

The SignOnDoc Data Privacy Promise

Our commitment to you is top-notch security. Any and all customer data in our possession will always be stored safely and securely. If ever you need to know more about the data we hold, please send an email to vijay@signondoc.com.

We know that we are being trusted to handle your most important business documents, so we want to ensure that you have all the information you need regarding the safety and security of your business and customer data.

SignOnDoc & Your Data: FAQ

Here are some answers to frequently asked client questions:

Data Compliance

Is SignOnDoc compliant with GDPR?

Absolutely! We have taken all the necessary measures to ensure that we are compliant by updating our customer contracts, Terms of Service, Privacy Policy, and internal Data Protection.

In order to reach this point, we completed a company-wide data audit as of early May 2018. This process allowed us to ascertain that the majority of our existing data protection policies and processes were indeed GDPR compliant. We also consulted our legal team for input. We then made some simple adjustments to our product and data processes to ensure we are now officially 100% compliant.

Is SignOnDoc compliant with other industry data protection laws/requirements?

SignOnDoc always complies with all necessary legal requirements in the United States, United Kingdom, and the rest of the European Union. We work hard to keep up-to-date with each country's specific legislation and we do our best to remain compliant with industry-specific legal requirements. If you want to know more about the ways in which we ensure our support vijay@signondoc.com.

How does SignOnDoc (as well as its sub-processors and subcontractors) comply with GDPR?

Every single SignOnDoc team has been involved in ensuring GDPR compliance, from our IT and finance teams to our legal and product teams.

We have reviewed our CRM, our finance software, and our current data processes and policies. We have also vetted all of our suppliers to ensure they are compliant as well.

We provide mandatory data security and protection training for all team members who have access to customer data. We also share all relevant information about data protection with the rest of our team via video training.

Who is responsible for SignOnDoc's compliance?

Alongside our legal team – which advises us on remaining up-to-date and compliant with global regulations – we have also nominated a Data Privacy Manager to govern our data processes, including storage, access, retention, and deletion.

Our customers are data controllers who are free to determine which personal data is processed and stored on the SignOnDoc cloud software on your

Where can I read your full Terms of Service and Privacy Policy?

You can read the full Terms of Service [here](#), which was last updated on May 2018.

You can read the full Privacy Policy [here](#), which was last updated on May 2018.

What privacy certifications does SignOnDoc have?

There are several country-specific legislatures that specify the necessary requirements to ensure that an electronically signed document is legally binding.

We are compliant with the EU eIDAS Regulation, which sets out rules for electronic identification and trust services, and ensures the identity of individuals and businesses online or the authenticity of electronic documents.

We are also compliant with the United States E-SIGN Act of 2000, which is equivalent to eIDAS in the EU.

As requested by customers who are handling highly confidential data, we are also happy to sign Data Protection Agreements (DPAs).

What Electronic Trust Services does SignOnDoc offer customers?

SignOnDoc's secure audit trail contains IP addresses, timestamps, and validated email addresses for all the signers on each document.

Data Storage

Where is SignOnDoc data located?

All customer data is located in the United States.

Can I choose which country you store my personal / business data from SignOnDoc?

As of now, we do not offer data localisation, as our data centers in the United States meet all of the legal data protection requirements.

Data Encryption

Can the SignOnDoc team or management see the contents of any uploaded documents?

No. We ensure that all the documents that are uploaded, sent, and stored on our cloud use encryption, so we cannot see the original documentation.

How does your encryption work?

All of the data and content you upload – whether it is at rest or in motion – is encrypted so that it cannot be read. For data in motion, we use standard SSL encryption, and our traffic is served on the HTTPS channel.

Can new products, updates and new feature rollouts affect data security?

We take your data privacy very seriously, and are adhering to the new Privacy by Design concept as outlined in the GDPR. Our product team works closely with our IT and legal teams to ensure that any new products, product updates, and features are rolled out with no risk to data security.

Data Retention & Deletion

Does SignonDoc retain my personal data?

Yes, we retain all personal data, however it can be deleted upon request.

What is SignOnDoc's Right to be Forgotten process?

If you wish to have your data deleted, please email us with your deletion request at vijay@signondoc.com. As soon as we receive your email, your data will immediately be deleted from all of our SignOnDoc systems. We will also ensure that data stored within our third party systems is deleted within 30 days. We will send you a confirmation email when your data has been

How can I as a SignOnDoc customer limit access to accounts when an employee leaves?

If you wish to limit or amend any access to your SignOnDoc account when one of your employees leaves the company, you can easily re-assign that license to another employee by logging into SignOnDoc's user-friendly dashboard and making the change yourself. Alternatively, you can submit a support ticket or email us at vijay@signondoc.com. we will be happy to

How does SignOnDoc ensure that data access is prohibited if a members of its staff leaves?

As soon as a member of our team leaves the company, we ensure that their access to SignOnDoc internal tools, data, and our email system is terminated during our employee exit process. We also have trails of who is accessing customer data that are intended to inform us of any

Data Access

How does GDPR apply to SignOnDoc's employees?

All data protection responsibilities apply to every team member that handles data.

What personal data does SignOnDoc management hold about its customers?

We retain the following customer information: email, name, personal details, IP address, documents and document names, device ID, enriched data. We use this data for personalization, product use, security, and sales analysis purposes.

If I ask Signondoc to close my account or to remove my data, is the Audit Trail still valid? How can I access it?

The audit trail on all of your electronically signed documents is always valid, even if you leave SignOnDoc or if you do not have a paid account with us. The audit trail certificate is emailed to you as soon as you sign a document, so there is no need to request it from us. In case you lose a specific certificate and need a duplicate, contact vijay@signondoc.com. and we will generate one for you, as we do keep a copy of the certificates on our servers.

How does SignOnDoc transfer data from one individual to another?

SignOnDoc never transfers data from one individual to another. We use our own servers to transfer data via encryption to our users.

Data Breaches

What is the process if SignOnDoc notices that there has been a breach in data privacy and protection?

While not impossible, we believe it would be highly unlikely for a data breach to occur. However, if ever there was a data breach, our process is as follows: we adhere to all applicable GDPR rules and ensure that our customers and supervisory authorities are notified about any unlawful or unauthorized access or acquisition of your data within 72 hours. The mode of communication is dependent on the individual circumstance.