VIDIZMO.AI

VIDIZMO DATA PROCESSING AGREEMENT

Last Updated: August 2025

TABLE OF CONTENT

This DPA applies to VIDIZMO, LLC ("vidizmo.ai"), including its subsidiaries and affiliates, in both direct Controller–Processor relationships and Sub-Processor roles under a primary Processor.

1. Definitions

For the purposes of this Data Processing Agreement (DPA), the following terms shall have the meanings set forth below:

- "Controller" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal or Customer's Data.
- "Processor" means the entity that processes Customer Data on behalf of the Controller.
- "Sub-Processor" means any third-party processor engaged by the Processor or by any other Sub-Processor who agrees to process Personal or Customer's Data on behalf of the Controller and in accordance with the Controller's instructions and this DPA.
- "Customer" means the individual or legal entity, including its subsidiaries and affiliates, that enters into an agreement with VIDIZMO, LLC (vidizmo.ai) for the use of its products or services. For the purposes of this DPA, the Customer acts as the Controller (or, where applicable, has been authorized by a Controller) and determines the purposes and means of processing Personal or Customer's Data that is submitted to VIDIZMO, LLC for processing in connection with the provision of Services.
- "Personal Data" means any information relating to an identified or identifiable natural person ("Data Subject"), as defined under the General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA/CPRA), and other applicable privacy laws.
- "Customer's Data" means any data, information, or content—including Personal Data—submitted by, for, or on behalf of the Customer to VIDIZMO, LLC (vidizmo.ai) for processing in connection with the provision of Services, as defined in this DPA.
- "Processing" refers to any operation or set of operations performed on Customer's Data or Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.
- "Data Subject" means any identified or identifiable natural person whose Personal Data is processed.
- "Applicable Data Protection Laws" refers to all laws and regulations relating to the Processing of Customer Data under this DPA, including but not limited to the GDPR, UK GDPR, CCPA/CPRA, and other relevant state, federal, or international privacy regulations.
- "Anonymization" means the processing of Customer Data in such a manner that the data can no longer be attributed to a specific Data Subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures.
- "Pseudonymization" means the processing of Customer Data in such a way that the Customer Data can no longer be attributed to a specific Data Subject without the use of

additional information, provided that such additional information is kept separately and is subject to technical and organizational measures.

- "Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data transmitted, stored, or otherwise processed.
- "Services" means the AI-driven products and services provided by VIDIZMO, LLC (vidizmo.ai), including but not limited to Digital Evidence Management, Redaction Solutions, Enterprise Video Content Management, VIDIZMO AI Platform, and related modules, as described in the Scope of this DPA.

2. Purpose and Scope

This Data Processing Agreement (DPA) establishes the framework for the processing of Customer's Data by VIDIZMO, LLC (vidizmo.ai) in connection with its suite of AI-powered products and services. The agreement applies to a range of offerings, including:

- Digital Evidence Management
- Redaction Solutions
- Enterprise Video Content Management
- The VIDIZMO AI Platform and its associated solutions
- AI & Machine Learning (ML) modules, encompassing model training, inference, and analytics

The DPA is designed to ensure that all handling of Customer's Data aligns with strict regulatory standards and legal requirements. VIDIZMO, LLC's processing activities are governed by, and maintain compliance with, the following regulations and frameworks:

- General Data Protection Regulation (GDPR), UK GDPR, and related EU data protection legislation
- United States Federal laws, including HIPAA, the Federal Trade Commission Act, and the Criminal Justice Information Services (CJIS) Security Policy
- State-specific privacy statutes within the US, such as CCPA/CPRA, Virginia CDPA, Colorado CPA, Connecticut DPA, Utah CPA, and Texas DPSA
- Additional global privacy regulations that may be applicable to the Customer's Data processed by VIDIZMO, LLC

By setting forth clear standards and responsibilities for both Controller and Processor roles, this DPA provides a comprehensive structure for the secure, lawful, and transparent processing of Customer's Data throughout all stages of service delivery.

3. Roles and Responsibilities

VIDIZMO may act in different capacities when processing Customer Data:

Processor: When acting on behalf of a Data Controller, VIDIZMO processes Customer Data as directed by the Controller and according to the terms of this DPA.

Sub-Processor: When engaged by a primary Processor under a contract with the Data Controller, VIDIZMO acts based on the instructions received from the Processor. In this role, VIDIZMO provides the technical platform and tools that allow the Processor to set and enforce their own data handling policies, security measures, and compliance requirements. VIDIZMO's responsibility is limited to making these technical options available; it does not monitor, audit, or enforce the Processor's internal policies. Oversight and enforcement of such policies remain the responsibility of the Processor.

VIDIZMO will:

- Process Customer Data only as permitted by the Controller or Processor, in line with applicable data protection laws and contractual agreements.
- Offer administrative features in the software to support Processor-defined policy settings, such as data access controls, retention options, audit logs, and security configurations.
- Ensure that, when acting as Sub-Processor, all data processing activities follow instructions provided by the Processor through VIDIZMO's technical interface, without taking further operational responsibility beyond offering these configuration capabilities.

4. Data Processing Activities

VIDIZMO may process customers' data for a variety of purposes essential to the provision and enhancement of services. These purposes include, but are not limited to:

- Service delivery and ongoing platform maintenance, ensuring that customers' data is used solely to fulfill contractual obligations and support service functionality.
- AI-powered analytics and automation features, strictly governed by the parameters established by the Controller or primary Processor, and always in accordance with the documented instructions and requirements set forth in this DPA.
- Training and continuous improvement of AI and machine learning models, as detailed in Clause 6 of this DPA. Customer data will only be used for model development if permitted under the agreed-upon terms, with appropriate safeguards for privacy and security in place.
- Security threat detection, incident prevention, and timely response activities, where customers' data may be analyzed or monitored to maintain the integrity, confidentiality, and availability of the platform and related services.
- Provision of customer support, where access to customers' data is limited to authorized personnel and strictly for the purpose of resolving technical issues, service requests, or incidents in a manner consistent with contractual and regulatory obligations.

All processing of customers' data under this DPA is governed by strict adherence to the Controller's or Processor's instructions, as well as applicable data protection laws and contractual commitments. VIDIZMO implements robust technical and organizational measures to ensure that all processing activities are transparent, auditable, and limited to what is necessary for the performance of the specified services.

5. Data Minimization and Privacy by Design

VIDIZMO employs data minimization practices across its platform, ensuring that the processing of customers' data is limited strictly to what is necessary for fulfilling contractual obligations and enhancing service performance.

Privacy-by-design principles are embedded in all AI workflows and operational procedures. From the very beginning, technical and organizational safeguards are implemented to ensure ongoing adherence to applicable data protection laws and contractual requirements.

All data processing is guided by the configurations and instructions provided by the Customer (Controller) or, when relevant, the primary Processor. VIDIZMO processes customers' data only according to these documented instructions and selected configurations. When acting as a sub-processor, VIDIZMO handles customers' data solely within the boundaries defined by the primary Processor and the Controller's contractual framework.

These measures guarantee that customers' data is never processed beyond what is explicitly authorized. Customers maintain control over how their data is managed within the platform, supported by transparency and accountability throughout all operations.

6. Use of Data for AI and ML Training

VIDIZMO processes customer data for the purposes of training, refining, and enhancing artificial intelligence (AI) and machine learning (ML) models solely in accordance with the documented instructions and valid consent of the Controller or, where applicable, the Processor. Unless otherwise specified by the Controller in writing, data may be used for these purposes subject to the constraints set out in the Data Processing Agreement (DPA) and applicable law.

Where VIDIZMO acts as a Sub-Processor, use of customer data for AI/ML training is contingent upon explicit, written authorization from both the primary Processor and the Controller. The scope and nature of such processing shall remain strictly limited to that which is authorized under the governing contractual framework and relevant legislation.

VIDIZMO implements the following safeguards during AI/ML training processes:

- Data is subject to anonymization prior to use in model development to mitigate the risk of identification.
- Customer data is segregated, ensuring separation of datasets and restricting unauthorized access.

- Access to data is limited to authorized personnel and is subject to internal controls and audit trails.
- Retention periods for training data are established and enforced, with secure deletion protocols implemented upon expiry.

At all times, the Controller maintains authority to opt out of data usage for AI/ML training by written instruction; VIDIZMO will cease such processing immediately upon receipt of such notice. Opt-out may affect certain service features that rely on AI/ML capabilities, but shall not interfere with core platform functions. All processing activities are documented and available for audit.

These provisions are incorporated into the DPA to ensure that use of customer data for AI and ML training is governed by explicit consent, contractual limitations, and appropriate technical and organizational safeguards.

Additionally, reference is made to the Addendum: Compliance and Effectiveness in PII Redaction, which articulates not only the methodologies and compliance criteria for protecting personally identifiable information (PII), but also provides a thorough rationale for why training on customer data is essential for developing more effective AI models. The Addendum sets out how such data use aligns with various legal frameworks and demonstrates the necessity of incorporating real-world customer datasets to improve AI accuracy, reliability, and compliance with applicable laws. This approach underscores VIDIZMO's commitment to transparency, regulatory adherence, and ongoing enhancement of AI solutions, while ensuring robust protection of customer privacy throughout the data processing lifecycle.

7. Engagement of Sub-Processors

VIDIZMO may engage sub-processors to assist in the processing of customer data under the DPA. Customers will be provided with a minimum of 30 days' advance notice prior to the appointment of any new sub-processor, unless immediate engagement is required to comply with legal or regulatory requirements. Customers retain the right to review and, where permitted by applicable law or contractual terms, object to the engagement of new sub-processors.

VIDIZMO shall ensure that all sub-processors are bound by written agreements that impose data protection obligations equivalent to those set forth in this DPA. These agreements require sub-processors to implement security, confidentiality, and data protection measures consistent with VIDIZMO's standards.

VIDIZMO remains responsible and liable for the performance of its sub-processors. In the event that a sub-processor fails to meet its data protection obligations, VIDIZMO shall take appropriate steps to investigate, notify affected parties as required, and implement remediation measures in accordance with the terms of this DPA.

This section is intended to ensure transparency in the selection and oversight of sub-processors, and to provide assurance that customer data will be processed in accordance with contractual and regulatory requirements throughout the data processing lifecycle.

8. International Data Transfers

VIDIZMO shall implement procedures to ensure that transfers of customer data outside a jurisdiction's borders are compliant with applicable data protection laws. International transfers shall utilize mechanisms including Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other safeguards as required by the General Data Protection Regulation (GDPR) or relevant data privacy frameworks.

Where customer data is transferred outside the European Economic Area (EEA) or other regions with similar transfer restrictions, such transfers shall occur only to recipients that provide an adequate level of protection, as defined by applicable law. VIDIZMO will review and update transfer mechanisms as necessary to account for changes in the legal and regulatory environment.

For customer data governed by U.S. law enforcement regulations, including data subject to Criminal Justice Information Services (CJIS) requirements, all hosting and processing activities shall be limited to CJIS-compliant facilities within the United States.

These provisions form part of the DPA to ensure compliance, transparency, and accountability in the conduct of international data transfers.

9. Physical and Environmental Security

VIDIZMO leverages the robust physical security measures of Microsoft Azure data centers, which include facility access controls, visitor management protocols, and environmental protections. These data centers are specifically designed to prevent unauthorized access, tampering, and physical damage to Customer Data. In addition, data stored in Azure is safeguarded through multi-layered security protocols, ensuring that all Customer Personal Data remains protected from both physical and environmental threats.

10. Business Continuity and Disaster Recovery

VIDIZMO ensures business continuity through the use of Geo-Redundant Storage (GRS) in Microsoft Azure, delivering high availability and resilience. In the event of a service disruption, established backup and recovery procedures enable rapid and secure restoration of Customer Data. These procedures are regularly tested to validate their effectiveness, ensuring that VIDIZMO can meet recovery objectives, minimize downtime, and maintain uninterrupted access to data.

11. Data Subject Rights

VIDIZMO shall support Controllers and primary Processors in fulfilling their obligations with respect to Data Subject rights under applicable data protection laws, including but not limited to the GDPR.

Upon receipt of a Data Subject Access Request (DSAR), or any request relating to access, rectification, erasure, restriction of processing, objection, or data portability, VIDIZMO will notify the Controller or primary Processor without undue delay and in any event within 2 business days.

VIDIZMO, acting on the documented instructions of the Controller or primary Processor, shall implement appropriate technical and organizational measures to assist in addressing such requests. This support may include facilitating access to, correction or erasure of, or restriction of processing of customer data, as instructed.

In cases where sub-processors are involved, VIDIZMO shall ensure that relevant requests are communicated to the sub-processor and that the sub-processor cooperates to address the data subject request in a timely manner.

All actions in response to data subject requests shall be recorded as evidence of compliance with the obligations set forth in this DPA.

These procedures are incorporated into the DPA to enable Controllers and primary Processors to comply with their legal obligations regarding Data Subject rights.

12. Data Protection Impact Assessments (DPIAs)

VIDIZMO conducts Data Protection Impact Assessments (DPIAs) for any new or significantly changed processing activities that may affect Customer Personal Data, particularly those deemed high-risk under applicable Data Protection Laws (including GDPR). DPIAs are performed to identify and evaluate potential privacy risks and to ensure that appropriate safeguards are implemented before the commencement of processing. This proactive approach supports compliance and enhances the protection of Customer Data. For more information, please visit VIDIZMO Security Overview.

13. Data Retention and Deletion

Upon termination of processing activities governed by this Agreement, VIDIZMO shall, at the instruction of the Controller or primary Processor, promptly delete or return all Customer's Data processed on behalf of the Controller or primary Processor. This obligation applies unless applicable law or regulatory requirements require continued retention of such data. In circumstances where retention is mandated by law or regulation, VIDIZMO shall ensure that the Customer's Data is securely isolated and protected from any further processing, except as necessary to comply with the applicable legal or regulatory obligations.

All deletion activities shall be executed using industry-standard methods designed to ensure the complete and irreversible removal of Customer's Data from VIDIZMO's systems, except where retention is lawfully required. VIDIZMO shall, upon request, provide written confirmation of the deletion or return of Customer's Data to the Controller or primary Processor.

Furthermore, VIDIZMO shall not retain Customer's Data beyond the expiration of the processing relationship except where required by applicable law, regulation, or judicial order. In such cases, VIDIZMO agrees to maintain the confidentiality and security of all retained Customer's Data in accordance with the terms of this Agreement, and shall not access, use, or disclose the Customer's Data except as strictly necessary to fulfill legal obligations.

Any exceptions to the foregoing requirements must be agreed in writing by the Controller or primary Processor and VIDIZMO, and shall specify the legal basis, duration, and measures taken to ensure ongoing protection of the retained Customer's Data.

All actions related to data deletion, return, or continued retention shall be documented by VIDIZMO and made available to the Controller or primary Processor upon request, as evidence of compliance with this section and applicable law.

14. Liability and Indemnification

VIDIZMO shall be responsible for any breach of this Agreement or applicable data protection laws caused by its acts or omissions, including those of any sub-processors engaged on its behalf. Where the involvement of a sub-processor results in a breach of obligations equivalent to those imposed on vidizmo.ai under this Agreement, vidizmo.ai shall remain liable to the Controller or primary Processor for the performance of the sub-processor's obligations.

Unless otherwise expressly specified in the primary contract or this Agreement, any limitations on liability, monetary caps, or indemnification obligations relating to data protection shall be as provided in the principal agreement governing the processing relationship between the parties. In the absence of such stipulations, the parties agree that vidizmo.ai shall indemnify and hold harmless the Controller or primary Processor from and against any direct losses, claims, damages, expenses, or fines imposed by regulatory authorities as a result of proven breaches attributable to vidizmo.ai or its sub-processors.

The Controller or primary Processor agrees that, to the extent permitted by applicable law, no party shall be liable for indirect, consequential, or punitive damages arising from the performance or non-performance of obligations under this Agreement, except in cases of gross negligence, willful misconduct, or where otherwise mandated by law.

Any claims for indemnification or damages shall be subject to the notice, cooperation, and mitigation requirements as may be stipulated in the primary agreement or, where not specified, as required by applicable law.

The provisions of this section shall survive termination of this Agreement for so long as either party retains Customer Data processed under this Agreement.

Unless otherwise expressly specified in this Agreement, any limitations on liability, monetary caps, or indemnification obligations relating to data protection shall be as provided in the VIDIZMO Subscription Service Agreement governing the provision of Services to the Customer. This limitation shall apply to all claims under this Data Processing Agreement, including indemnification obligations, except to the extent prohibited by applicable law.

15. Governing Law and Jurisdiction

This DPA is governed by the laws of Virginia, USA, unless otherwise specified in the primary agreement when vidizmo.ai acts as a Sub-Processor.

16. Term and Termination

Upon termination of this Agreement, the requirements and procedures for deletion or return of Customer's Data shall be as set forth in Section 13 (Data Retention and Deletion). The parties shall comply with all obligations outlined in Section 13 regarding the handling, retention, and destruction of Customer's Data.

Any exceptions to these requirements must be documented and agreed in writing by the Controller or primary Processor and vidizmo.ai, specifying the legal basis for retention, the duration of such retention, and the measures for continued protection and confidentiality of Customer's Data.

The obligations pertaining to audit rights, cooperation, and notification of security incidents shall continue to apply following termination of this Agreement for so long as Customer's Data remains in the custody or control of vidizmo.ai or any sub-processor. All actions taken in fulfillment of these obligations shall be fully documented and made available to the Controller or primary Processor upon request to demonstrate compliance with this section and applicable law.

ADDENDUM: COMPLIANCE AND EFFECTIVENESS IN PII REDACTION

This addendum supplements the main Data Processing Agreement and is to be referenced in conjunction with all relevant sections regarding the processing, handling, and protection of Customer's Data. It addresses the compliance obligations and effectiveness requirements associated with the redaction of Personally Identifiable Information (PII), with particular attention to the necessity of using actual customer data to train automated AI/ML-based redaction systems. The provisions herein elaborate on statutory and contractual requirements impacting both the Controller and Processor in the context of operationalizing automated PII redaction.

Accuracy Requirements under Data Protection Laws: Pursuant to GDPR Article 5(1)(d) and corresponding provisions in CCPA/CPRA and Virginia CDPA, the Controller and Processor must ensure that customer data is processed with accuracy and integrity. The effectiveness of automated PII redaction, a core function of VIDIZMO's product, closely depends on the quality and relevance of the training data used for AI/ML models.

Necessity of Customer-Specific Training Data: Generic training datasets cannot account for unique data formats, document structures, or domain-specific terminologies present in each customer's operational environment. Training AI/ML models on actual customer data enables the Processor and Controller to calibrate redaction tools to the specific context, thereby enhancing the precision and reliability of PII identification and redaction.

Lawful Basis for Anonymization and Training: When customer data is anonymized according to GDPR Recital 26 and equivalent standards under CCPA/CPRA, such information is no longer subject to Customer Data restrictions and may be lawfully used for enhancing AI/ML model performance. Current data protection agreements and opt-out provisions empower customers with control over the use of their data for training purposes.

Enforcement of Statutory Obligations: Improving AI/ML redaction capabilities through training on customer data is essential to uphold data subject rights and statutory obligations, such as the right to erasure, rectification, and restriction of processing under the GDPR, as well as consumer rights to information and deletion under CCPA/CPRA. Enhanced AI/ML performance supports the Processor and Controller in fulfilling these responsibilities with demonstrable compliance.

Security and Law Enforcement Data: In environments governed by CJIS or similar regulatory frameworks, documented training and audit protocols utilizing customer data are necessary to ensure that automated redaction meets the stringent legal standards applicable to sensitive law enforcement information.

In summary, automated PII redaction using AI/ML models must be trained on actual customer data to ensure compliance with relevant data protection statutes and to achieve the accuracy and reliability required in operational settings. The Controller and Processor acknowledge that such training is fundamental to providing compliant and effective redaction services under this Agreement, subject at all times to applicable safeguards, documentation requirements, and customer control mechanisms as outlined herein.