SECURITY AND DATA PROTECTION

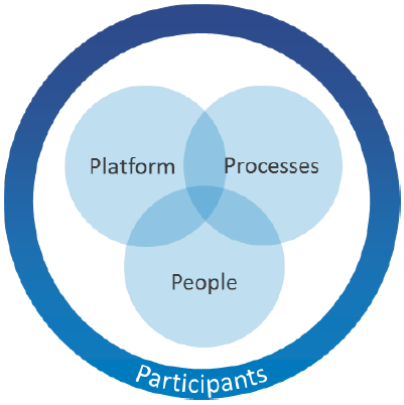
Security is a fundamental requirement for any software-based solution. Processes involving electronic signatures are particularly security-sensitive.

When business transactions contain sensitive information, such as personal data, pricing, or any other business-related information, no risks can afford to be taken on the process side. Thanks to its rigorous security standards, DocuSign has established itself as a market leader in the field of security and data protection. Protecting customers and their data is the company's top priority, and that's why DocuSign is the most widely used solution for electronic signatures in the world, with more than 85 million customers in 188 countries.

DocuSign meets or exceeds the requirements of even the most security-conscious and security-sensitive customers. These include Fortune 500 companies, banks and financial institutions, and other globally operating businesses.

This document provides an overview of the topic of security with reference to DocuSign and the electronic signing process at CHG-MERIDIAN, and looks in more detail at DocuSign's security strategy and associated key areas.

DOCUSIGN SECURITY ASSURANCE PROGRAM



The Security Assurance Program is the linchpin of the security strategy. It is a three-pronged approach combining people, processes and platform. This comprehensive approach allows the company to meet all its ambitious objectives in terms of security, data protection, and the validity of signatures.

People: Security is the responsibility of every individual at DocuSign. We invest in training and in raising people's awareness, to ensure that security remains a top priority for all our employees.

Processes: The security of customer data is a key consideration in every business process. This include internal guidelines, software development, and platform monitoring.

Platform: Every component of the platform – hardware and infrastructure, systems and operations, applications and access, and the transmission and storage of data – undergoes security scrutiny.

DocuSign takes into consideration all aspects and areas to ensure that sensitive data and transactions are safeguarded. This ensures that requirements for security, data protection, and legal validity are met around the world. Not even DocuSign employees have access to sensitive customer data.

CERTIFICATIONS AND AUDITS

ISO 27001:2013
ISO 27001:2013 is a standard for information security management systems published by the International Organization for Standardization (ISO).

SSAE 16, SOC 1 Type 2, SOC 2 Type 2
Published by the American Institute of Certified Public Accountants (AICPA), SSAE 16 reports focus on the design and operational effectiveness of internal controls.

xDTM Standard, Version 1.0
The first standard dedicated to digital transaction management.

PCI DSS 3.1
PCI DSS 3.1 is a data protection standard for organizations that process payment card holder data.

CloudTrust
The criteria for meeting this standard were developed in collaboration with the Cloud Security Alliance.

LOCATIONS OF DATA CENTERS

DocuSign has a total of three European data centers in Germany, France, and the Netherlands. CHG-MERIDIAN is using only the European data centers for its European customers. When providing an e-signature account, DocuSign specifies the data center ring (EU or USA) on which the account is located. All electronic documents that are uploaded for review or signature using an account will be stored on only one of the two rings.

ADDITIONAL SECURITY FEATURES

The following security features ensure the confidentiality, authentication, and binding nature of the signed documents, and prevent them from being tampered with or revoked:

AES 256-bit encryption for documents at application level. This ensures that confidentiality is guaranteed.

Access and transfer of data by and to DocuSign via HTTPS.

The use of Security Assertion Markup Language (SAML) provides users with the latest options for web-based authentication and authorization as well as a single sign-on option.

A digital checksum (mathematical hash value) verifies that documents have not been altered outside the signing process.

Once all participants have completed the signing process, a certificate of completion is automatically generated.

Signatures are verified, and data relating to the process participants is stored and cannot be altered: name, email address, IP address, signature events, time stamp, signing location (if available), and completion status.

A digital audit trail ensures that there are names, email addresses, authentication methods, IP addresses, envelope actions, and time stamps for every envelope.

IN CONCLUSION

DocuSign is committed to ensuring the strictest standards of protection for the data that is entrusted to it by its customers. The notion of security is firmly embedded in every part of the organization. This is demonstrated not least by the company's commitment to meet and exceed national and international security standards, including the ISO 27001: 2013 certification. At DocuSign, security comes first.