statutory timescales:

RIGHT	RESPONSE TIMEFRAME
Subject Access Request (SAR)	One calendar month (extensible to three months for complex requests)
Rectification	Without undue delay (aim: 72 hours for straightforward corrections)
Erasure	Without undue delay (aim: 30 days)
Restriction of processing	Without undue delay
Data portability	One calendar month
Objection to processing	Must stop processing immediately (unless compelling legitimate grounds)
AI conversation deletion	72 hours

6.2 All data subject requests must be directed to hello@innermedia.co.uk and immediately forwarded to the Data Protection Lead.

6.3 We may request proof of identity before processing a request. We will not charge a fee for routine requests.

7. DATA BREACHES

ALL suspected data breaches or security incidents involving personal

data must be reported to the Data Protection Lead immediately — and in

any event within 2 hours of discovery. Do not attempt to investigate or
contain a breach without involving the Data Protection Lead.

7.1 What Constitutes a Breach

A personal data breach is any security incident that results in the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes:

- Sending personal data to the wrong recipient (email, post, or file share);
- Loss or theft of a device containing personal data;
- Unauthorised access to systems containing personal data;
- AI product errors resulting in inappropriate disclosure of personal data;
- A sub-processor reporting a breach affecting InnerMedia client data.

7.2 Breach Response Process

On discovery of a suspected breach, the following steps shall be taken:

- Step 1 — Report: Notify the Data Protection Lead immediately (within 2 hours);
- Step 2 — Contain: Take immediate steps to stop ongoing harm (e.g. revoke access, suspend AI service);
- Step 3 — Assess: Data Protection Lead assesses severity, scope and likely consequences;
- Step 4 — Notify Controller: If the breach affects a Client's data, notify the Client within 72 hours;
- Step 5 — ICO Notification: If the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO within 72 hours of InnerMedia becoming aware;
- Step 6 — Document: Record all details of the breach, the response, and any remedial actions taken.

7.3 Not all breaches require ICO notification, but all breaches must be documented in the Breach Register maintained by the Data Protection Lead.

8. DATA MINIMISATION AND RETENTION

8.1 Staff must only collect the personal data that is genuinely necessary for the relevant purpose. When in doubt, less is more.

8.2 All personal data must be deleted or anonymised when it is no longer needed, in accordance with the retention periods in the Privacy Policy. Staff must not retain personal data in personal email accounts, local drives or unofficial storage.

8.3 AI interaction data is automatically deleted from InnerMedia systems after three hundred and sixty (360) days. Staff must not extract or copy this data beyond the agreed purposes.

9. THIRD PARTIES AND SUB-PROCESSORS

9.1 Before sharing personal data with any third party, the Data Protection Lead must confirm that an appropriate contract or agreement is in place (e.g. a DPA or sub-processor agreement).

9.2 New sub-processors must be approved by the Data Protection Lead before use. Clients must be notified of new sub-processors with at least thirty (30) days' notice.

9.3 Sub-processors must be vetted to confirm they implement appropriate technical and organisational security measures.

10. INTERNATIONAL TRANSFERS

10.1 No personal data may be transferred outside the UK or EEA without the prior written approval of the Data Protection Lead and a valid transfer mechanism (adequacy decision, SCCs, or Binding Corporate Rules).

10.2 The use of AWS UK/EU regions and Anthropic Claude via AWS Bedrock means that AI processing does not constitute an international transfer.

11. TRAINING

11.1 All staff must complete data protection induction training before accessing any personal data.

11.2 All staff must complete annual refresher training, updated to reflect any changes in law or InnerMedia's processing activities.

11.3 Staff working directly with AI products or client data must complete additional AI-specific data handling training.

11.4 Training completion records shall be maintained by the Data Protection Lead.

12. POLICY BREACHES

Any breach of this policy by a member of staff will be investigated and may result in disciplinary action up to and including dismissal. Serious breaches may also be referred to the ICO or other regulatory authorities.

13. POLICY REVIEW

This policy shall be reviewed annually by the Data Protection Lead and approved by the Board. It shall also be reviewed following any material change in UK GDPR, relevant guidance from the ICO, or a significant change to InnerMedia's data processing activities.