FOXIT ESIGN – COMPLIANCE ÜBERSICHT

Einige Unternehmen unterliegen einer Reihe von spezifischen gesetzlichen Anforderungen. Foxit eSign kann als Schlüsselkomponente für die Einhaltung Ihrer Verpflichtungen dienen. Im vorliegenden Dokument werden verschiedene Vorschriften nach Region und Branche beschrieben, deren Einhaltung Foxit eSign unterstützt.

WHITEPAPER

INHALTSVERZEICHNIS

NACH REGION

USA

Foxit eSign ist zu 100 % konform mit allen US-amerikanischen ESIGN Act- und UETA-Richtlinien und stellt Ihnen wichtige Tools zur Verfügung, mit denen Sie sicherstellen können, dass Ihre Dokumente rechtsverbindlich sind.

- Übersichtliche Aufzeichnungen über die Signaturzuordnung und die Signaturzuweisung (Prüfpfade)
- Festgelegte Richtlinien zur Aufbewahrung von Dokumenten
- Abschlussbescheinigung über jedes unterzeichnete Dokument
- Einfache Methoden, mit denen Nutzer ihre Absicht, elektronisch zu unterzeichnen und Geschäfte zu tätigen, eindeutig nachweisen können

Beachten Sie bitte, dass die Foxit eSign-Software Ihnen zwar dabei helfen kann, die ESIGN- und UETA-Gesetze einzuhalten, dass sie aber möglicherweise nicht ausreicht, um die Anforderungen Ihrer lokalen, staatlichen oder internationalen Märkte oder bestimmte Branchenanfordderungen zu erfüllen. Prüfen Sie immer die entsprechenden Richtlinien.

Kalifornisches Verbraucherschutzgesetz (CCPA)

In Bezug auf das Recht des Verbrauchers auf Kenntnisnahme, Zugang, Löschung, Opt-Out und und Nichtdiskriminierung seiner persönlichen Daten durch Unternehmen und die Übermittlung von Daten für kalifornische Verbraucher hält sich Foxit eSign an das kalifornische Verbraucherschutzgesetz (California Consumer Privacy Act, CCPA), das vom Staat Kalifornien erlassen wurde.

Foxit eSign bestätigt, dass es sich in Bezug auf diese Daten streng an das CCPA hält. Wir benachrichtigen den Kunden über jede Anfrage seiner Kunden und treffen Vorkehrungen, um die erforderlichen Maßnahmen in Übereinstimmung mit dem Gesetz zu ergreifen, sofern der Kunde zustimmt.

EUROPÄISCHE UNION

Wir setzen die strikte Einhaltung der elektronischen Identifizierung und Vertrauensdienste für elektronische Transaktionen (Electronic Identification, Authentication, and Trust Services, eIDAS) durch, die in den EU-Vorschriften für Transaktionen im europäischen Binnenmarkt festgelegt sind.

Die eIDAS-Verordnung Nr. 910/2014 definiert drei primäre Ebenen für elektronische Signaturen: Einfache elektronische Signaturen (Basic Compliance), Fortgeschrittene elektronische Signaturen (Advanced Electronic Signatures, AES) und Qualifizierte elektronische Signaturen (Qualified Electronic Signatures, QES).

Einfache elektronische Signaturen, die zu dieser Stufe gehören, bestehen in der Regel aus Kontrollkästchen oder der Eingabe Ihres Namens und erfordern keine weiteren technischen Protokolle.

Fortgeschrittene elektronische Signaturen (AES) Bei fortgeschrittenen elektronischen Signaturen ist die Signatur des Signaturgebers direkt mit dem Dokument verknüpft, alle Änderungen werden überwacht und dokumentiert, und ein digitales Zertifizierungsverfahren wird zur Validierung der Signatur verwendet.

Qualifizierte elektronische Signaturen (QES): Dies ist die höchste und sicherste Stufe für elektronische Signaturen. Diese Stufe garantiert einen privaten Signaturschlüssel, stellt sicher, dass die bei der Erstellung der Signatur verwendeten Daten nur einmal verwendet werden können, schützt vor Fälschungen und ermöglicht es dem Signaturgeber, die volle Kontrolle über den Signaturprozess zu behalten. Qualifizierte Signaturen können nicht verändert, dupliziert oder reproduziert werden und unterliegen der Aufsicht eines qualifizierten Vertrauensdienstes.

Foxit eSign erfüllt die festgelegten Vorraussetzungen für fortgeschrittene elektronische Signaturen (AES) sowie qualifizierte elektronische Signaturen (QES).*

*Foxit eSign bietet QES über ZealiD. ZealiD verfolgt eine Datensicherheitsstrategie, die auf eIDAS-zertifizierten Vertrauensdiensten, eIDAS-zertifizierten ETSI-Standards und neuesten EU-Vorschriften zur Fernidentifizierung beruht.

DSGVO

Als Kunde von Foxit eSign haben Sie die folgenden Rechte, die durch die DSGVO festgelegt und durch Foxit eSign geschützt sind:

- Das Recht, der Verarbeitung Ihrer personenbezogenen Daten zu widersprechen.
- Das Recht, unzutreffende Daten berichtigen und unvollständige personenbezogene Daten vervollständigen zu lassen.
- Unter bestimmten Umständen das Recht auf unverzügliche Löschung Ihrer

personenbezogenen Daten.

- Unter bestimmten Umständen das Recht, die Verarbeitung Ihrer personenbezogenen Daten einzuschränken.

- Das Recht, aus Gründen, die sich aus Ihrer besonderen Situation ergeben, gegen die Verarbeitung Ihrer personenbezogenen Daten Widerspruch einzulegen, jedoch nur insoweit, als die Rechtsgrundlage für die Verarbeitung darin besteht, dass die Verarbeitung für die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die uns übertragen wurde, oder zur Wahrung unserer berechtigten Interessen oder der eines Dritten erforderlich ist.

- Das Recht, der Verarbeitung Ihrer personenbezogenen Daten zu Zwecken des Direktmarketings zu widersprechen.

- Das Recht, aus Gründen, die sich auf Ihre besondere Situation beziehen, gegen die Verarbeitung Ihrer personenbezogenen Daten zu wissenschaftlichen oder statistischen Zwecken oder zu historischen Forschungszwecken Widerspruch einzulegen, es sei denn, die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die aus Gründen des öffentlichen Interesses durchgeführt wird.

Foxit eSign bietet die folgenden Funktionen, um Kunden bei der Einhaltung der DSGVO zu unterstützen:

Auskunft[1] – Auf die meisten personenbezogenen Daten eines Benutzers oder Signaturgebers kann die betreffende Person direkt über die Foxit eSign-Benutzeroberfläche zugreifen, ebenso wie die autorisierte Partei der Organisation, die die Informationen beim Signaturgeber von Dokumenten angefordert hat.

Korrektur – Alle personenbezogenen Daten, die über Benutzer oder Signaturgeber gesammelt werden, sind über die Benutzeroberfläche verfügbar. Wenn Änderungen erforderlich sind, können der Benutzer und der Signaturgeber diese direkt beim Signieren des Dokuments vornehmen. Änderungen können vom Signaturgeber nach dem Signieren eines Dokuments veranlasst werden, indem der autorisierte Absender um eine Überprüfung/Aktualisierung seiner Unterlagen gebeten oder eine weitere Signaturanforderung gestellt wird.

Löschung – Je nach der Rolle des Benutzers beim Signiervorgang gibt es unterschiedliche Aktionen. Der Benutzer, der die Vereinbarung sendet, muss den Antrag auf Löschung bei dem Unternehmen stellen, bei dem er beschäftigt ist. Foxit eSign hat keinerlei Kontrolle über die Daten, die der Arbeitgeber während der Transaktion gesammelt hat. Während des Signiervorgangs werden die folgenden Daten eines Signaturgebers erfasst: Name, E-Mail-Adresse und IP-Adresse. Diese Daten werden zusammen mit der signierten Vereinbarung gespeichert und von

[1] Foxit eSign betreibt vertrauenswürdige US-amerikanische und europäische Datencenter mit SSAE16-Einrichtungen, die SOC 2 Typ 2-konform und PCI-konform sind. In den Vereinigten Staaten befinden sich die Rechenzentren in North Virginia (US-Ost), Ohio (US-Ost) und Nordkalifornien (US-West). In Europa befinden sich die Datencenter in Frankfurt, Deutschland.

dem Unternehmen kontrolliert, das die Vereinbarung gesendet hat. Wenn ein Signaturgeber Informationen benötigt, die sich auf die mit dieser Vereinbarung erhobenen personenbezogenen Daten beziehen, muss er sich an den Absender der Vereinbarung wenden. Foxit eSign darf dem Signaturgeber keine Informationen über die Vereinbarung oder das Unternehmen, das ihm die Vereinbarung gesendet hat, zur Verfügung stellen. Wenn der Signaturgeber den Eindruck hat, dass der Absender nicht kooperiert, kann Foxit eSign den Absender im Namen des Signaturgebers kontaktieren und die Löschung durchführen, wobei der Absender den Nachweis erbringen muss, dass die Versuche beim Absender nicht erfolgreich waren.

NACH BRANCHE

HIPAA (GESUNDHEITSWESEN)

Foxit eSign ist als HIPAA-konform zertifiziert und kann dazu beitragen, dass Ihre personenbezogenen und vertraulichen Dokumente und die Ihrer Patienten stets den Vorschriften entsprechen. Zum Schutz personenbezogener Daten (PII) stellt Foxit eSign sichere Felder zur Verfügung, um diese Informationen zu verbergen. Wir verwenden Verschlüsselung und Tokenisierung, um die Weitergabe von PII-Daten zu verhindern. Alle Daten werden im Hintergrund und bei der Übertragung verschlüsselt. Jede Signaturtransaktion mit Foxit eSign enthält einen vollständig rückverfolgbaren, fälschungssicheren Prüfpfad und wird mit einem Abschlusszertifikat versehen.

Die in unseren SOC2-geprüften Rechenzentren gespeicherten Dokumente werden mit dem AES-256-Standard auf der Anwendungsebene für Kundendokumente verschlüsselt, um absolute Vertraulichkeit zu gewährleisten.

Foxit eSign bietet Vereinbarungen für Geschäftspartner (Business Associate Agreements, BAA) im Rahmen der Pro- und Enterprise-Tarife an.

Darüber hinaus werden mit Foxit eSign die HIPAA-Bestimmungen wie folgt erfüllt:

- Rechtsverbindliche elektronische Signaturen (gemäß UETA und ESIGN), die den gesetzlichen Anforderungen standhalten
- Strenge Einhaltung der HIPAA-Standards für die Sicherheit und den Schutz elektronischer Daten
- Detaillierte Dokumentationsstandards, die Quellen- und Identitätsüberprüfung, Kodierungsschlüssel, Hash-Algorithmen zum Sperren von Dokumenten und andere Signaturtechnologien zur Unterstützung der Einhaltung von Vorschriften umfassen
- Umfassende Prüfung, die die Übertragung und Unterzeichnung jedes Dokuments verfolgt

21 CFR PART 11 (LIFE-SCIENCE)

Für diejenigen, die der 21 CFR Part 11 der FDA unterliegen, unterstützt Foxit eSign die Einhaltung dieser Vorschrift, indem die Bestimmungen der FDA für die Verwendung elektronischer Signaturen eingehalten und die zur Erfüllung der Anforderungen erforderlichen Funktionen und Werkzeuge bereitgestellt werden. Die Identität des Signaturgebers wird zum Zeitpunkt der Signierung und bei jedem ersten Zugriff auf das zu unterzeichnende Dokument überprüft, indem mindestens das Anmeldekennwort nach der ersten Identitätsprüfung angegeben wird. Nach Unterzeichnung des Dokuments durch den Empfänger wird es elektronisch mit einem Abschlusszertifikat gespeichert, das das Signaturbild, den Zeitstempel des Schlüsselereignisses und die IP-Adresse des Signaturgebers enthält.

Foxit eSign erfüllt die Anforderungen von 21 CFR Part 11 wie folgt:

- Methoden zur Identitätsüberprüfung
- Detaillierte Prüfpfade
- Schutz vor Manipulationen an Dokumenten, Manipulationsnachweis
- Zeitstempel
- Bescheinigung über die Fertigstellung der signierten Dokumente

FERPA (BILDUNGSWESEN)

Foxit eSign macht es Lehrkräften und Administratoren leicht, die FERPA-Anforderungen einzuhalten. Die Daten werden sicher aufbewahrt und sind sicher zugänglich, um die 45-Tage-Anforderungen für die Erfüllung von Aufzeichnungsanforderungen zu erfüllen. Darüber hinaus unterstützt Foxit eSign die Einhaltung von FERPA wie folgt:

- Die elektronische Signatur der von FERPA geforderten Freigabeformulare durch die Schüler, wobei die Sicherheit und Integrität der Aufzeichnungen durch fälschungssichere und fälschungsaufdeckende Funktionen gewährleistet wird
- Schulen erhalten eine sichere und einfache Möglichkeit, von Schülern und Eltern signierte Genehmigungen zur Freigabe von Schülerdaten einzuholen
- Bereitstellung rechtsverbindlicher Lösungen, die mit ESIGN und UETA konform sind
- Anhand von detaillierten Prüffunktionen, Zertifikaten für die Vervollständigung von Signaturen und digitalen Signaturschlüsseln können Schulen betrügerische

Signaturen verhindern sowie die Gültigkeit sicherstellen und gleichzeitig die FERPA-Anforderungen zur Validierung elektronischer Signaturen erfüllen

- Foxit eSign bietet sichere Felder, um personenbezogene Daten (PII) zu verbergen. Zudem werden durch Verschlüsselung und Tokenisierung PII-Datenlecks verhindert
- Alle Daten werden im Hintergrund und während der Übertragung verschlüsselt

FINRA (FINANZWESEN)

Foxit eSign unterstützt die Konformität mit FINRA Rule 4512, einschließlich FINRA 2019 Regulatory Notice Amendment 19-13, und die Anforderungen an die Dokumentenaufbewahrung gemäß Rule 17a-4(f), d. h. Sie können sicherstellen, dass der Versand und das Signieren von Dokumenten stets mit den Branchenvorschriften konform sind. Foxit eSign unterstützt FINRA-Konformität wie folgt:

- Bereitstellung rechtsverbindlicher Lösungen, die von allen großen Banken anerkannt werden und mit ESIGN und UETA konform sind
- Ausstellung fälschungssicherer und fälschungsaufdeckender digitaler Signaturen mit einer 256-Bit-Verschlüsselung, die sicherstellt, dass bei einem Versuch, ein Dokument zu ändern, ein Nachweis aufgezeichnet wird
- Strenge SOC-2-Typ-2-Prüfung und -Einhaltung sowie strikte Einhaltung der von AICPA fünf entwickelten Vertrauensdienstprinzipien
- Umfassende und detaillierte Prüfung, die alle von Absendern und Signaturgebern durchgeführten Aktionen, einschließlich Datum, Uhrzeit und Ort, anzeigt
- Vorlage einer detaillierten Bescheinigung über die Fertigstellung aller Dokumente
- Bereitstellung von Optionen für die Identitätsüberprüfung, wie die Zwei-Faktor-Authentifizierung (2FA) und die wissensbasierte Authentifizierung (Knowledge-Based Authentication, KBA)
- Benutzer können das ausgefüllte und signierte Dokument speichern und herunterladen, um es aufzubewahren

PCI DSS

Der Datensicherheitsstandard der Kreditkartenbranche (Payment Card Industry Data Security Standard, PCI DSS) ist ein Informationssicherheitsstandard für Unternehmen, die mit Kreditkarten der großen Kartensysteme arbeiten, um die Kontrolle der Verwaltung von Karteninhaberdaten zu verbessern und Betrug zu reduzieren. Foxit eSign ist konform mit PCI DSS 3.2.1 und erfüllt und übertrifft die Anforderungen zum Schutz der Daten von Kreditkarteninhabern. Darüber hinaus wird Foxit eSign regelmäßig auf höchste Sicherheitsrisiken getestet, darunter diejenigen, die in den OWASP Top 10 aufgeführt sind.

Foxit
Lennéstr. 1
10785 Berlin, Deutschland

Vertrieb: +49 30 234849944
oder +49 30 234849945
Support: +49 30 21783691

sales-eu@foxit.com
Support Center
www.foxit.com