

SAMPLE TEMPLATE

Data Processing Agreement

AGENTIC VISION LTD (trading as Vidcomply)

This public sample is provided for discussion and is subject to legal review, negotiation, and execution. It does not create binding obligations until signed by both parties.

This Data Processing Agreement ("Agreement") is made as of **[Effective Date]** between **[Data Controller]**, of **[Controller Address]** ("Controller"), and AGENTIC VISION LTD (trading as Vidcomply), 14 East Bay Lane, London, E15 2GW, Company No. 16720340 ("Processor"). Controller and Processor are together the "Parties".

1. Definitions

1.1 Data Protection Laws means applicable laws and regulations relating to personal data and privacy, including the UK GDPR, EU GDPR, the Data Protection Act 2018, and applicable United States privacy laws.

1.2 Personal Data means information relating to an identified or identifiable natural person.

1.3 Processing means any operation performed on Personal Data, including collection, storage, use, disclosure, restriction, erasure, or destruction.

1.4 Subprocessor means a third party appointed by Processor to process Personal Data for Controller.

1.5 Main Agreement means the principal agreement between Controller and Processor to which this Agreement relates.

2. Subject Matter and Duration

2.1 Subject Matter. This Agreement governs Processor's processing of Personal Data on behalf of Controller as described in Appendix A for the provision of media-compliance services, including ingestion, storage, analysis, and compliance verification using automated tools and AI models.

2.2 Duration. This Agreement begins on the Effective Date and continues until the Main Agreement ends, unless otherwise specified in Appendix A or terminated under Section 12.

3. Data Processing

3.1 Instructions. Processor will process Personal Data only as necessary to perform the Main Agreement and on Controller's documented instructions, unless applicable law requires otherwise. Where permitted, Processor will inform Controller of that legal requirement before processing.

3.2 Restriction on AI Training. Processor will not use Controller's Personal Data, uploaded video or audio, or outputs to train, retrain, or improve Processor's base AI or ML models. Processor will apply equivalent restrictions to Subprocessors where such contractual controls are available.

3.3 Compliance. Processor will comply with applicable Data Protection Laws and the principles of lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, and confidentiality.

3.4 Confidentiality. Processor will ensure authorised personnel are bound by confidentiality obligations and will maintain appropriate confidentiality procedures.

4. Data Subject Rights

4.1 Assistance. Taking into account the nature of processing, Processor will reasonably assist Controller, at Controller's cost where applicable, with requests concerning access, correction, erasure, restriction, portability, objection, and automated decision-making rights.

4.2 Requests. Processor will promptly notify Controller of a Data Subject request concerning Controller Personal Data and will respond only on Controller's documented instructions or as required by law.

5. Security Measures

5.1 Technical and Organisational Measures. Processor will maintain measures appropriate to risk, including encryption in transit and at rest; access controls; isolated processing and storage; resilience and recovery procedures; and processes for evaluating control effectiveness. The customer-specific deployment and any dedicated resources are defined in the applicable Order Form or Security Schedule.

5.2 Assessments and Audits. On reasonable prior notice and during normal business hours, Controller may request information reasonably necessary to demonstrate compliance. Audits will be coordinated to avoid unnecessary disruption and remain subject to confidentiality, security, and cost arrangements in the Main Agreement.

6. Subprocessing

6.1 Authorisation. Controller authorises Processor to engage the Subprocessors identified through Processor's current subprocessor notice and customer documentation. Processor will provide notice of material changes and an opportunity to object on reasonable data-protection grounds as agreed in the Main Agreement.

6.2 Flow-down and Liability. Processor will impose materially equivalent data-protection obligations on each Subprocessor and remains responsible for its Subprocessors' performance to the extent required by Data Protection Laws.

7. International Transfers

7.1 Locations. Hosting region, processing locations, and approved international transfers will be specified in the Order Form, Security Schedule, or current subprocessor notice applicable to Controller's deployment.

7.2 Safeguards. Processor will implement an appropriate transfer mechanism where Data Protection Laws require one, such as adequacy regulations, the UK International Data Transfer Addendum, or approved Standard Contractual Clauses.

8. Personal Data Breach

8.1 Notification. Processor will notify Controller without undue delay after becoming aware of a Personal Data breach affecting Controller Personal Data and, where contractually agreed, within 72 hours. Notification will include available details about the nature, scope, likely consequences, contact point, and mitigation measures.

8.2 Cooperation. Processor will take reasonable corrective action and cooperate with Controller's lawful response, mitigation, and notification obligations.

9. Retention, Return, and Deletion

9.1 Retention. Processor will retain Personal Data only for the period agreed in the Main Agreement, Order Form, or Security Schedule, or as required by law.

9.2 Return or Deletion. At the end of the Main Agreement or on Controller's written request, Processor will return or delete Controller Personal Data as instructed, unless law requires retention. Processor will provide written confirmation within the contractually agreed period, which is ordinarily 30 days.

10. Liability and Indemnity

10.1 Liability. Each Party's liability under this Agreement is subject to the limitations and exclusions in the Main Agreement, except where liability cannot lawfully be limited.

10.2 Indemnity. Any indemnity concerning a breach of this Agreement will be governed by the Main Agreement and applicable law.

11. General

11.1 Amendments. Amendments must be in writing and signed by both Parties, except updates expressly permitted under the Main Agreement.

11.2 Governing Law. Unless the Main Agreement states otherwise, this Agreement is governed by the laws of England and Wales and the courts specified in the Main Agreement have jurisdiction.

11.3 Confidentiality. Each Party will protect confidential information received under this Agreement and disclose it only as permitted by the Main Agreement or required by law.

11.4 Severability and Notices. Invalid terms will be interpreted or severed without affecting remaining terms. Notices must be provided using the method specified in the Main Agreement.

12. Termination

12.1 Relationship to Main Agreement. This Agreement terminates when Processor has ceased processing Controller Personal Data after termination or expiry of the Main Agreement, unless the Parties agree otherwise.

12.2 Survival. Confidentiality, return or deletion, audit, liability, and other provisions intended by their nature to survive will remain effective.

SIGNATURES

Execution

The Parties have executed this Data Processing Agreement as of the Effective Date.

CONTROLLER	PROCESSOR
[Controller legal name] Name: _____ Title: _____ Date: _____	AGENTIC VISION LTD (trading as Vidcomply) Name: _____ Title: _____ Date: _____

APPENDIX A

Details of Processing

1. Nature and Purpose

Processor provides media-compliance services to Controller. Processing may include secure ingestion, storage, analysis, and generation of compliance evidence, reports, alerts, or approved workflow outputs.

The enabled processing stages, data flows, and integrations are limited to the services selected in the Order Form or Security Schedule.

2. Duration and Retention

Processing continues for the term of the Main Agreement. Retention periods are specified in the Order Form or Security Schedule. At the end of the agreed period, Personal Data is returned or securely deleted, subject to legal retention obligations.

3. Categories of Data Subjects

Individuals appearing or heard in customer-provided media; customer personnel and authorised users; and other individuals whose Personal Data is included in customer-provided content or metadata.

4. Types of Personal Data

Video and audio recordings; images, voices, actions, and contextual identifiers; media metadata; transcripts and derived analysis; and authorised user account information. Special-category or sensitive data may be processed only where present in customer-provided content and lawfully instructed by Controller.

5. Hosting Region and Data Residency

Hosting region: As specified in the applicable Order Form or Security Schedule.

Data residency and transfers: As specified for the selected deployment and approved services. Customer-specific commitments take precedence over this sample.

6. Approved Subprocessors

The current public overview is maintained at <https://www.vidcomply.ai/security/subprocessors.html>. The customer-specific list, permitted purposes, locations, and transfer safeguards are confirmed in the Order Form, Security Schedule, or executed DPA.

7. Technical and Organisational Measures

Measures may include TLS 1.2+ in transit; AES-256 or AWS KMS-backed encryption at rest; logically isolated storage and processing; dedicated resources where agreed; MFA and role-based access; restricted administrative access; infrastructure and API logging; controlled network ingress and egress; recovery procedures; vulnerability management; and incident-response processes.

CUSTOMER-SPECIFIC SCHEDULE

The final executed DPA should attach or reference the applicable Order Form and Security Schedule. Those documents define the actual region, subprocessors, retention period, enabled integrations, security commitments, and any negotiated audit terms.