

ReadySign electronic signature software is built with the security of your documents in mind. We've taken every measure possible to ensure your data remains both accessible and secure.

Data Protection

We take extra steps to protect the confidential data in your agreements and to ensure only authorized users have access to the information they need.

Data Protection	
Third-Party Examination Report	SOC 2®, Type 2 Report
Encryption of Data	256-bit encryption of all data, both in transit and at rest.
Secure Connections	All connections are protected using TLS with a 256-bit symmetric encryption and 2048-bit authenticated key agreement.
Password Protection	Passwords are masked with a separate salt and encrypted with Bcrypt.
Data Center Protection	While at the data centers, all data remains encrypted using 256-bit AES, which is certified for use by the U.S. Government for top-secret documents.
Offsite Backup for Disaster Recovery	We store all information in multiple data centers, which are located in geographically separate locations for both our United States and European Union-based data centers. This acts as a protection against hardware failure, theft, virus attack, deletion, and natural disaster.
Encrypted Online Backup	Automatic encrypted online hourly backup is a critical component in any disaster recovery plan and comes standard with every account.
Privacy	ReadySign never has back-end access to your data.

Amazon Web Services

ReadySign utilizes Amazon Web Services (AWS), the leader in public cloud security, which has extensive security measures that ReadySign leverages to protect data, including security verification from independent third-party examination reports.

Amazon Web Services (AWS)	
Secure Data Center Location	Locations in both the United States and European Union.
Network Security	AWS takes a diversified approach to ensuring network security, such as segmentation, firewalls, and intrusion detection, among others.
Third-Party Examination Reports	Service Organization Control (SOC) Reports 1, 2, & 3
ISO 27001 Certified Data Centers	Security measures include; electronic key-cards, pin codes, biometric hand scans, and onsite security officers 24 hours a day, 365 days a year.

For more information on AWS visit: <https://aws.amazon.com/>

Additional Security Measures

We've added additional security features to every account to give you the option of increasing the security of your confidential information.

Additional Security Measures	
Multi-Factor Authentication (MFA)	ReadySign offers both SMS authentication and authentication app options.
SAML 2.0/Single-Sign-On (SSO)	Securely access ReadySign by signing into one central program such as Microsoft Active Directory, OneLogin, or Okta. Easily add and remove users from the system while enforcing company-wide password policies.
Access Control	Restrict system access to ensure only certain users have access to specific information.
Audit Logs	Track system activity by user, date, time, and action taken.

Dedicated Security Features

Every account comes standard with these dedicated security features:

- **One-Click privacy blind**
- **Auto time-out**
- **Watermarks with personally-identifiable information**
- **Customizable NDA**
- **Expiring invitations**

Additional Questions?

If you have additional questions about ReadySign, please contact your account manager directly, or email sales@readysign.com at any time.



Electronic Signature Specifications

ReadySign electronic signature software is built with the security and enforceability of your documents and signatures in mind. We've taken every measure to ensure your data is protected, and your electronic signatures are recognized as valid under the United States Electronic Signatures in Global and National Commerce Act and the Uniform Electronic Transactions Act.

ESIGN & UETA Compliant

ReadySign is built in accordance with both the United States Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA), and covers the following requirements to ensure your electronic signatures are valid and enforceable:

Consent to do business electronically	Whenever a document is sent for signature with ReadySign, parties are prompted to confirm their consent to sign documents electronically.
Intent to sign	ReadySign allows parties to decline or transfer signature requests.
Association of signature with record	Similar to a human fingerprint, each signer is assigned a unique identifier and customizable signature that is recorded and retained.
Signed copies	All signers receive a fully executed copy of the agreement, which can be downloaded and retained for record.
Record retention	ReadySign securely stores data using certified AWS data centers and 256-bit data encryption, both in transit and at rest. Documents can also be downloaded and retained outside of the system.

Additional Measures to Secure your Electronic Signature:

- **LTV (Long Term Validation) enabled**
- **Member of the Adobe Approved Trust List (AATL)**
- **Audit trail reporting**
- **Multi-factor authentication**
- **Tamper evident seal**

Additional Questions?

If you have additional questions about ReadySign, please contact your account manager directly, or email sales@readysign.com at any time.