How Data Governance Regulations and Standards Shape Leading-edge Practices for Security and Privacy at DocuSign

Introduction

All eSignature solutions tout a high level of security and privacy. Every eSignature provider aspires to keep customer confidential 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 providers apart is how they approach data governance.

DocuSign's commitment to and significant ongoing investment toward protecting customer data extends to all of DocuSign's operating environments across the DocuSign System of Agreement platform. It takes a comprehensive approach that spans the entire organization and extends to the people and processes. Applying the same stringent controls globally helps DocuSign maintain confidentiality, integrity, privacy, and availability of customer data.

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. It outlines how DocuSign approaches to data governance with ongoing, multi-faceted analysis of security requirements.

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 the details of 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).

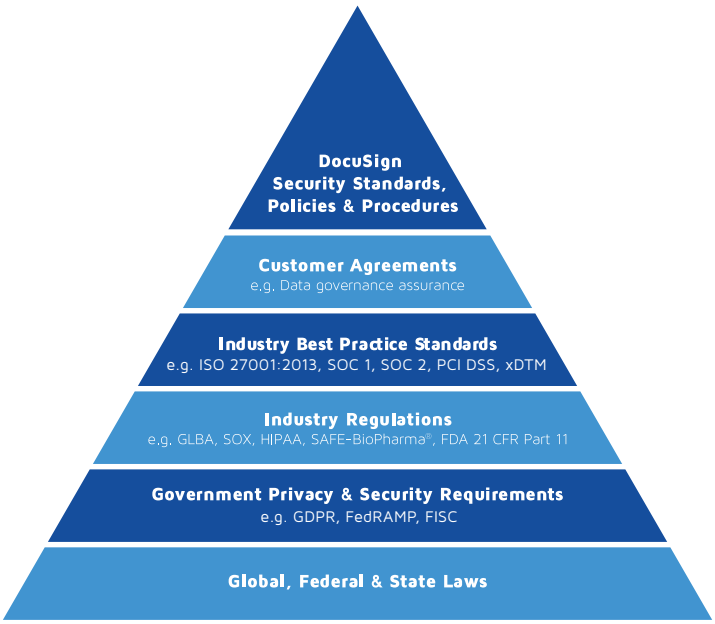

Figure 1:
DocuSign data governance standards, policies and procedures are informed by an understanding of laws, regulations, and best practices for securing customer data.

Global, Federal and State Laws

DocuSign works diligently to stay abreast of security and privacy requirements as set forth under international, federal and state laws. By continually monitoring the security and privacy landscape, DocuSign can modify its data governance approach to remain in step and comply with the latest requirements.

Government Privacy and Security Requirements

DocuSign has demonstrated compliance with government regulations and frameworks around the world that were developed to ensure the privacy and security of personal and sensitive confidential information, including:

- **FedRAMP** – The Federal Risk and Authorization Management Program, or FedRAMP, is a U.S. government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by Government agencies. DocuSign has agency sponsorship by the Federal Communications Commission (FCC) and is listed on the FedRAMP marketplace.
- **FISC –** The Center for Finance Industry Information Systems (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 is a European Union (EU) data protection law that requires organizations that process personal data to be responsible for that data and stipulates requirements for handling personal data and documenting those practices. DocuSign is committed to data privacy. Its strong compliance culture, policies, and robust security safeguards reflected in its ISO 27001 certification provide a solid foundation for the company's continued GDPR efforts. In addition, DocuSign has received EU commission approval for its Binding Corporate Rules (BCR), widely considered the gold standard for data protection.

Industry Regulations

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

- **Food & Drug –** The Code of Federal Regulations Title 21 Part 11 (21 CFR Part 11 and Annex 11 in EU) 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 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 Gramm-Leach-Bliley Act includes a Safeguards Rule that requires financial institutions to develop and maintain procedures to secure and keep customer data confidential.

- **Pharmaceuticals** – The SAFE-BioPharma® digital identity and digital signature standard blends technology, rules and legal agreements to establish common ways of managing digital identity credentials and applying unique digital signatures to documents for pharmaceutical, biotech, and healthcare industries worldwide.
- **Public Companies** – Sarbanes-Oxley 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 the company has earned, including:

- **ISO 27001:2013** – The highest level of certification available today for assuring global information security. DocuSign has earned this certification for all aspects of the enterprise, including data centers, the eSignature platform, 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** – Provides confirmation of DocuSign's financial and information security controls. A SOC 1 Type 2 report describes the internal controls in place over financial reporting at an organization and requires a third-party service auditor to review and examine the organization's operations over a set period of time.

  The SOC 2 Type 2 report specifically indicates that DocuSign's technology meets the criteria for security, availability, confidentiality, and processing integrity and is protected against unauthorized physical and logical access. The report also confirms the platform is available for operation and use as an information system designated as confidential and protected, and is complete, accurate, timely, and authorized..
- **PCI DSS** – The Payment Card Industry Data Security Standard outlines the security requirements for organizations that process, manage and store cardholder data.
- **Skyhigh CloudTrust** – Mandates stringent requirements for the protection, identity verification, and security controls of cloud-based data, based on detailed criteria developed in conjunction with the Cloud Security Alliance.

Customer Contractual Agreements

DocuSign provides assurance to customers about data governance for privacy and security with the DocuSign signature platform, 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 outlined earlier from multiple perspectives. DocuSign has dedicated teams that continually review and assess the company's data governance posture to ensure customer needs are met and new risks adequately mitigated. All teams collaborate together to ensure alignment of security and privacy practices, providing regular updates to the Executive Staff at DocuSign. The 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 data centers housing customer data and documents.

The Privacy Team develops and implements policies and procedures that are designed to ensure that DocuSign and its suppliers process personal data in compliance with law and as required by DocuSign's own policies and contractual commitments to customers. The privacy team includes attorneys in Seattle, San Francisco, Dublin and London.

The Internal Audit Team analyzes DocuSign operations to determine if DocuSign policies and procedures are adequately being followed and provides guidance on remediation if required.

The Compliance Team oversees the Compliance and Industry Best Practices program, engaging with external thirdparty 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.

Follow Us

About DocuSign

DocuSign® helps organizations connect and automate how they prepare, sign, act-on, and manage agreements. As part of its cloud-based System of Agreement Platform, DocuSign offers eSignature—the world's #1 way to sign electronically on practically any device, from almost anywhere, at any time.

For U.S. inquiries: toll free **866.219.4318** | docusign.com

For EMEA inquiries: phone **+44 203 714 4800** | email: emea@docusign.com | docusign.co.uk

Data Governance_WP_TW_052819_COMPL_PUB_GL