videosign
accelerating business

Privacy

Policy

Contents

Company and Background

Videosign Limited, ("The Company", "us" or "we") is a Software as a Service ("SaaS") company that provides advanced functionality in conjunction with a number of technology partners, including Oracle, Amazon, Vonage, Netverify, Zymplifyn and Zoominfo. The "Videosign" platform is a friction-less 'suite' of tools which enables the modern professional advisor to engage with their clients in a dedicated, virtual, secure and private digital meeting room. Providing video meetings, audio and video meeting recording, document collaboration, screen sharing, electronic signing and embedded web forms, Videosign delivers all the core capability to manage a virtual client business relationship.

The data storage and privacy implications vary according to the model that customers can elect, they also vary by legal jurisdiction and geographic location. Such privacy implications are described more fully below with the widest scope for Videosign, although in practice the implications may be significantly less if customers choose to self-store or use their choice of third-party provider for such records (such as for their CRM records).

Overview

Data privacy and protection legislation is continuously changing at different speeds around the globe. It is commonly considered that the 'highest standard' currently in operation is that of the EU General Data Protection Regulation ("GDPR"). For brevity, this document describes Videosign policy viewed through a GDPR lens. You should check with your Data Privacy and Protection compliance team if your jurisdiction or clients warrant any different considerations – and contact us if you are unsure.

The data protection law changed in various European Union ("EU") countries recently (e.g. in 2016 from the Data Protection Act (1998) in the UK (and similar national legislative acts across Europe) to the EU General Data Protection Regulation (GDPR) in the EU (including UK) which became enforceable on the 25th of May 2018.
We want to ensure complete transparency for you to understand how your personal information is held and processed and what your rights as an individual are under the new GDPR. We take your privacy very seriously and will only use your personal information for the purposes laid out below. When you provide us your information, we are holding it only for the legal grounds described and will keep it safe and secure.

Our legal basis for processing for the personal data:

- contractual obligations as stated in the Terms ands Conditions or within your specific Enterprise Software Agreement;
- to maintain an audit trail and, where applicable, regulatory evidence of professional advice being delivered online via Videosign meetings;
- to maintain adequate business records for billing and taxation purposes.

We routinely collect and use personal data about individuals, including permanent staff, freelancers, contracted staff, or business partners ("you"). We are aware of our responsibilities to handle your personal data with care, to keep it secure and comply with applicable privacy and data laws/regulation.
Videosign is designed so that customers can easily elect from three options to store their own customer meeting data (documents, videos):

- Videosign's standard default scenario allows customers to store their video recordings in a Videosign-managed secure archive; or
- Customer owned "integrated cloud where our customer can provide access to their own Cloud storage options; or
- Customer owned on premise "Pluggable Storage" option, where meeting artefacts are stored in a client repository so that Videosign only stores a reference to the document and basic meta-data. This integration is achieved using Videosign's secure APIs (see API's section).

This document assumes the Videosign 'standard default scenario' for the purposes of completeness. Please check with your own Data Privacy compliance team where you choose to store data on your systems or with your partner's Data Privacy compliance team where you choose a third party for processing and/storage.

How we Use your Information

This privacy notice tells you what to expect when we collect personal information. You should be aware that although we will be principally responsible for controlling and looking after your personal data, we may pass your details to other members within the company when required. Your data will comply with the standards set out in this policy and when we pass it on to an external third party for processing, we will not do so without your knowledge and consent. We will also stipulate how they must process your data, ensure it is held securely and they are transparent with any data breaches of your data as well as ensuring that they do not pass your data on to any other third parties without your consent.

Rights of the individual

As the owner of your data, GDPR is the toolset that allows you to ensure your data protection rights as an individual, including:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

This policy shows you how we manage your data to ensure these rights.

What do we Collect and Why?

When we collect your personal information, we ensure it is managed properly and securely. The core information stored is your name, email address and possibly contact phone number. In addition, Videosign or our customers or our customer's partner may store meeting data such as documents, videos and the like.

We typically do not collect information classified as "sensitive"(as name, email address and possibly telephone number are personal but not sensitive information), but if we do work with customers or organisations where this is a requirement then if we collect any additional "sensitive information" as classified by GDPR Article 9 (which relates to physical or mental health, racial or ethnic origin, political opinions, trade union membership, religious beliefs, sexual preferences, commission or alleged commission of an offence and the sentence of any court, and the processing of genetic or biometric data for the purpose of uniquely identifying a natural person), we will ask specifically to collect it and ensure there is extra security around its management and storage.

Below are where and how we collect personal data:

- As standard, your subscription and related personal data, including billing and payment details if a Subscription Client
- Video, Audio, Document and Chat records may be collected but are only stored by us with your consent and as a Subscription customer (Corporate

customers use their own systems or their preferred partner systems to store such)

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.

In terms of a subscription we will collect your data as per your agreement and under the terms stated in your contract or within our standard Terms and Conditions (published on our website), allowing us to administer your subscription holding only the minimal required data to do so.

During registration, we also ask for your consent about a number of matters related to data handling. We ask for these consents to meet the requirements for the protection of privacy set by various countries: consent for the handling of personal information (including e-mail address and mobile phone number), consent for the handling of sensitive personal information, and consent for the transfer of data to a country other than your home country (Videosign uses servers provided by a third party to support its service). These servers may be located either within the EU or outside it. The actual user data and information such as the system's monitoring data is saved on service providers' servers currently located within the EU.

Handling of Personal Information and its Transfer Outside the EU

Videosign's services may be delivered using resources and servers located in various countries (such as the U.S.). Therefore, your information may be processed outside the country that the service you are using is based in, including countries outside the European Economic Area (EEA) where the standard of protection of privacy does not meet the requirements set by the European Commission (such as the U.S.). When you register for Videosign which requires information transfer to another country for processing, we request your permission for the transfer. When transferring information, we comply with all applicable laws to guarantee sufficient protection of your privacy. In general, when transferring your personal data from one country to another we apply the relevant terms, such as the terms of the EU-U.S. Privacy Shield or those of agreements based on European Commission's standard

In line with the principles mentioned above, your information may be transferred or access to it may be permitted to Videosign's subcontractors (such as the supplier of our Customer Care system) that carry out tasks related to Videosign's website, products and services. Our subcontractors are not authorised to use the personal information for any other purpose and Videosign's subcontractors' services are always covered by a confidentiality clause.

Videosign never discloses any of your personal information without a separate permission from you, unless it is necessary for handling your subscription, carrying out your request, or managing our interactive customer programs. Information may, however, be disclosed if necessary because of law, a court order, or a regulation or request issued by authorities.

For statistical purposes, Videosign may deliver collected anonymized statistical data on its customers, sales, traffic types information, and similar web site information to our third-party technology partners. These statistics do not contain identifiable personal information.

Visitors to our website

When someone visits www.videosign.co.uk, Videosign governs the privacy of its users who choose to use it. It explains how we comply with the GDPR (General Data Protection Regulation), the UK's DPA (Data Protection Act -pre-GDPR regulation] and the PECR (Privacy and Electronic Communications Regulations), which will be superseded by the ePrivacy Regulation and which will work alongside the GDPR.

This policy will explain areas of the website that may affect your privacy and personal details, how we process, collect, manage and store those details and how your rights under the GDPR, DPA and PECR are adhered to. Our contact information is provided if you have any questions.

Security and Performance

We use a number of third-party services, Oracle, Amazon, Vonage, Zymplify, Zoominfo and Netverify, to help maintain the security and performance of our website and to provide professional standards of customer service.

There are always risks associated with providing personal data, whether in person, by phone or via the internet or other technologies, and no system or technology is completely safe or "tamper"/"hacker" proof. Videosign takes appropriate precautions to prevent unauthorised access to and improper use of your personal data. For example, Videosign uses encryption and firewall technology when collecting personal data. Videosign sites that support online transactions will use industry standard security measures to protect the confidentiality and security of these transactions. We use industry standard security measures, such as SSL authentication, to ensure that your credit card information, as well as other personal data submitted as part of the subscription process, is appropriately safe from third party interception.

Links to other Websites

This privacy notice does not cover the links within this site linking to other websites. We encourage you to read the privacy statements on the other websites you visit.

Use of Cookies

This website may use cookies to better the users experience while visiting the website. As required by legislation, where applicable this website uses a cookie control system, allowing the user to give explicit permission or to deny the use of /saving of cookies on their computer / device.

What are Cookies?

Cookies are small files saved to the user's computer hard drive that track, save and store information about the user's interactions and usage of the website. This allows the website, through its server to provide the user with a tailored experience within this website.Users are advised that if they wish to deny the use and saving of cookies from this website on to their computers hard drive they should take necessary steps within their web browsers security settings to block all cookies from this website and its external serving vendors or use the cookie control system if available upon their first visit.

Website Visitor Tracking

This website may choose to use tracking software to monitor its visitors to better understand how they use it. The software will save a cookie to your computer's hard drive in order to track and monitor your engagement and usage of the website, but will not store, save or collect personal information.

Downloads & Media Files

Any downloadable documents, files or media made available on this website are provided to users at their own risk. While all precautions have been undertaken to ensure only genuine downloads are available, users are advised to verify their authenticity using third party anti-virus software or similar applications.We accept no responsibility for third party downloads and downloads provided by external third-party websites and advise users to verify their authenticity using third party anti-virus software or similar applications.

People who communicate with us

Users contacting this us through this website or via email, such as job applicants sending a CV/resume, we may keep it for up to 1 year, do so at their own discretion and provide any such personal details requested at their own risk. Your personal information is kept private and stored securely until a time it is no longer required or has no use.

People who Contact us via Social Media

We use social media, such as LinkedIn, Facebook, Twitter and Instagram, to communicate with our industry peers and people in the industry. If you send us a private or direct message via social media, we may keep it for up to 1 year. We do not pass on to external processors without your consent.

People who Email us

Any email sent to us, including any attachments, may be monitored and used by us for reasons of security and for monitoring compliance with office policy. Email monitoring or blocking software may also be used. Please be aware that you have a responsibility to ensure that any email you send to us is within the bounds of the law and virus free.

Support/ Customer Care

Videosign's Customer Care helps you with any problems you may have with our services. Our Customer Care maintains two registers: A "Contact Us" mailbox and Support Requests. Information is saved to both via the www.videosign.co.uk web site. Customers fill the necessary information in the forms themselves, from where it is transferred to Videosign's systems. The data stored in Videosign's systems may be saved on servers located in the USA or on Videosign's service providers' servers either within or outside the EU. Read more about the transfer of data and related protective mechanisms here. Videosign's Customer Care operates globally in various countries to ensure that we can offer support services in several countries and time zones.

The Contact Us mailbox: the information recorded in the e-mail is transferred to a third-party Customer Care system used by Videosign. This system is available to all Videosign's Customer Care personnel. The data recorded in the system is stored on the service provider's servers located in the USA, and the EU. Your contact information (such as an e-mail address and country) is recorded to enable us to respond effectively to your query. Your information is handled confidentially, and the service provider does not have access to the actual data. The information is stored for 6 years unless the local legislation requires longer storage.

Support Request: the information recorded on this form is used to record requests for support, which is recorded in our Global Service System (GSS). The data is used to record details of the request and sending automatic e-mail messages about the progress and completion of request, submitting additional requests related to service. Data from the Request is transferred to Videosign's GSS. The information is stored for 6 years unless the local legislation requires longer storage.

Job Applicants, Current and Former Employees

When individuals apply to work with us, we will only use the information they supply to us within the company and to process their application. Where we want to disclose information to a third party, for example where we want to obtain a ‘disclosure’ from the UK Disclosure and Barring Service, we will not do so without informing them beforehand unless the disclosure is required by law.

Personal information about unsuccessful candidates will be held, with your explicit permission, for up to 1 year (unless agreed otherwise) after the recruitment exercise has been completed, at which time it will then be destroyed or deleted.

Once a person has been hired by us, we will compile a file relating to their service / employment with us. The information contained in this will be kept secure and will only be used for purposes directly relevant to that person’s employment. Once their employment with us has ended, we will retain the file in accordance with the requirements of our retention schedule and then delete it when required to do so.

Complaints Regarding your Personal Data

We try 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.

How to Voice your Concerns to us

This privacy notice was drafted with brevity and clarity in mind. It does not provide exhaustive detail of all aspects of our collection and use of personal information. However, we are happy to provide any additional information or explanation needed. Any requests for this should be addressed for the attention of our Data Protection Officer at the email address: enquiries@videosign.co.uk

If you are unhappy with our response you have the right to escalate this to the Information Commissioner's Office (ICO) @ https://ico.org.uk/concerns/

Access to Personal Information

We try to be as open as we can be in terms of giving people access to their personal information. Individuals can find out if we hold any personal information by making a 'subject access request', where ourselves and/or any related data controller/processors may charge a reasonable fee based on administrative costs to the individual and in a machine-readable format. We will advise you of such fees, if applicable, before continuing further. Once this is confirmed by our receipt of such a written request, if we do hold information about you, we will:

- give you a description of it;
- tell you why we are holding it;
- tell you who it could be disclosed to, and;
- let you have a copy of the information in an intelligible form within one calendar month.

To make a request to Videosign for any personal information we may hold, you need to put the request in writing, addressing it to our Data Protection Officer at enquiries@videosign.co.uk

If we do not hold information about you due to it being erased, possibly due to the retention dates being expired or through a previous request for erasure, we will inform you. Any further question can be submitted to our Data Protection Lead and, should you feel the response not be adequate, you have the opportunity to escalate to the ICO.

Right to be Forgotten

Within GDPR every individual has the right for their data to be forgotten or erased, unless there are legal grounds which do not allow the erasure, such as:

- legal obligations, such as the tax legalisation or legal investigation;
- a contractual obligation that must be fulfilled by the company;
- public task or interest where it is helping with the detection or prevention of a criminal act.

Should you request to be forgotten or make this request through an authorised third-party, such as your solicitor, we will confirm your/their identity and then proceed to remove your personally identifiable data from our records and send you an audit. We will keep the minimum data to identify you as a living person, in case of an audit by the ICO or where a second request should come in, to prove we have acted in accordance with the GDPR.

Again, should you not be happy with the process, you have the right to complain to our Data Protection Lead, and, in turn, if the response is not adequate you retain the right to escalate this to the ICO.

API Integration

Videosign's proprietary Application Programming Interface (API) provides a direct information sharing link between the ecosystem and third-party data systems. With our API's, our customers may transfer data related to their personal information, which includes: name and e-mail address(es) of meeting participant(s).

For third-party developers:
To third party systems, Videosign offers an API interface and instructions that enable the third party to register its own application in the Videosign system and to add users.

The developers use their Videosign developer "token" to log in to the Videosign API services. A new application is registered by providing information on the application and the company. Approval of Terms of Use is required. Personal information collected in connection with registration is collected for billing purposes.
When a customer subscribes to using Videosign, they enter into an agreement with Videosign or its representative. Under this agreement, Videosign acts as the data processor while the customer is the data controller. As the data controller, the customer is responsible for what information is saved in the system and how it is handled. The customer is also responsible for the accuracy of the users' information and data-related requests by individual users and participants (such as requests to delete the information). The customer is also responsible for requesting permission from the user or participant or, in case of a minor, their guardian(s) or carer before adding them to the service.

Customers using the API integration are responsible for linking the third-party services they want to use with their Videosign account. Information is retrieved by the third-party services and sent by Videosign when the user creates a meeting. Videosign is not responsible for data once it is transferred out of Videosign's system and it no longer has any influence on the data. Users are responsible for managing the information they share or transfer out of the system.

People who make a Complaint to us

When we receive a complaint from a person we log the details of the complaint and validate them against our records. This normally contains the identity of the complainant and any other individuals involved in the complaint. We will only use the personal information we collect to process the complaint.
We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

We will keep personal information contained in complaint files in line with our retention policy. This means that information relating to a complaint will be retained for 6 years from closure. It will be retained in a secure environment and access to it will be restricted according to the "need to know" principle.

Similarly, where enquiries are submitted to us we will only use the information supplied to us to deal with the enquiry and any subsequent issues.

Retention and Deletion of Data Records

We will ensure your data is retained for the agreed retention period and is properly deleted at that point. This also includes any data transmissions that hold data temporarily, as we will ensure they are deleted after the event.

Data Breaches

We ensure all your data is held securely and our staff are trained to understand the many different types of breaches, such as:

Hacking by external parties: We ensure we have the correct security in place to secure our premises and the correct access internally should an internal party look to hack into secure areas.

Break-ins to our premises and stealing of data or computer equipment: We abide by a clear desk policy to ensure personal data is secured every evening and security on our premises is checked regularly.

Virus affecting our IT infrastructure: We have state of the art anti-virus software with backups and disaster recovery in place should we have issues
Couriers, cleaners or third parties having access to our premises Our clear desk policy, physical security checks and staff awareness ensure we have a safe and secure environment.

Any data breaches will be detected, reported to the ICO within 72 hours and we will let the individuals know who have been affected while we carry out our investigations.

Changes to this Privacy Notice

We keep our privacy notice under regular review. This privacy notice was last updated on 1st September 2022.

Third Party technology partners and their privacy policies

For the avoidance of doubt, Videosign utilises technology services from Oracle, Amazon, Vonage and Netverify.

The links below provide confirmation of the individual Privacy Policies of each organisation:

- Oracle – https://www.oracle.com/uk/legal/privacy/privacy-policy.html
- Amazon – https://aws.amazon.com/privacy/
- Vonage – https://www.vonage.com/legal/privacy-policy/
- Netverify – https://www.jumio.com/legal-information/privacy-notices/jumio-corp-privacy-policy-for-online-services/
- Zymplify – https://zymplify.com/privacy-policy-2/
- Zoominfo – https://www.zoominfo.com/about-zoominfo/privacy-policy

How to contact Videosign

If you want to request information about our privacy policy, you can email our Data Protection Administrator at enquiries@videosign.co.uk