

GDPR COMPLIANCE POLICY

Media Activation Ltd

HealthPoint TV Ltd · Vistavue Ltd

Version 2.0 | Effective: 21 June 2026 | Review: June 2027

Version	Author / Reviewer	Date
1.0 – Initial issue	Julian Clogg, GDPR Lead	21 June 2026
2.0 – Annual review	Julian Clogg, GDPR Lead	21 June 2027

1. Purpose and Scope

This GDPR Compliance Policy ("Policy") sets out the obligations of Media Activation Ltd ("the Company", "we", "us") under the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA 2018). It governs all personal data processing carried out by the Company in the course of managing advertising campaigns on behalf of two distinct screen networks:

Network	Environment	Sensitivity Classification
HealthPoint TV Ltd	Digital screens in pharmacies and healthcare retail premises across the UK	Elevated – healthcare retail; potential inference of OTC health needs
Vistavue Ltd	Digital screens in GP surgeries and NHS-affiliated primary care premises across the UK	High – clinical environment; patient-facing; NHS data security obligations engaged

This Policy applies to all employees, contractors, consultants, agency staff, and third-party data processors acting on behalf of Media Activation Ltd. Compliance with this Policy is mandatory. Breach of this Policy may result in disciplinary action, contract termination, and/or regulatory referral to the Information Commissioner's Office (ICO).

This Policy should be read alongside the Company's Privacy Notice, Data Retention Schedule, Data Breach Response Procedure, Data Protection Impact Assessment (DPIA) Register, and Records of Processing Activities (RoPA).

2. Key Definitions

The following terms have the meanings given in the UK GDPR and DPA 2018 unless otherwise stated:

Term	Definition
Personal Data	Any information relating to an identified or identifiable natural person (data subject).
Special Category Data	Data revealing racial/ethnic origin, political opinions, religious beliefs, trade union membership, genetic data, biometric data (where used for unique identification), health data, sex life or sexual orientation. Subject to heightened protection under Article 9 UK GDPR.
Processing	Any operation performed on personal data, including collection, storage, use, disclosure, deletion.
Data Controller	The entity that determines the purposes and means of processing personal data. Media Activation Ltd is a controller in respect of its own business operations.
Data Processor	An entity processing data on behalf of and under the instructions of a controller. Media Activation Ltd acts as processor when managing campaigns on behalf of advertising clients.

Joint Controllers	Two or more controllers who jointly determine the purposes and means of processing. Where applicable, arrangements must be documented under Article 26 UK GDPR.
Data Subject	The identified or identifiable living individual to whom personal data relates.
Lawful Basis	The legal ground under Article 6 UK GDPR (or Article 9 for special category data) that permits processing.
DPIA	Data Protection Impact Assessment – a structured risk analysis required prior to high-risk processing operations.
RoPA	Record of Processing Activities – the mandatory internal register of all processing operations, required under Article 30 UK GDPR.
ICO	Information Commissioner's Office – the UK supervisory authority for data protection.
NHS DSP Toolkit	NHS Data Security and Protection Toolkit – the self-assessment framework applicable to organisations handling NHS patient data or operating within NHS-affiliated premises.

3. Data Protection Principles

Article 5 UK GDPR establishes six foundational principles. Media Activation Ltd treats these as non-negotiable obligations that govern every processing activity across both networks.

#	Principle	How We Apply It
1	Lawfulness, Fairness & Transparency	We identify and document a lawful basis before commencing any processing activity. We publish a Privacy Notice and display network-specific notices at HealthPoint TV and Vistavue GP screen locations. We do not process data in ways that data subjects would not reasonably expect.
2	Purpose Limitation	Personal data is collected for specified, explicit, and legitimate purposes and is not further processed in a manner incompatible with those purposes. Campaign analytics data is not repurposed for individual profiling or cross-network linkage without a fresh lawful basis assessment.
3	Data Minimisation	We collect only the minimum personal data necessary to fulfil the identified purpose. Audience measurement on both networks operates at an aggregated, anonymised level by default. We do not collect patient identifiers or clinical data in any form.
4	Accuracy	Reasonable steps are taken to ensure personal data is accurate and, where necessary, kept up to date. Client and supplier contact records are reviewed at least annually.

5	Storage Limitation	Personal data is not retained longer than necessary. Retention periods are documented in the Company's Data Retention Schedule and are enforced through automated deletion or documented manual review processes.
6	Integrity & Confidentiality	Appropriate technical and organisational security measures are applied to protect personal data against unauthorised access, loss, destruction, or damage. Heightened security controls apply to data flows associated with the Vistavue GP (NHS-adjacent) network.

The Company also observes the accountability principle under Article 5(2) UK GDPR: we must be able to demonstrate compliance with all of the above. This is achieved through maintenance of the RoPA, DPIA register, training records, audit logs, and this Policy.

4. Roles and Responsibilities

4.1 Data Controller and Processor Roles

Media Activation Ltd operates in dual capacities depending on the processing activity:

Processing Activity	MAL's Role	Implications
Internal business operations (HR, finance, supplier management)	Data Controller	Full controller obligations apply: lawful basis, subject rights, retention, security, breach notification.
Managing advertising campaigns on behalf of clients (HealthPoint TV, Vistavue)	Data Processor	Must act only on documented client instructions. Article 28 DPA required. Cannot sub-process without written authorisation. Must assist controller with subject rights and DPIAs.
Joint audience analytics activities where both MAL and network operator determine purposes	Potential Joint Controller (Article 26)	Written arrangement required. Transparency obligations must be fulfilled. Responsibility allocation must be documented.

4.2 Internal Accountability Structure

Role	Responsibilities
Board / Senior Management	Accountable for the Company's data protection compliance. Approve this Policy. Ensure adequate resource is allocated to data protection. Receive quarterly GDPR compliance reports.
GDPR Lead / Data Protection Officer (if appointed)	Day-to-day oversight of GDPR compliance. Maintain RoPA and DPIA register. Advise on lawful bases and high-risk processing.

	Manage ICO correspondence. Lead breach response. Deliver staff training. Review this Policy annually.
Campaign Managers	Ensure all campaign briefs, data sharing arrangements, and audience measurement methods for HealthPoint TV and Vistavue GP networks comply with this Policy. Escalate novel processing activities to the GDPR Lead before implementation.
Technology & Systems Team	Implement and maintain technical security controls. Conduct penetration testing. Manage vendor security assessments. Support DPIA technical assessments.
Finance & Legal	Ensure data processing agreements (Article 28) are in place with all data processors and network operators. Review contractual data protection obligations. Manage insurance and regulatory risk.
All Staff	Complete mandatory GDPR training. Report suspected breaches immediately to the GDPR Lead. Not to share personal data outside of authorised channels. Refer data subject requests to the GDPR Lead without delay.

4.3 Data Protection Officer

Media Activation Ltd [has appointed / will appoint] a Data Protection Officer (DPO) [or: does not meet the mandatory DPO threshold under Article 37 UK GDPR but has designated a GDPR Lead with equivalent responsibilities]. The DPO / GDPR Lead can be contacted at:

Email: julian@mediaactivation.co.uk

Post: Media Activation Ltd Albany House, 3 Temple Court, Temple Way, Coleshill, Warcs B46 1HH marked 'Data Protection'

The DPO / GDPR Lead operates with independence, reports directly to the Board, and may not be dismissed or penalised for performing their duties.

5. Lawful Basis for Processing

5.1 Article 6 Lawful Bases

Every processing activity must be assigned a lawful basis before processing commences. The basis must be documented in the RoPA. The following bases are applicable to Media Activation Ltd's operations:

Lawful Basis	When We Use It	Network / Activity
Legitimate Interests (Art. 6(1)(f))	Aggregated audience analytics; maintaining professional contact records; fraud prevention; business analytics.	Both networks. LIA conducted and documented for each application.
Contract (Art. 6(1)(b))	Processing necessary to deliver campaign services to advertising clients; administration of network operator agreements; supplier contracts.	Both networks.

Legal Obligation (Art. 6(1)(c))	Tax, financial reporting, employment law compliance; NHS DSP Toolkit obligations (Vistavue GP context).	Both networks; NHS obligations specific to Vistavue GP.
Consent (Art. 6(1)(a))	Non-essential cookies on Company digital properties; opt-in marketing communications.	Both networks (digital properties). Freely given, specific, informed, unambiguous. Withdrawable at any time.

5.2 Special Category Data (Article 9)

Neither HealthPoint TV Ltd nor Vistavue Ltd campaigns are designed to process special category data. However, both networks operate in environments where the risk of inadvertent special category data processing is material:

Network	Special Category Risk & Mitigation
HealthPoint TV Ltd (Pharmacies)	Risk: Audience presence in a pharmacy could permit inference of health-related purchasing behaviour. Mitigation: No individual-level audience data is collected or retained. All measurement is aggregated and anonymised. No audience data is linked to purchase records, loyalty schemes, or prescription data. DPIA required before any campaign proposing individual-level health-contextual targeting.
Vistavue Ltd (GP Surgeries)	Risk: Significantly elevated. Presence in a GP surgery is itself potentially health-revealing. Audience measurement data, even aggregated, must not enable inference of health status at individual or micro-cohort level. Patient data processed by GP practices is entirely outside MAL's processing activities. Mitigation: Privacy-by-design audience measurement only. No biometric identification. No linkage to patient records. DPIA mandatory for all new measurement methodologies. NHS DSP Toolkit compliance required for all technology partners with data flows in NHS premises.

Where any processing activity engages special category data, the Company must identify a condition under Article 9(2) UK GDPR (most likely Article 9(2)(a) explicit consent or Article 9(2)(j) public interest/research with appropriate safeguards) before processing commences. The GDPR Lead must approve all such processing.

5.3 Legitimate Interests Assessments

Where the Company relies on legitimate interests, a three-part Legitimate Interests Assessment (LIA) must be completed and retained:

- Purpose test: Is there a genuine legitimate interest?
- Necessity test: Is processing necessary for that purpose, or is there a less intrusive means of achieving the same result?
- Balancing test: Do the individual's interests, rights, and freedoms override the legitimate interest? Given the healthcare environments of both networks, the balancing test is applied with heightened scrutiny.

6. Categories of Personal Data Processed

Data Category	Data Subjects	Network	Lawful Basis
Aggregated anonymised audience analytics (footfall, dwell time, estimated demographic ranges)	General public / patients / pharmacy visitors	Both	Legitimate Interests
Client / agency employee contact data (name, email, phone, job title)	Client & agency staff	Both	Contract / Legitimate Interests
Campaign financial & billing data	Client authorised signatories	Both	Contract / Legal Obligation
Client portal login credentials	Client & agency staff	Both	Contract
Supplier / partner contact data	Supplier staff	Both	Legitimate Interests / Contract
GP practice manager / site liaison contact data	Practice administrative staff	Vistavue GP only	Legitimate Interests / Contract
NHS commissioner / ICB contact data (where applicable)	NHS staff	Vistavue GP only	Legitimate Interests / Contract
Employee / HR data	MAL employees	Internal	Contract / Legal Obligation
Website / portal cookie data (consented)	Website visitors	Both (digital properties)	Consent

7. Data Subject Rights

The Company is committed to facilitating the exercise of all data subject rights under Chapter III UK GDPR. The following rights apply to individuals whose data we process:

Right	Our Obligation	Deadline
Access (Art. 15)	Confirm whether we process data; provide a copy and supplementary information. Note: pharmacy or GP patient records are held by the network operator / practice, not MAL.	1 month (extendable to 3 months for complexity)
Rectification (Art. 16)	Correct inaccurate data; complete incomplete data.	1 month

Erasure (Art. 17)	Delete data where no longer necessary, consent withdrawn, or processing unlawful. Subject to legal retention obligations.	1 month
Restriction (Art. 18)	Restrict processing during accuracy disputes or objection assessment.	Without undue delay
Portability (Art. 20)	Provide data in structured machine-readable format where basis is consent or contract and processing is automated.	1 month
Object (Art. 21)	Cease processing based on legitimate interests unless compelling grounds demonstrated. Absolute right to object to direct marketing.	Immediately for direct marketing; otherwise assessed
No Automated Decisions (Art. 22)	MAL does not engage in solely automated decision-making with legal or significant effects. If this changes, explicit consent or legal basis required.	N/A – not currently applicable

7.1 Handling Data Subject Requests

- All data subject requests must be forwarded to the GDPR Lead immediately upon receipt, regardless of how or to whom they are addressed.
- Identity must be verified before disclosure. Where identity cannot be verified, the Company may request additional information. We will not charge for this verification.
- Requests are responded to free of charge unless manifestly unfounded or excessive, in which case a reasonable fee may be charged or the request refused.
- Where MAL acts as a processor, data subject requests will be referred to the relevant controller (advertising client or network operator) without undue delay.
- A log of all data subject requests, their outcome, and the timeline of response must be maintained by the GDPR Lead.

8. Data Retention

Personal data must not be retained beyond the period necessary for the purpose for which it was collected. The following retention schedule applies. The full Data Retention Schedule (a separate document) governs all categories in detail.

Data Category	Retention Period	Basis for Retention Period
Campaign delivery & performance data	3 years from campaign end (or longer if contractually required)	Limitation Act 1980; client contract terms
Client / agency contact records	Duration of relationship + 6 years	Limitation Act 1980
Financial & invoicing records	7 years from financial year end	HMRC / Companies Act 2006

Supplier / partner records	Duration of contract + 6 years	Limitation Act 1980
GP practice site contact records (Vistavue GP)	Duration of site agreement + 6 years	Limitation Act 1980
Employee / HR records	Duration of employment + 6 years (certain categories longer per statutory requirement)	Employment Rights Act 1996; statutory obligations
Data breach records	5 years from breach date	ICO accountability requirement
DPIA records	Life of processing activity + 3 years	ICO accountability requirement; Art. 35 UK GDPR
Correspondence & communications	3 years (unless relevant to live proceedings)	Business need; limitation periods
Consent records	Duration of consent + 1 year after withdrawal	Art. 7(1) UK GDPR accountability

At the expiry of the applicable retention period, personal data must be securely deleted, pseudonymised, or anonymised. Anonymised or aggregated data that no longer constitutes personal data for UK GDPR purposes may be retained indefinitely for analytical purposes.

9. Data Security

9.1 Technical and Organisational Measures

The Company implements measures proportionate to the risks of processing, with enhanced controls applied to Vistavue GP network data flows given the NHS-adjacent context. Measures include:

Measure	Detail	Network Applicability
Encryption	Data encrypted in transit (TLS 1.2+) and at rest (AES-256 or equivalent)	Both networks
Access Controls	Role-based access; principle of least privilege; quarterly access reviews	Both networks
Authentication	Multi-factor authentication mandatory for all systems containing personal data	Both networks
Penetration Testing	Annual independent penetration test; critical vulnerabilities remediated within 30 days	Both networks
Vulnerability Management	Monthly automated scanning; patch management policy	Both networks

NHS DSP Toolkit Alignment	All technology partners with Vistavue GP data flows assessed against NHS DSP Toolkit standards	Vistavue GP only
Physical Security	Clean desk policy; locked storage for physical documents; visitor management	Both networks
Staff Training	Mandatory annual GDPR and security awareness training; phishing simulation exercises	Both networks
Audit Logging	Access to personal data systems logged and reviewed quarterly	Both networks
Business Continuity	Documented BCP and disaster recovery procedures; tested annually	Both networks

9.2 Data Breach Response

A personal data breach is any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. The following response procedure applies:

Step	Action
1	CONTAIN: Immediately take steps to limit the breach (isolate systems, revoke access, preserve evidence). Any member of staff who suspects a breach must notify the GDPR Lead without delay.
2	ASSESS: The GDPR Lead assesses the nature, scope, and likely consequences of the breach within 24 hours of discovery. Complete the Breach Assessment Form.
3	NOTIFY ICO: If the breach is likely to result in a risk to individuals' rights and freedoms, notify the ICO within 72 hours of becoming aware. If notification is late, document reasons for delay.
4	NOTIFY INDIVIDUALS: If the breach is likely to result in a high risk to individuals, notify affected data subjects without undue delay. Notification must describe the breach, likely consequences, and steps taken.
5	NOTIFY NETWORK OPERATORS: Where a breach involves data flows associated with HealthPoint TV Ltd or Vistavue Ltd, notify the relevant network operator and (for Vistavue GP) the NHS Data Security and Protection lead without delay.
6	DOCUMENT: Record all breaches in the Breach Register, including those not notified to the ICO, with rationale for the decision taken. Retained for a minimum of 5 years.
7	REVIEW: Conduct a post-breach review within 30 days. Implement remediation measures. Report to the Board.

10. Data Processing Agreements and Third-Party Management

10.1 Article 28 UK GDPR Requirements

Where the Company engages a third party to process personal data on its behalf, or where the Company itself processes personal data as a processor on behalf of a client, a written Data Processing Agreement (DPA) compliant with Article 28 UK GDPR must be in place before processing commences. All DPAs must include provisions requiring the processor to:

- Process personal data only on documented instructions from the controller;
- Ensure persons authorised to process the data are bound by appropriate confidentiality obligations;
- Implement appropriate technical and organisational security measures under Article 32;
- Not engage sub-processors without prior specific or general written authorisation from the controller, and impose equivalent obligations on any sub-processor;
- Assist the controller in responding to data subject requests, conducting DPIAs, and meeting breach notification obligations;
- Delete or return all personal data upon termination of the processing relationship;
- Make available to the controller all information necessary to demonstrate compliance with Article 28 obligations.

10.2 Key Third-Party Categories and Requirements

Third-Party Category	Data Protection Requirement	Additional Requirement (Vistavue GP)
HealthPoint TV Ltd (network operator)	Article 26 joint controller arrangement or Article 28 DPA as appropriate to the data flows. Clear allocation of controller responsibilities in writing.	N/A
Vistavue Ltd (network operator)	Article 26 joint controller arrangement or Article 28 DPA. Additional NHS DSP Toolkit alignment clause required.	Written confirmation of NHS DSP Toolkit compliance status; contractual obligation to notify MAL of any NHS data security incidents.
Audience measurement technology providers	Article 28 DPA. Evidence of privacy-by-design architecture. No individual-level data retention.	NHS DSP Toolkit assessment. Data localisation preference (UK/EEA only). Annual security review.
Campaign management software providers	Article 28 DPA. International transfer safeguards if non-UK/EEA. SOC 2 Type II or ISO 27001 certification preferred.	As left, plus NHS DSP Toolkit where data flows touch NHS premises.
Cloud hosting / infrastructure providers	Article 28 DPA. IDTA or equivalent international transfer mechanism if applicable. Annual security attestation.	UK data residency preferred for Vistavue GP network data.
Advertising clients (MAL acts as processor)	MAL must enter Article 28 DPA as processor. Client's instructions	Additional healthcare advertising compliance clauses required.

	must be documented. Clients must not instruct MAL to process data in breach of UK GDPR.	
--	---	--

11. International Transfers of Personal Data

The transfer of personal data outside the UK is restricted under Chapter V UK GDPR. No transfer of personal data to a third country or international organisation may take place unless one of the following mechanisms applies:

- Adequacy Regulation: The destination country or territory is covered by an adequacy regulation made by the Secretary of State under section 17A DPA 2018;
- International Data Transfer Agreement (IDTA): An IDTA approved by the ICO (or the ICO Addendum to EU SCCs) is executed between the exporter and importer prior to transfer;
- Binding Corporate Rules: Where applicable for intra-group transfers; or
- Article 49 Derogations: As a last resort only, and with GDPR Lead approval.

For data flows associated with the Vistavue GP (NHS-adjacent) network, UK data residency is the default position. Any proposed transfer of Vistavue GP-related data outside the UK must be approved by the GDPR Lead and, where applicable, notified to Vistavue Ltd and the relevant NHS body.

All international transfer mechanisms in place must be documented in the RoPA and reviewed annually or upon any change in the adequacy status of the destination country.

12. Data Protection Impact Assessments

12.1 When a DPIA is Required

A DPIA is mandatory under Article 35 UK GDPR before commencing any processing that is likely to result in a high risk to individuals' rights and freedoms. Given the sensitive environments in which both networks operate, a DPIA is required for:

Trigger (Both Networks)	Trigger (Vistavue GP – Additional)
• Introduction of any new audience measurement technology • Large-scale processing of health-contextual data • Systematic processing using new technologies (AI, machine learning, computer vision) • Processing that could result in discrimination or denial of rights to individuals • Profiling of individuals (even if aggregated, where re-identification risk exists) • Transfer of personal data to a new third-country recipient	• Any new audience measurement methodology deployed within GP premises • Any data sharing with NHS bodies or integrated care boards • Any changes to the technical infrastructure of Vistavue GP screens • Introduction of any AI-based content personalisation on Vistavue GP screens • Any processing of data that could be linked (directly or indirectly) to patient attendance patterns

12.2 DPIA Process

- Campaign Managers or the GDPR Lead identify the need for a DPIA using the Company's DPIA Screening Checklist before any new processing activity commences.
- The DPIA is completed by the GDPR Lead in consultation with the relevant business team, technology partners, and (where applicable) the network operator.
- Where processing involves NHS premises or NHS-affiliated data flows, the relevant NHS Data Security and Protection lead must be consulted as part of the DPIA process.
- Where a DPIA identifies a high residual risk that cannot be mitigated to an acceptable level, the ICO must be consulted under Article 36 UK GDPR (prior consultation) before processing commences.
- All completed DPIAs are retained in the DPIA Register by the GDPR Lead and reviewed at least annually or upon any material change to the processing activity.

13. Network-Specific Compliance Obligations

13.1 HealthPoint TV Ltd – Pharmacy Screen Network

Compliance Area	Obligation
Audience Measurement	All audience data collected in pharmacy environments must be aggregated and anonymised. No individual-level health, purchasing, or prescription data may be collected or inferred. Privacy notices must be displayed at screen locations.
Campaign Content	All campaigns must comply with: CAP Code (Healthcare section); MHRA guidance on medicine advertising; Medicines Act 1968 and Human Medicines Regulations 2012; General Pharmaceutical Council (GPhC) standards applicable to pharmacy premises.
OTC Health Context	The Company acknowledges that pharmacy environments involve consumers engaging with over-the-counter health products. No campaign targeting may be designed to exploit health vulnerability or create undue pressure in a healthcare purchasing context.
Data Sharing with HealthPoint TV Ltd	A written data sharing / joint controller or Article 28 agreement must govern all data flows between MAL and HealthPoint TV Ltd. The allocation of data controller responsibilities must be expressly documented.
Children	Campaign content appropriate for the general pharmacy environment, which may include children. No audience data may be used to profile or target children.

13.2 Vistavue Ltd – GP Surgery Screen Network

Compliance Area	Obligation
NHS Data Security & Protection	All technology partners with data flows within NHS-affiliated GP premises must be assessed against and contractually required to comply with the NHS Data Security and Protection Toolkit. MAL

	must maintain its own DSP Toolkit compliance record where applicable.
Patient Data Firewall	No personal data processed by GP practices in connection with patient clinical care (medical records, appointment data, prescription records) may be accessed, processed, or linked to MAL's audience analytics activities under any circumstances. This is an absolute prohibition.
Audience Measurement	Privacy-by-design mandatory. Aggregated and anonymised data only. No biometric identification. No data capable of linking an individual's presence to a health condition. DPIA required for all new measurement technologies deployed in GP premises.
Campaign Content	All campaigns must comply with: CAP Code (Healthcare section); MHRA guidance; Human Medicines Regulations 2012; PMCPA Code of Practice (pharmaceutical advertisers); NHS England guidance on commercial activity in primary care premises. MAL will decline campaign creative that is inappropriate to a clinical waiting environment or conflicts with NHS public health messaging.
Patient Dignity	Campaign content must be reviewed for appropriateness in a GP surgery context. Content causing distress to unwell patients, undermining clinical authority, or creating a commercial atmosphere inconsistent with an NHS primary care environment is prohibited.
GMC / Professional Standards	MAL will not act in any manner that could cause a participating GP practice to breach its GMC obligations, CQC registration conditions, or GPhC standards applicable to any co-located pharmacy.
Data Sharing with Vistavue Ltd	A written agreement (Article 26 or Article 28 as applicable) must govern all data flows between MAL and Vistavue Ltd, incorporating NHS data security obligations. MAL must be notified immediately of any NHS data security incident affecting Vistavue GP network infrastructure.
Children in GP Waiting Rooms	Absolute prohibition on collecting, profiling, or targeting children from audience data. Campaign content reviewed for suitability in environments where children are regularly present.
NHS Incident Notification	Where a breach or security incident involves NHS-affiliated premises, MAL must notify Vistavue Ltd, the relevant NHS Data Security and Protection lead, and (where applicable) the relevant integrated care board in addition to ICO notification obligations.

14. Records of Processing Activities (RoPA)

The Company maintains a Record of Processing Activities (RoPA) as required by Article 30 UK GDPR. The RoPA records all processing activities carried out by the Company, both as a controller and as a processor, and must include:

- Name and contact details of the controller and, where applicable, the DPO;
- Purposes of processing;
- Categories of data subjects and personal data;
- Categories of recipients, including third countries or international organisations;

- Transfers to third countries and the safeguards in place;
- Retention periods; and
- A general description of technical and organisational security measures.

The RoPA is maintained by the GDPR Lead, reviewed quarterly, and updated immediately upon any new or materially changed processing activity. The RoPA must be made available to the ICO on request.

15. Staff Training and Awareness

- All new employees and contractors with access to personal data must complete mandatory GDPR induction training before being granted system access.
- All staff must complete annual GDPR refresher training. Completion is recorded and monitored by the GDPR Lead.
- Campaign Managers responsible for HealthPoint TV and Vistavue GP network accounts receive enhanced training covering healthcare-specific data protection obligations, NHS DSP Toolkit requirements (for Vistavue GP), and DPIA screening responsibilities.
- Technical staff responsible for audience measurement systems receive specific training on privacy-by-design principles and the technical safeguards required for health-adjacent environments.
- Training records are retained for a minimum of 3 years and are available for ICO inspection.
- The GDPR Lead provides a quarterly internal briefing on regulatory developments, ICO enforcement activity, and any changes to the Company's data protection practices.

16. Audit, Monitoring, and Policy Review

- The GDPR Lead conducts a formal annual audit of the Company's compliance with this Policy, reviewing the RoPA, DPIA register, DPA register, breach register, training records, and supplier compliance documentation.
- The results of the annual audit are reported to the Board and any material findings remediated within 90 days.
- Spot-check audits of audience measurement data practices for both networks are conducted at least twice per year.
- This Policy is reviewed and updated at least annually, or immediately upon any material change in the Company's processing activities, applicable law, or ICO guidance.
- The version history and document control table at the head of this Policy records all material revisions.
- All staff are notified of material policy changes and must confirm re-acknowledgement in writing.

17. Regulatory Engagement and Enforcement

Media Activation Ltd is committed to constructive engagement with the ICO and all relevant regulatory bodies. In the event of regulatory correspondence:

- All correspondence from the ICO must be directed to the GDPR Lead immediately and acknowledged within 5 business days.
- No substantive response to ICO correspondence may be issued without GDPR Lead and Board-level sign-off.
- Where the ICO conducts an assessment or investigation involving the Company's activities on either network, the relevant network operator (HealthPoint TV Ltd or Vistavue Ltd) will be notified promptly.
- The Company will cooperate fully and transparently with any ICO investigation, audit, or enforcement action.

In addition to ICO obligations, activities on the Vistavue GP network may engage the oversight of NHS England, the Care Quality Commission (CQC), and the Medicines and Healthcare products Regulatory Agency (MHRA). The Company will cooperate with all such bodies within the scope of their regulatory remit.

18. Governing Law

This Policy is governed by and construed in accordance with the laws of England and Wales. The Company’s primary data protection obligations arise under the UK GDPR and the Data Protection Act 2018. To the extent that the Company processes personal data of individuals located in the European Economic Area, the EU GDPR (Regulation (EU) 2016/679) may additionally apply, and the Company will ensure compliance with both instruments where relevant.

19. Policy Acknowledgement and Enforcement

This Policy is binding on all employees, contractors, consultants, and agency staff of Media Activation Ltd. All personnel with access to personal data processed in connection with HealthPoint TV Ltd or Vistavue Ltd campaigns must sign a Policy Acknowledgement Form upon commencement of their engagement and upon each material revision of this Policy.

Breach of this Policy may result in:

- Formal disciplinary action up to and including dismissal (for employees);
- Termination of contract (for contractors, consultants, and agency staff);
- Personal liability where breach results from wilful misconduct or gross negligence; and/or
- Referral to the ICO or other regulatory authority.

Board Approval	GDPR Lead Sign-Off
Signed: Julian Clogg Title: Date: 21 June 2026	Signed: Julian Clogg Title: Director Date: 21 June 2026

— END OF GDPR COMPLIANCE POLICY —

Media Activation Ltd | GDPR Compliance Policy v2.0 | 21 June 2026