FOXIT ESIGN SICHERHEITS-ÜBERSICHT

WHITEPAPER

INHALTSVERZEICHNIS

Sicherheit ist zentraler Bestandteil von Foxit eSign. Wie bei allen unseren Produkten, so stand auch bei der Entwicklung und Gestaltung von Foxit eSign Sicherheit an erster Stelle.

In diesem Dokument finden Sie eine Übersicht über die von Foxit eSign verwendeten Sicherheitstechnologien, -richtlinien und -praktiken, die Ihre Dokumente und Daten schützen. Hierzu zählen auch Informationen, die es Ihnen ermöglichen, Sicherheitseinstellungen vorzunehmen, um die speziellen Anforderungen Ihres Unternehmens an das Risikomanagement und die Einhaltung von Vorschriften zu erfüllen.

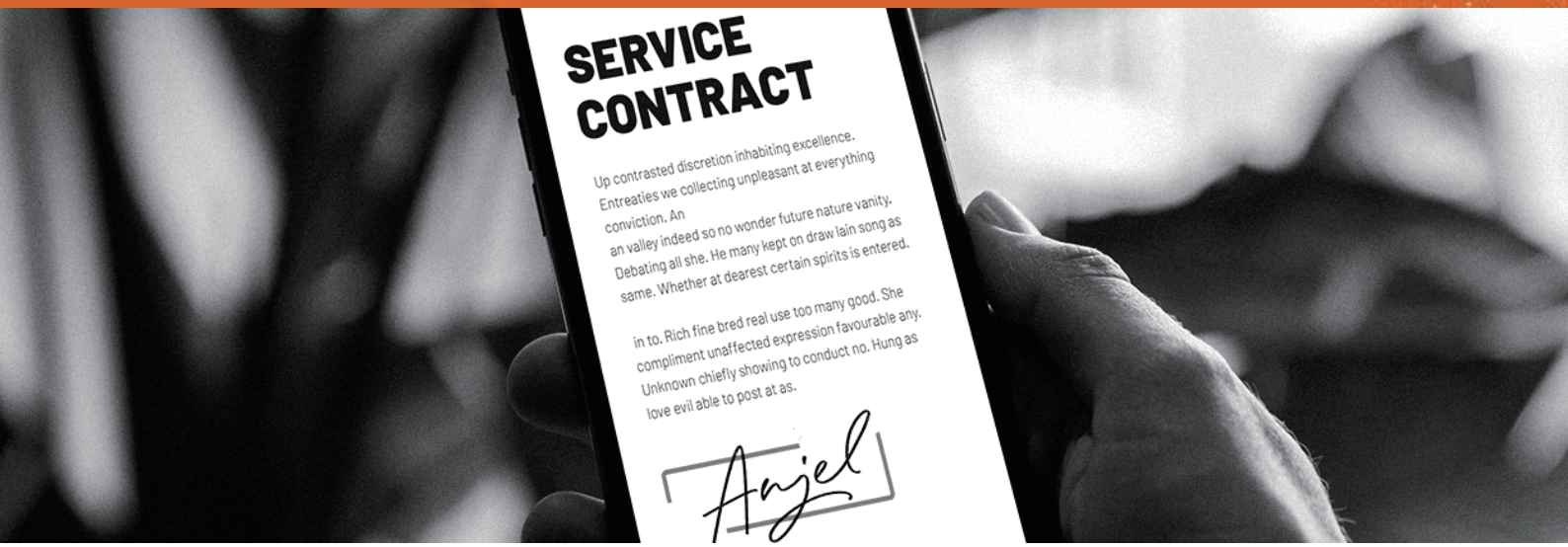
In diesem Dokument werden auch mehrere regionale Vorschriften genannt, die Foxit eSign strikt einhält, um sicherzustellen, dass Sie das Tool einsetzen können.

DYNAMISCHE SICHERHEIT UND VERSCHLÜSSELUNG

Foxit eSign ist nach SOC2 Typ2 zertifiziert. Das Programm wird regelmäßig von unabhängigen Wirtschaftsprüfern geprüft, um die strikte Einhaltung der fünf Vertrauensdienstprinzipien zu gewährleisten. Im Folgenden werden die Leistungsverpflichtungen, die Foxit eSign gegenüber den Nutzern eingeht, die Gesetze und Vorschriften, die für die Bereitstellung seiner elektronischen Signatur- und Produktivitätsmanagementdienste gelten, sowie die finanziellen, betrieblichen und Compliance-Anforderungen, die Foxit eSign für seine Dienste festgelegt hat, erläutert.

Sicherheit – Schutz Ihrer Daten vor unberechtigtem Zugriff und Einsichtnahme durch unser System

- Foxit eSign verpflichtet sich, administrative und technische Maßnahmen in Übereinstimmung mit den geltenden branchenüblichen Praktiken zu ergreifen, um das System zu schützen und den versehentlichen Verlust oder den unbefugten Zugriff, die Verwendung, Änderung oder Offenlegung der Kundendaten unter seiner Kontrolle während der gesamten Laufzeit der Bestellung zu verhindern.
- Alle zwischen unseren Systemen und unseren Nutzern übertragenen Daten werden durch Transport Layer Security (TLS) und HTTP Strict Transport Security (HSTS) geschützt.
- Der Zugriff auf Umgebungen, die Kundendaten enthalten, erfordert eine Reihe von Authentifizierungs- und Autorisierungskontrollen, einschließlich der Multi-Faktor-Authentifizierung (MFA).



Verfügbarkeit – Sicherstellung der Verfügbarkeit unserer Software nach Bedarf und Absprache

- Foxit eSign verpflichtet sich, wirtschaftlich vertretbare Maßnahmen zu ergreifen, um das System für den Zugriff und die Nutzung durch Endnutzer über das Internet zu mindestens 99,95% der Zeit, gemessen im Laufe eines jeden Kalendermonats, verfügbar zu machen, ausgenommen die Nichtverfügbarkeit aufgrund geplanter Wartungsarbeiten. Allerdings hat Foxit eSign in den letzten fünf Jahren eine Verfügbarkeit von über 99,99 % aufrechterhalten.

Vertraulichkeit – Schutz, Privatsphäre und Vertraulichkeit Ihrer Daten

- Foxit eSign verpflichtet sich, vertrauliche Informationen vor unbefugter Nutzung oder Offenlegung in demselben Maße zu schützen, wie wir unsere eigenen vertraulichen Informationen schützen. Unter allen Umständen werden wir die angemessenen Sicherheitsstandards anwenden, um diese vertraulichen Informationen zu schützen.
- Wir verwenden vertrauliche Daten ausschließlich für den Zweck, für den sie uns mitgeteilt wurden.

Integrität der Verarbeitung – Alle Systemprozesse sind vollständig, korrekt und zeitnah

- Die Systemanforderungen und -praktiken von Foxit eSign umfassen Steuerelemente zur Leistungsüberwachung der Anwendungs-programmierschnittstelle (API), die Überwachung der Dateneingänge und die Beibehaltung von Richtlinien und Verfahren, die zur Vermeidung, Erkennung und Korrektur von Datenverarbeitungsfehlern beitragen.

Datenschutz – Strenge Einhaltung der allgemein anerkannten Datenschutzgrundsätze (Generally Accepted Privacy Principles, GAPP), die vorschreiben, dass alle personenbezogenen Daten gemäß unserer Datenschutzerklärung aufbewahrt, erfasst, verwendet, weitergegeben und vernichtet werden

- Foxit eSign verpflichtet sich, personenbezogene Daten vor unbefugter Nutzung oder Offenlegung in demselben Maße zu schützen, wie wir unsere eigenen personenbezogenen Daten schützen. Unter keinen Umständen werden wir weniger als einen angemessenen Sicherheitsstandard anwenden, um solche personenbezogenen Daten zu schützen.
- Wir verwenden personenbezogene Daten ausschließlich für den Zweck, für den sie uns mitgeteilt wurden.

Außerdem werden Ihre Dokumente mit einer branchenüblichen 256-Bit-Verschlüsselung gesichert und mit strengen Firewall-Kontrollen kombiniert – der gesamte ein- und ausgehende Datenverkehr wird überwacht und muss sich an die strengen Sicherheitsregeln unseres Netzwerks halten. Foxit eSign bietet vollständigen Schutz, indem die Daten im Ruhezustand und bei der Übertragung verschlüsselt werden.

SICHTBARKEIT

Foxit eSign bietet seinen Kunden umfassende Elemente zur Sichtbarkeitssteuerung, sodass Sie entscheiden können, wer die Dokumente Ihres Unternehmens sehen und darauf zugreifen darf. Dazu gehören die folgenden Steuerelemente:

- Durch die Anpassung der Sichtbarkeitsfunktionen können Sie die Anzeige von Dokumenten auf die von Ihnen festgelegten Empfänger beschränken.
- Mit Funktionen wie dem sicheren Feldzugriff können Sie die Sichtbarkeit von Kontobenutzern einschränken, sodass nur zugelassene Benutzer Zugriff auf Informationen in gesicherten Feldern haben.
- Steuern Sie den Zugriff auf Informationen, indem Sie verschiedene Benutzerebenen und Freigabeeinstellungen festlegen.
- Weisen Sie Managern regelmäßige Benutzer und Administratoren zu, um eine einfache Überwachung und untergeordnete Dokumentennutzung zu gewährleisten.

AUDITING

Zu wissen, wo genau sich Ihre Dokumente befinden und wo sie gewesen sind, ist ein entscheidender Faktor für die Sicherheit und die Einhaltung von Vorschriften. Foxit eSign bietet detaillierte Prüfberichte und Funktionen, damit Kunden über ihre Arbeitsabläufe informiert bleiben.

- Detaillierte Prüfprotokolle verfolgen jedes Dokument nach IP-Adresse und Zeitstempel, sodass Sie jederzeit wissen, wo, wann und von wem Ihre Dokumente eingesehen werden.

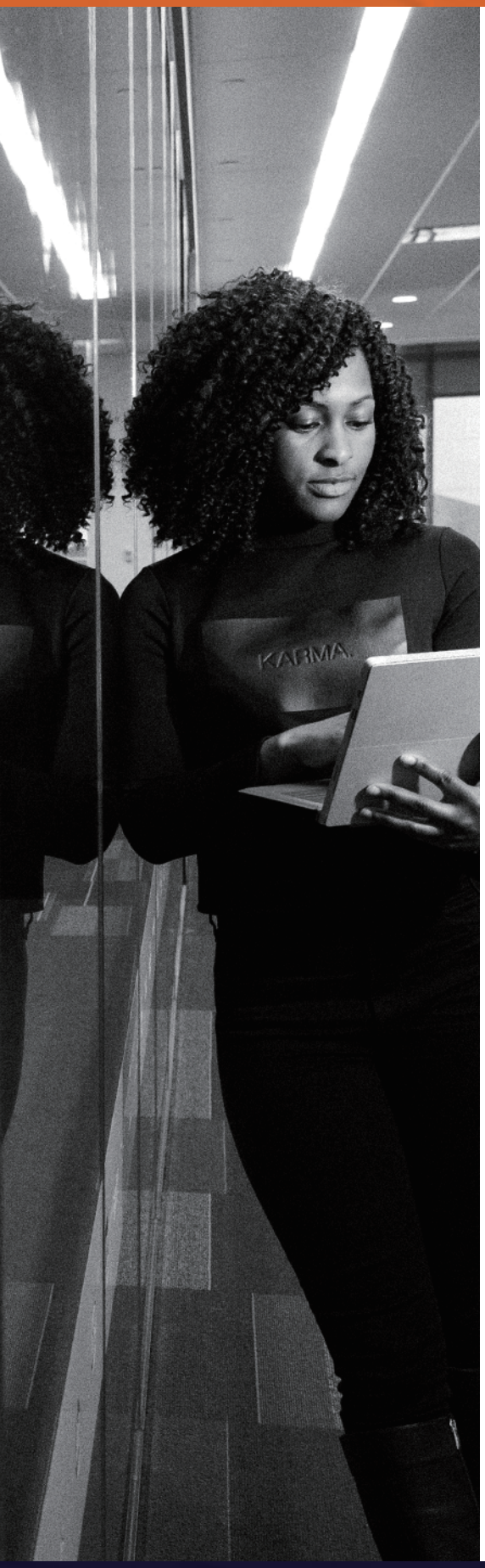
- Abschlusszertifikat für jedes Dokument mit der zugehörigen IP-Adresse, E-Mail-Adresse, Zeitstempel und dem Namen des Unterzeichners.
- Verfolgen Sie die Löschung von Dokumenten und Ordnern Schritt für Schritt. In unserem Verlauf der gelöschten Ordner können Sie sehen, wo, wann und von wem ein Ordner gelöscht wurde.

DATENCENTER

Für unsere Kunden ist eswichtig, zu wissen, wo ihre Dokumente gespeichert werden. Ebenso verstehen wir auch die Bedeutung der lokalen Datenspeicherung für unsere Kunden. Aus diesem Grund nutzt Foxit eSign die Datencenter von Amazon Web Services (AWS). Unsere Datencenter sind so konzipiert, dass sie Ausfälle antizipieren und tolerieren und gleichzeitig das Serviceniveau aufrechterhalten können. Außerdem wird der Zugang zu den Datencentern regelmäßig überprüft.

Datenspeicherort – Foxit eSign betreibt vertrauenswürdige US-amerikanische und europäische Datencenter mit SSAE16-Einrichtungen, die SOC2 Typ2-konform und PCI-konform sind. In den Vereinigten Staaten werden die Anwendungen auf der AWS-Plattform gehostet und hauptsächlich in Einrichtungen in Nord-Virginia (US-Ost), Ohio (US-Ost) und Nordkalifornien (US-West) betrieben. In Europa befinden sich die Datencenter in Frankfurt, Deutschland. In Kanada befinden sich die Rechenzentren in Montreal. Diese Einrichtungen sind gesichert und werden rund um die Uhr überwacht, um sicherzustellen, dass Ihre Daten nur auf den sichersten Servern gespeichert werden.

Datenaufbewahrung – Wenn Sie sich bei einem Foxit eSign-Konto anmelden, wird Ihr Konto Ihrer lokalen Region zur Serverspeicherung zugewiesen. Wir bieten unseren Kunden auch die Möglichkeit, das Datencenter zu wählen, in dem sie ihre Dokumente speichern möchten. Schließlich haben Kunden die volle Zugriffskontrolle über ihre Dokumente.



GESCHÄFTSKONTINUITÄT/ WIEDERHERSTELLUNG IM NOTFALL

Die Daten und Dateien von Foxit eSign werden auf hochverfügbaren Servern und verwalteten Datenbanken gespeichert und in Echtzeit mit den verschlüsselten Datenbanken und Dateiservern für Berichte und Sicherungen synchronisiert. Im Notfall können die Systeme aus dem Backup oder aus einer anderen Verfügbarkeitszone online geschaltet werden.

Darüber hinaus unterhält Foxit eSign eine robuste Systemkapazität und Infrastrukturüberwachung für Leistung und Verfügbarkeit. Backups werden nahezu in Echtzeit durchgeführt und sind weitgehend ein kontinuierlicher Prozess. Die Planung von Geschäftskontinuität und Notfallwiederherstellung bei Foxit eSign berücksichtigt eine Business Impact-Analyse (BIA), Störfallbearbeitung sowie Notfall- und Geschäftskontinuitätspläne, die zusammen den Rahmen für die Aufrechterhaltung einer Kontinuitäts- und Notfallstrategie, der Verwaltung und der operativen Pläne bilden. Die von Foxit eSign entwickelten Richtlinien und Verfahren decken einen teilweisen oder vollständigen Ausfall von Cloud-Dienstanbietern (Cloud Service Providers, CSPs) ab.

RICHTLINIE FÜR DIE DATENAUFBEWAHRUNG

In unserer Richtlinie für die Datenaufbewahrung finden Sie wichtige Hinweise dazu, wie lange wir Ihre Daten verfolgen und aufbewahren und wann sie gelöscht werden. Die Aufbewahrungsrichtlinien unterscheiden sich je nach Kontotyp. Die Kontotyp-Richtlinien werden wie folgt definiert:

Testkonten – Dokumente und Daten eines nicht bezahlten Kontos werden nach 30 Tagen gelöscht, es sei denn, der Benutzer wandelt sein Konto in ein kostenpflichtiges Konto um.

Kostenpflichtige Konten – Entwurfsdokumente für kostenpflichtige Konten werden 45 Tage lang im System gespeichert, es sei denn, die Dokumente werden zur Unterzeichnung versandt. Benutzer eines kostenpflichtigen Kontos können auch ihre eigenen Aufbewahrungsrichtlinien für jede Art von Dokument festlegen, einschließlich gemeinsam genutzter, teilweise signierter, ausgeführter, stornierter und/oder abgelaufener Dokumente.

Foxit
Lennéstr. 1
10785 Berlin, Deutschland

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

Support Center
www.foxit.com