DocuSign®

Whitepaper

How Data Governance Regulations and Standards Shape DocuSign's Rigorous Security and Privacy Practices

Introduction

Every e-signature provider seeks to keep confidential customer data secure throughout the e-signing process and ensure that the data remains accurate, complete, and consistently available to those authorized to access it. But what sets them all apart is their approach to data governance.

DocuSign's commitment to and significant ongoing investment toward protecting customer data extends to every operating environment across the DocuSign Agreement Cloud. In fact, information security and privacy are in our DNA and engrained in our people, processes, and technologies—globally.

Our approach is simple: every employee is responsible for information security, including protecting:

– DocuSign-owned information assets
– Customer and partner information assets
– The underlying technology infrastructure and the data generated, processed, and stored in DocuSign environments

This document details DocuSign's commitment to delivering robust data governance through specific policies and capabilities, rooted in an understanding of laws, regulations, standards, and best practices.

From global regulations to contractual commitments

Effective security capabilities stem from a full range of factors that inform the security approach, from the broadest government laws and regulations to specific contractual agreements.

DocuSign data governance standards, policies, and procedures are informed by a firm grasp of these factors, resulting in security and privacy capabilities and an overall security mindset that are integrated into everything that the company does to cultivate ongoing customer trust (see diagram).

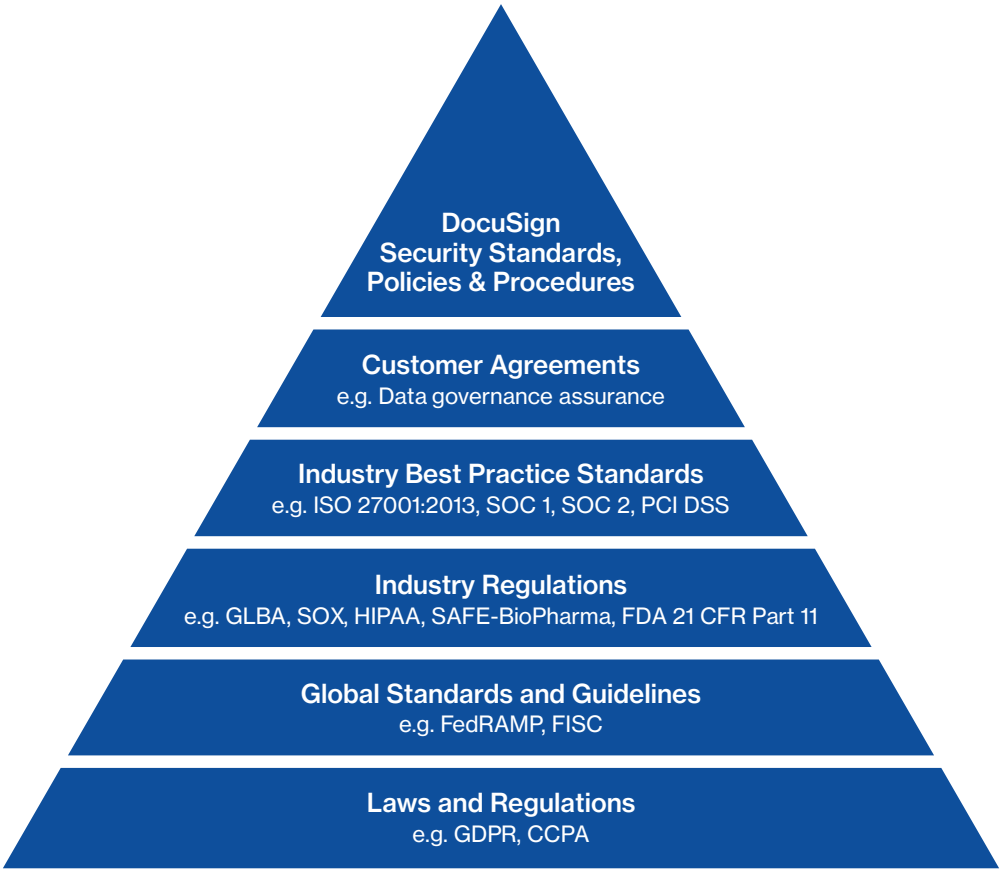

Figure 1:
DocuSign data governance standards, policies, and procedures are informed by an understanding of laws, regulations, and best practices for securing customer data.

Global standards and guidelines

DocuSign works diligently to stay abreast of security and privacy regulations and frameworks around the world. By continually monitoring the security and privacy landscape, we can modify our data governance approach to remain in step and comply with the latest standards and guidelines, including:

United States (U.S.) Federal Risk and Authorization Management Program (FedRAMP)
FedRAMP is a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. DocuSign was awarded the FedRAMP Agency authorization and is listed on the U.S. Federal Government's FedRAMP marketplace with a **Government Community Cloud deployment model for DocuSign eSignature** and a **Public Cloud deployment model for DocuSign Contract Lifecyle Management (FKA SpringCM)**.

Japanese Center for Finance Industry Information Systems (FISC)
FISC develops security guidelines for information systems, which are followed by most financial institutions in Japan. These include guidelines for security measures to be put in place while creating system architectures, auditing of computer system controls, contingency planning, and developing security policies and procedures. DocuSign is a member of FISC and is compliant with FISC Security Guidelines.

General Data Protection Regulation (GDPR)
The GDPR represents the most important data protection regulation change in over 20 years. It aims to strengthen data protection for individuals within the European Union (EU), giving them greater say over what companies can do with the personal data that has been collected on them and making data privacy rules uniform for businesses handling EU personal data.

As an organization focused on trust and careful handling of customer data, DocuSign has been committed to privacy since inception. Our strong compliance culture and robust security safeguards, which are reflected in our ISO 27001 certification, provide a solid foundation for ongoing **GDPR compliance efforts**. In addition, DocuSign has received EU commission approval for our **Binding Corporate Rules (BCR)**, widely considered the gold standard for data protection.

California Consumer Privacy Act (CCPA)
The CCPA is a California-specific privacy law that requires organizations to protect the personal information of California residents and establishes similar individual rights and associated obligations as the GDPR. This is the first state-specific privacy legislation in the United States, signaling an increasing level of regulatory attention on data governance practices. DocuSign's commitment to privacy as a critical capability allows us to navigate the rapidly shifting privacy landscape.

Industry regulations

The operating models in DocuSign's security and privacy programs are further informed by regulations in specific industries. We continually review our security capabilities in light of new regulations as they're released. Moreover, the DocuSign eSignature service enables organizations to demonstrate compliance with industry regulations and includes options for where to store documents, as well as audit trails providing detailed information on who e-signed a document, when and how. Below are representative examples of such regulations:

Health and Life Science

The U.S. Title 21 Code of Federal Regulations Part 11 (21 CFR Part 11) defines the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records by the Food and Drug Administration (FDA). It establishes requirements for how all FDA-regulated industries (e.g. drug makers, medical device companies, and biotech companies) may process and submit information electronically to the FDA.

Healthcare

Title II of the U.S. Health Insurance Portability and Accountability Act (HIPAA) includes a privacy rule that regulates the use and disclosure of protected health information. It protects personal information from being shared without explicit authorization of the patient except to facilitate treatment or payment.

Banking

The U.S. Gramm-Leach-Bliley Act includes a safeguards rule that requires financial institutions to develop and maintain procedures to secure and keep customer data confidential.

Public Companies

Sarbanes-Oxley (SOX) establishes requirements for financial reporting for all public companies in the United States.

Industry best-practice standards

Regardless of industry, the need for data governance has driven the creation of best practices and standards to guide companies in their security and privacy strategy and capabilities. Evidence of DocuSign's commitment to data governance at all levels is provided by the certifications and attestations of compliance we've earned, including:

ISO 27001:2013

The highest level of certification available today for assuring global information security. DocuSign maintains this certification for the eSignature platform, including the supporting data centers and company operations. ISO 27001 is core to DocuSign's security standard model, and DocuSign's ISO 27001 results can be made available to customers so that they can map them into their own vendor management programs.

SOC 1 Type 2, SOC 2 Type 2

As a SOC 1 and SOC 2-certified organization, DocuSign complies with the reporting requirements stipulated by the American Institute of Certified Public Accountants (AICPA). We undergo yearly audits across our production operations, including our datacenters, and have sustained and surpassed requirements.

PCI DSS

DocuSign maintains compliance with the current version of the PCI Data Security Standard (DSS) to ensure safe and secure handling of credit card holder information. As overseen by the Payment Card Industry Security Standards Council (PCI SSC), DocuSign places stringent controls around cardholder data as both a service provider and merchant. DocuSign is listed as a PCI Service Provider on the **Visa Global Registry of Service Providers**.

CSA STAR Program

DocuSign adheres to the requirements of the Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) program. The CSA STAR comprises key principles of transparency, rigorous auditing, and harmonization of standards. Our Consensus Assessments Initiative Questionnaire (CAIQ) documents the rigor and strength of DocuSign's security posture and best practices and is publicly accessible for viewing and download from the CSA STAR registry for both **DocuSign eSignature** and **DocuSign Contract Lifecycle Management (FKA SpringCM)**.

Customer contractual agreements

DocuSign provides assurance to customers about data governance for privacy and security for all of our products and services, which are outlined in DocuSign's contractual agreements.

Layered, defense-in-depth approach to protecting customer data

To implement an effective, multi-layered approach to data governance, DocuSign evaluates the collective industry requirements from multiple perspectives. We also have dedicated teams that continually review and assess our data governance posture to ensure customer needs are met and new risks adequately mitigated. All teams collaborate to ensure alignment of security and privacy practices, providing regular updates to DocuSign's executive staff. These teams are comprised of subject matter experts from some of the most security-conscious organizations in the world, including multinational financial institutions and law enforcement agencies in the United States and United Kingdom:

- **The information security team** protects the confidentiality, integrity, and availability of electronic data and has a global presence across all DocuSign locations.
- **The physical security and global safety team** protects company personnel, physical assets, and facilities against unauthorized physical access, damage, and harm, including company-managed datacenters housing customer data and documents.
- **The privacy team** develops and implements policies and procedures that are designed to ensure that DocuSign and our suppliers process personal data in compliance with law and as required by DocuSign's own policies and contractual commitments to customers.
- **The internal audit team** analyzes DocuSign operations to determine if DocuSign policies and procedures are being followed adequately and provides guidance on remediation if required.
- **The compliance team** oversees the compliance and industry best practices program, engaging with external third-party auditors to validate that DocuSign security policies, procedures, and operations comply with industry and governmental regulations and standards.
- **The supplier risk team** screens third-party vendors in order to provide a more thorough view of the suppliers that engage with DocuSign.

Conclusion

Reviewing and analyzing a broad range of considerations from global regulations to contractual commitments significantly contributes to DocuSign's approach to security and privacy. Dedicated teams focus on delivering the confidentiality, integrity, availability, and privacy that regulations dictate and that customers expect, so that companies can embark upon digital transformation with confidence.

DocuSign, Inc.
221 Main Street, Suite 1550
San Francisco, CA 94105

docusign.com

For more information
sales@docusign.com
+1-877-720-2040

2020.01.30