



Privacy Notice

Policy





Contents

Introduction	3
Who we are	3
Data Controller and Data Processor Roles	3
Personal Data we Collect	4
Special Category Data	6
Website Visitors and Marketing Communications	6
Cookies and Website Analytics	6
How we use Personal Data	7
Service Analytics and Product Improvement	7
Lawful Basis for Processing	7
Identity Verification, AML and Fraud Prevention	8
Electronic Signatures and Qualified Electronic Signatures (QES)	9
Integrations and Third-Party Services	9
Customer Data Storage Options	9
Sharing Personal Data	10
Data Security	11
Data Breaches	11
International Data Transfers	11
Data Retention	12
Individual Rights	13
Complaints Regarding your Personal Data	13
Changes to this Privacy Notice	14



Introduction

Videosign Limited ("Videosign", "we", "us" or "our") is committed to protecting and respecting personal data and privacy rights in accordance with the UK General Data Protection Regulation ("UK GDPR"), the Data Protection Act 2018, the Privacy and Electronic Communications Regulations (PECR) and other applicable data protection legislation.

This Privacy Notice explains how Videosign collects, uses, stores, shares and protects personal data when providing its services, operating its websites, engaging with customers, suppliers and prospective customers, and supporting users of the Videosign platform.

Who we are

Videosign Limited is a Software-as-a-Service (SaaS) provider offering digital customer engagement, identity verification, remote meetings, document collaboration, electronic signatures, compliance evidence capture and workflow orchestration services.

For privacy enquiries, please contact enquiries@videosign.co.uk (marked FAO Data Protection Lead).

Individuals also have the right to lodge a complaint with the Information Commissioner's Office (ICO) at www.ico.org.uk.

Data Controller and Data Processor Roles

Videosign as Data Controller

Videosign acts as Data Controller in relation to its own business operations, including:

- Customer account contacts
- User accounts created directly with Videosign
- Billing contacts
- Supplier contacts
- Employee and contractor records
- Website visitors
- Marketing contacts and prospects
- Customer support interactions
- Financial and invoicing information
- Contract management records
- Account management activities



Videosign as Data Processor

Videosign acts as Data Processor when providing services to customers using the Videosign platform, including:

- Customer meeting recordings
- Client documents
- Identity verification results
- Signature records
- Audit trails
- Customer communications
- Uploaded evidence
- Customer onboarding information

In these circumstances, our customer is typically the Data Controller and determines the purposes and means of processing.

Personal Data we Collect

Videosign will only collect personal data need to fulfil the service being provided. This may include:

Contact Information • Name • Email address • Telephone number • Job title • Organisation name
Account Information • User credentials • Login and authentication records • User preferences • Service usage data
Customer Account and Billing Information • Billing contact details • Invoice information • Payment and transaction records • Contractual information • Subscription and service usage information
Customer Engagement Data Depending on the services used by our customers, Videosign may process meeting recordings, audio recordings, chat messages, shared documents, electronic signatures and associated audit records. Storage and retention of these records may be determined by customer configuration and contractual requirements. • Meeting attendance records • Meeting recordings



- Chat messages
- Shared documents
- Electronic signature records
- Audit trail information

Identity Verification Data

Where enabled by customers, Videosign may process identity verification information through integrated verification providers.

This may include:

- Name
- Address
- Date of birth
- Identity document information
- Identity verification outcomes
- AML screening results
- PEP and sanctions screening results
- Fraud indicators
- Verification audit records

Biometric Information

Where customers deploy biometric identity verification services, Videosign may process biometric verification results provided by integrated identity verification providers.

This may include:

- Facial comparison results
- Liveness detection results
- Verification confidence scores
- Fraud and spoofing indicators

Videosign does not use biometric information for profiling, marketing or unrelated purposes.

Compliance and Audit Data

Videosign may generate and retain audit records relating to:

- User authentication
- Meeting attendance
- Identity verification events
- Electronic signatures
- Document access and sharing
- Consent capture
- Workflow actions
- Administrative activity

These records support regulatory compliance, fraud prevention, dispute resolution and service security.



Videosign primarily uses hosting providers with infrastructure located within the UK and EEA. Where international data transfers occur, appropriate safeguards are implemented in accordance with UK GDPR.

Special Category Data

Videosign does not generally require the collection of Special Category Data. However, depending on customer use cases, regulated industry requirements or identity verification services, certain categories of Special Category Data may be processed where permitted by applicable law and subject to appropriate safeguards.

Where Special Category Data is processed, Videosign and its customers will ensure an appropriate lawful basis, condition for processing and appropriate safeguards are in place.

Website Visitors and Marketing Communications

This Privacy Notice applies to visitors to the Videosign website and users of Videosign services.

When individuals visit our website, contact us, request information, attend events or subscribe to marketing communications, Videosign acts as Data Controller for the personal data collected in connection with those activities.

Personal data collected may include:

- Name
- Organisation
- Job title
- Email address
- Telephone number
- Website usage information

Such information is used to respond to enquiries, provide requested information, manage business relationships, improve our services and administer our website.

Cookies and Website Analytics

Videosign uses cookies and similar technologies to support website functionality, security and analytics.

Further information regarding the cookies used by Videosign is available within our Cookie Policy.



How we use Personal Data

Videosign processes personal data in accordance with applicable data protection legislation and applies appropriate governance, security and access controls to ensure personal data is handled lawfully, fairly, transparently and securely. This Privacy Notice explains how Videosign collects, uses, stores, shares and protects personal data when providing its services and conducting its business operations.

Videosign processes personal data for the following purposes:

- Delivering contracted services
- Identity verification and fraud prevention
- Customer onboarding
- Electronic signatures and document execution
- Compliance and audit evidence
- Platform security and monitoring
- Customer support
- Billing and financial administration
- Regulatory compliance
- Product improvement and service optimisation
- Recruitment and employment administration

Access to personal data is restricted to authorised personnel who require access for legitimate business, operational, support, security or regulatory purposes.

Where Videosign engages third-party service providers, appropriate contractual, technical and organisational measures are implemented to ensure personal data is processed securely and in accordance with applicable data protection legislation.

Service Analytics and Product Improvement

Videosign may create aggregated or anonymised statistical information relating to platform usage, service performance and operational metrics. Such information does not identify individuals and cannot reasonably be used to identify a person. We use this information to improve services, enhance security, support operational reporting and develop new functionality.

Lawful Basis for Processing

Depending on the activity, Videosign relies upon one or more of the following lawful bases:

Contract

Processing necessary to provide services under a contract. Examples include:

- User account management
- Meeting services
- Identity verification services
- Electronic signatures
- Customer onboarding
- Compliance evidence capture



• Regulatory record keeping associated with customer interactions and advice processes
Legal Obligation Processing necessary to comply with legal or regulatory requirements. Examples: • Financial records • Billing and taxation records • Regulatory audit requirements • Legal and regulatory reporting obligations
Legitimate Interests Processing necessary for legitimate business interests where these interests do not override individual rights. Examples: • Information security • Service monitoring • Fraud prevention • Business continuity • Customer support
Consent Where required by law, Videosign will obtain consent before processing specific categories of data or undertaking certain activities.
Vital Interests Processing necessary to protect an individual's vital interests where required by law.

Identity Verification, AML and Fraud Prevention

Videosign provides identity verification services through integrated specialist providers. Verification services may include:

- Identity document verification
- Facial biometric verification
- Liveness detection
- Bank-based identity verification
- AML screening
- PEP screening
- Sanctions screening
- Fraud detection checks

Verification services are configured and controlled by the customer organisation using the Videosign platform.

Videosign processes verification data solely for authorised verification and compliance purposes.



Videosign does not make legally significant decisions about individuals solely through automated processing.

Where integrated identity verification, fraud prevention or compliance screening providers use automated technologies to support verification decisions, risk assessment or fraud detection, such processing is undertaken within customer-defined workflows and human review remains available where appropriate.

Electronic Signatures and Qualified Electronic Signatures (QES)

Videosign supports electronic signature services, including:

- Digital Signatures
- Advanced Electronic Signatures (AES)
- Qualified Electronic Signatures (QES)

Where QES services are used, additional identity verification and certificate issuance information may be processed through approved trust service providers.

Integrations and Third-Party Services

Videosign provides APIs and integration capabilities that enable customers to connect the platform to third-party applications, identity verification services, CRM systems, document repositories and other business systems.

Customers are responsible for selecting and authorising the third-party services they choose to connect to the Videosign platform.

Where personal data is shared with customer-authorised third parties, Videosign processes such data in accordance with customer instructions and the applicable contractual arrangements.

Where customers use Videosign to process personal data relating to their customers, prospects or employees, Videosign typically acts as Data Processor and the customer acts as Data Controller.

Where personal data is transferred to third-party systems selected by the customer, subsequent processing of that data will be governed by the applicable third-party provider's privacy policies, contractual terms and data protection obligations.

Customer Data Storage Options

Videosign supports multiple deployment and storage models depending on customer requirements.

These may include:

- Videosign-managed secure cloud storage.
- Customer-managed cloud storage repositories.
- Customer-managed on-premise storage environments.



Depending on the selected deployment model, Videosign may store customer content directly, retain references to customer-managed content, or process data on behalf of customers within their chosen storage environment.

The applicable processing arrangements will be documented within the relevant contractual and data processing agreements.

Sharing Personal Data

Videosign may share personal data with carefully selected third parties where necessary to deliver services, comply with legal obligations, support business operations or fulfil customer instructions.

These parties may include:

- Cloud hosting and infrastructure providers.
- Identity verification providers.
- Qualified trust service and electronic signature providers.
- CRM, workflow and integration partners.
- Customer-authorised third-party systems and applications.
- Professional advisers, auditors and insurers.
- Regulators, courts, law enforcement agencies and other public authorities where legally required.

Where Videosign acts as a Data Processor, personal data is processed and shared only in accordance with the documented instructions of the customer acting as Data Controller.

Where customers choose to integrate Videosign with third-party applications, document repositories, CRM platforms or other business systems, personal data may be exchanged with those systems as part of the customer-configured workflow. Customers remain responsible for selecting and authorising the third-party services connected to their Videosign environment.

Videosign uses carefully selected third-party service providers ("sub-processors") to support delivery of its services. These sub-processors may provide services relating to:

- Cloud infrastructure and hosting.
- Communications services.
- Identity verification.
- Electronic signatures and trust services.
- Customer support.
- Security monitoring and operational resilience.

Appropriate contractual, technical and organisational safeguards are implemented to ensure personal data is processed securely, confidentially and in accordance with applicable data protection legislation.

A current list of significant sub-processors is available upon request or through customer contractual documentation.



Videosign does not sell personal data and does not permit third parties to use personal data for their own marketing purposes.

Where personal data is transferred internationally, appropriate safeguards are implemented as described in the International Data Transfers section of this Privacy Notice.

Data Security

Videosign maintains appropriate technical and organisational security measures designed to protect personal data against unauthorised access, disclosure, alteration or destruction.

These measures include:

- Encryption in transit
- Encryption at rest where applicable
- Access controls
- Multi-factor authentication
- Security monitoring
- Vulnerability management
- Audit logging
- Backup and disaster recovery processes
- Staff training and awareness programmes

Data Breaches

Videosign maintains incident management and personal data breach response procedures designed to identify, assess, investigate and remediate security incidents involving personal data.

Where a personal data breach occurs, Videosign will assess the nature and impact of the incident and take appropriate steps to contain, investigate and remediate the issue.

Where required by applicable law, Videosign will notify the relevant supervisory authority and affected customers or individuals within the applicable regulatory timescales.

Videosign maintains appropriate technical and organisational measures, including security monitoring, access controls, employee training and business continuity processes, to reduce the likelihood and impact of personal data breaches.

International Data Transfers

Videosign may use service providers located outside the United Kingdom or European Economic Area.

Videosign operates a cloud-based service and may use service providers located in multiple jurisdictions. Personal data may therefore be processed in countries outside the UK or EEA where appropriate safeguards are in place.



Where international transfers occur, Videosign implements appropriate safeguards, including:

- UK International Data Transfer Agreement (IDTA)
- UK Addendum to EU Standard Contractual Clauses
- European Commission Standard Contractual Clauses
- Adequacy decisions where available

Where required to deliver services, Videosign may engage approved sub-processors and service providers. Appropriate contractual, technical and organisational safeguards are implemented to ensure personal data remains protected and is processed only for authorised purposes.

Prior to engaging service providers that involve international transfers, Videosign assesses the applicable transfer mechanisms, security controls and data protection obligations to ensure an appropriate level of protection is maintained.

Videosign regularly reviews international transfer arrangements to ensure ongoing compliance with applicable data protection legislation.

Data Retention

Videosign retains personal data only for as long as necessary to fulfil the purposes for which it was collected, comply with contractual, regulatory and legal obligations, and support agreed customer retention requirements.

Retention periods vary depending on:

- Service type
- Customer configuration
- Regulatory requirements
- Contractual obligations

Where Videosign acts as Data Processor, retention periods are generally determined by the customer acting as Data Controller.

We will only keep your data in line with our agreed retention policies, unless we have an exception to this, in which case we will ensure you understand the reasons why we will hold for longer.



Individual Rights

Subject to applicable law, individuals may have the right to:

- Be informed
- Access their personal data
- Rectify inaccurate information
- Request erasure
- Restrict processing
- Object to processing
- Data portability
- Withdraw consent where applicable
- Request information about automated decision-making and profiling activities where applicable

The right to erasure is not absolute and may be limited where Videosign is required to retain information to comply with legal, regulatory, contractual or security obligations.

Data protection requests, including requests relating to individual rights under applicable data protection legislation, should be submitted to enquiries@videosign.co.uk

Requests are generally free of charge. However, Videosign reserves the right to charge a reasonable fee or refuse a request where permitted by law, including where requests are manifestly unfounded or excessive.

Videosign will respond to valid requests without undue delay and generally within one month of receipt, subject to applicable legal requirements.

Where Videosign acts as a Data Processor on behalf of a customer, requests relating to customer-controlled data may need to be directed to the relevant customer acting as Data Controller. Videosign will assist customers in fulfilling such requests in accordance with applicable contractual and legal obligations.

Complaints Regarding your Personal Data

Videosign aims to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously.

We encourage people to bring it to our attention if they think that our collection or use of information is unfair, misleading, inappropriate or data has been unfairly shared, lost or held inappropriately.

We would also welcome any suggestions for improving our procedures.

If you are dissatisfied with our response, you may lodge a complaint with the Information Commissioner's Office (ICO): <https://www.ico.org.uk>



Changes to this Privacy Notice

We keep our Privacy Notice under regular review.

This privacy notice was last updated May 2026.