SICHERHEIT & DATENSCHUTZ

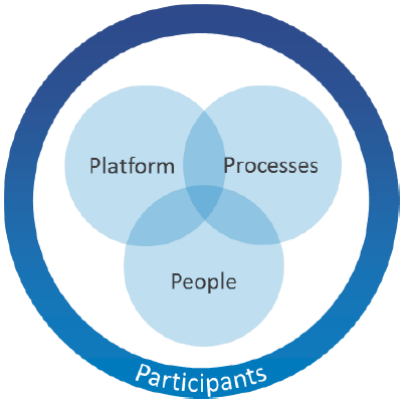
Sicherheit ist essenzielle Grundvoraussetzung einer jeden software-basierten Lösung. Dennoch zählen Prozesse in Verbindung mit elektronischen Signaturen zu besonders sicherheitssensiblen Geschäftsprozessen.

Sobald Geschäftstransaktionen sensible Informationen wie bspw. personenbezogene Daten, Preisinformationen oder sonstige geschäftsrelevante Informationen erhalten, darf prozessseitig kein Risiko eingegangen werden. Aus diesen Gründen nimmt DocuSign eine Vorreiterrolle im Bereich Sicherheit und Datenschutz ein. Der Schutz der Kunden und deren Informationen hat für DocuSign höchste Priorität. Daher ist DocuSign die weltweit meist genutzte Lösung für elektronische Signaturen. Über 85 Millionen Kunden in 188 Ländern.

DocuSign erfüllt oder übertrifft selbst die Anforderungen der sicherheitsbewusstesten und -sensibelsten Kunden. Dazu zählen Fortune 500 Unternehmen genauso wie Finanz- und Kreditinstitute und andere global agierende Unternehmen.

Auf den folgenden Seiten erhalten Sie einen Überblick zum Thema Sicherheit im Rahmen des elektronischen Signaturprozesses der CHG-MERIDIAN mit DocuSign. Dabei lernen Sie den Sicherheitsansatz sowie die zugehörigen Schlüsselgebiete von DocuSign näher kennen.

DOCUSIGN SECURITY ASSURANCE PROGRAM



Kern des Sicherheitsansatzes bildet das „Security Assurance Programm“. Es vereint die dabei die Bereiche „People“, „Processes“ sowie „Plattform“. Mit diesem umfassenden Ansatz gelingt die Realisierung sämtlicher Ansprüche hinsichtlich Sicherheit, Datenschutz und Gültigkeit der Signaturen.

People (Mitarbeiter): Sicherheit ist die Aufgabe eines Jeden bei DocuSign. Wir investieren in Ausbildung und Sensibilisierung, um sicherzustellen, dass Sicherheit höchste Priorität bei allen unseren Mitarbeitern bleibt.

Processes (Prozesse): Die Sicherheit der Kundendaten spielt in allen DocuSign Geschäftsabläufen eine zentrale Rolle. Dies beinhaltet interne Richtlinien, Software-Entwicklung und Plattform-Monitoring.

Platform (Plattform): Zur sicheren Plattform von DocuSign zählen Hardware und Infrastruktur, Systeme und Betrieb, Applikationen und Zugang sowie die Übertragung und Speicherung von Daten.

DocuSign berücksichtigt sämtliche Bereiche und Aspekte um sensible Daten und Transaktionen zu schützen. Auf diese Weise können Anforderungen an Sicherheit, Datenschutz und Rechtsgültigkeit rund um den Globus erfüllt werden. Noch nicht einmal DocuSign-Mitarbeiter haben Zugriff auf die sensiblen Daten der Kunden.

ZERTIFIKATE UND TESTS

ISO 27001:2013
ISO 27001:2013 ist an Standard für Informationssicherheits-Managementsysteme welcher von der International Organization for Standardization (ISO) herausgegeben wurde.

SSAE 16, SOC 1 Type 2, SOC 2 Type 2
Herausgegeben vom American Institute of Certified Public Accountants (AICPA), zielen SSAE 16 Reports auf die Gestaltung und die operative Effektivität von internen Kontrollen ab.

xDTM Standard, Version 1.0
Der erste Standard der den Fokus auf das digitale Transaktionsmanagement setzt.

PCI DSS 3.1
PCI DSS 3.1 ist ein Datenschutz-Standard für Organisationen die Kreditkartenhalter-Informationen verarbeiten.

CloudTrust
Die Kriterien zur Erfüllung dieses Zertifikats wurden gemeinsam mit der Cloud Security Alliance entwickelt.

STANDORTE DER RECHENZENTREN

DocuSign verfügt über insgesamt drei europäische Rechenzentren in Deutschland, Niederlande und Frankreich. CHG-MERIDIAN nutzt für seine europäischen Kunden ausschließlich die europäischen Rechenzentren. Bei der Bereitstellung des e-Signatur-Accounts wird durch DocuSign festgelegt, auf welchem Ring von Rechenzentren (EU oder USA) der Account liegt. Alle elektronischen Dokumente, die über einen Account zum Einsehen oder Signieren hochgeladen werden, werden damit nur auf einem der beiden Ringe gespeichert.

WEITERE SICHERHEITSFUNKTIONEN

Folgende Sicherheitsfunktionen von DocuSign stellen sowohl Vertraulichkeit, Fälschungssicherheit, Authentifizierung als auch Verbindlichkeit und Unwiderlegbarkeit der unterzeichneten Dokumente sicher:

AES 256-bit Verschlüsselung auf Applikationsebene für Dokumente. Auf diese Weise wird die Vertraulichkeit gewährleistet.

Zugang und Übertragung von Daten von und zu DocuSign via HTTPS.

Die Nutzung der Security Assertion Markup Language (SAML) gibt den Nutzern die neuesten Möglichkeiten für webbasierte Authentifizierung und Autorisierung wie auch eine Single-Sign-On Option.

Eine digitale Checksumme (mathematisch Hash Value) validiert, dass Dokumente nicht außerhalb des Signaturprozesses verändert wurden.

Nachdem alle Teilnehmer den Zeichnungsprozess abgeschlossen haben, wird automatisch ein Abschlusszertifikat erstellt.

Signatur Verifikation und unveränderbare Speicherung der Daten der Prozessteilnehmer:
Name, E-Mail- und IP-Adresse, Signaturereignisse, Zeitstempel, Zeichnungsort (wenn zur Verfügung gestellt) und Komplettierungsstatus.

Ein digitaler Prüf-Pfad sichert für jeden Umschlag Namen, E-Mail-Adressen, Authentifizierungsmethoden, IP-Adressen, Umschlagsaktionen und Zeitstempel.

ABSCHLUSSBETRACHTUNG

DocuSign verpflichtet sich, die Daten, die ihnen durch Kunden anvertraut werden, strengstens zu schützen. Der Sicherheitsgedanke ist daher fest in jeden Teil der Organisation eingewoben. Belegt wird dies unter anderem durch die Investitionstätigkeit in der Erfüllung und Übererfüllung nationaler und internationaler Sicherheitsstandards, einschließlich der Zertifizierung für ISO 27001: 2013. Sicherheit hat für DocuSign oberste Priorität.