

VISÃO GERAL DA CONFORMIDADE DO FOXIT ESIGN

Algumas organizações estão sujeitas a vários requisitos regulatórios específicos, e o Foxit eSign pode servir como um componente principal para cumprir suas obrigações de conformidade. Este documento descreve vários regulamentos, tanto por região quanto por setor, com os quais o Foxit eSign oferece suporte à conformidade.



SUMÁRIO

Por região	3
Estados Unidos	3
Lei de Privacidade do Consumidor da Califórnia (CCPA)	3
União Europeia	4
GDPR	4
Por setor	6
HIPAA (Saúde)	6
21 CFR Parte 11 (Ciências da Vida)	6
FERPA (Educação)	7
FINRA (Finanças)	8
PCI DSS	8

POR REGIÃO



ESTADOS UNIDOS

O Foxit eSign é 100% compatível com todos os regulamentos de conformidade da Lei E-SIGN e UETA dos EUA e fornece ferramentas importantes para ajudar a garantir que seus documentos sejam juridicamente vinculativos.

- Limpe registros de associação e de atribuição de assinatura (trilhas de auditoria)
- Política definida de retenção de documentos
- Certificado de conclusão fornecido para cada documento assinado
- Métodos fáceis para os usuários demonstrarem a intenção clara de assinar e realizar negócios eletronicamente

É importante ter em mente que, embora o software Foxit eSign possa ajudar a cumprir as leis E-SIGN e UETA, isso poderá não ser suficiente para seus requisitos locais, estaduais, internacionais ou do setor. Verifique sempre as diretrizes correspondentes.



LEI DE PRIVACIDADE DO CONSUMIDOR DA CALIFÓRNIA (CCPA)

O Foxit eSign está em conformidade com a Lei de Privacidade do Consumidor da Califórnia (CCPA), conforme estabelecido pelo estado da Califórnia em relação ao direito do consumidor de saber, de ter acesso, de excluir, de não discriminar, direito à não discriminação de suas informações pessoais de quaisquer empresas que tenham negócios e transfiram dados para os consumidores da Califórnia.

O Foxit eSign certificou que cumpre estritamente a CCPA em relação a esses dados. Notificaremos o cliente de qualquer solicitação dos seus clientes e tomaremos as medidas jurídicas necessárias mediante o consentimento do cliente, conforme necessário.



UNIÃO EUROPEIA

Reforçamos a estrita conformidade com os Serviços de Identificação, Autenticação e Confiança Eletrônica (eIDAS), conforme estabelecido pelos regulamentos da UE para as transações no Mercado Único Europeu.

O regulamento eIDAS nº 910/2014 define os três principais níveis de assinaturas eletrônicas: Conformidade básica, Assinaturas eletrônicas avançadas (AES) e Assinaturas eletrônicas avançadas qualificadas (QES ou QAES).

Conformidade básica: as assinaturas que se enquadram nesse nível geralmente consistem em caixas de seleção ou digitação do seu nome e não exigem nenhum protocolo tecnológico adicional.

Assinaturas eletrônicas avançadas (AES): com as assinaturas eletrônicas de nível avançado, a assinatura do assinante é vinculada diretamente ao documento, todas as alterações são monitoradas e documentadas e é usado um processo de certificação digital para validar a assinatura.

Assinaturas eletrônicas avançadas qualificadas (QES ou QAES): este é o nível de assinatura eletrônica mais alto e mais qualificado. Esse nível garante uma chave de assinatura privada, assegura que os dados usados na criação da assinatura só possam ser usados uma vez, protege contra falsificação e permite que o signatário mantenha o controle total do processo de assinatura. As assinaturas qualificadas não podem ser alteradas, duplicadas ou reproduzidas e permanecem sob a supervisão de um provedor de confiança qualificado.

O Foxit eSign está em conformidade com os pré-requisitos definidos pelo Assinaturas Eletrônicas Avançadas (AES) e Assinaturas Eletrônicas Qualificadas (QES).*

*O Foxit eSign oferece QES via ZealiD. ZealiD adere a uma estratégia de segurança de dados baseada em serviços de confiança com certificação eIDAS, padrões ETSI com designação eIDAS e regulamentos de identificação distante da UE de ponta.



GDPR

Como cliente do Foxit eSign, você tem os seguintes direitos, conforme estabelecido pela lei GDPR e protegido pelo Foxit eSign:

- O direito de confirmar o processamento de seus dados pessoais.
- O direito de corrigir dados imprecisos e preencher dados pessoais incompletos.
- Em algumas circunstâncias, o direito à exclusão dos seus dados pessoais sem atrasos injustificados.

- Em algumas circunstâncias, o direito de restringir o processamento dos seus dados pessoais.
- O direito de se opor ao processamento de seus dados pessoais por motivos relacionados à sua situação particular, mas apenas na medida em que a base jurídica para o processamento seja que o processamento seja necessário para: o desempenho de uma tarefa realizada no interesse público ou no exercício de qualquer autoridade oficial que nos seja conferida; ou as finalidades dos interesses legítimos adotados por nós ou por terceiros.
- O direito de se opor ao nosso processamento dos seus dados pessoais para marketing direto.
- O direito de se opor ao nosso processamento de seus dados pessoais para pesquisa científica ou histórica ou para fins estatísticos por motivos relacionados à sua situação particular, a menos que o processamento seja necessário para o desempenho de uma tarefa realizada por motivos de interesse público.

O Foxit eSign oferece os seguintes recursos para ajudar os clientes a cumprir o GDPR:

Acesso¹ – A maioria das informações pessoais sobre um usuário ou signatário pode ser acessada diretamente por essa pessoa na interface de usuário do Foxit eSign e pela parte autorizada da organização que solicitou as informações durante a assinatura dos documentos.

Correção – Todas as informações pessoais coletadas sobre usuários ou signatários estão disponíveis na interface do usuário. Se for necessário fazer alterações, o usuário e o signatário podem fazê-las diretamente ao assinar o documento. As alterações podem ser iniciadas pelo signatário após a assinatura de qualquer documento, solicitando ao Remetente autorizado uma revisão/atualização em seus registros ou reiniciando outra solicitação de assinatura.

Exclusão – Existem diferentes ações dependendo da função do usuário no evento de assinatura. O Usuário que enviar o contrato deverá fazer o pedido de exclusão à empresa na qual está empregado. O Foxit eSign não controla os dados que o empregador coletou durante a transação. O processo de assinatura coleta as seguintes informações sobre um assinante durante o evento de assinatura: nome, endereço de e-mail e endereço IP. Essas informações são armazenadas com o contrato com sua assinatura e são controladas pela empresa que enviou o contrato. Se um Signatário precisar de informações relacionadas às informações pessoais coletadas com esse contrato, ele deverá entrar em contato com o Remetente do contrato. O Foxit eSign não pode fornecer nenhuma informação ao Signatário sobre o contrato ou a empresa que o enviou. Se o signatário sentir que não há cooperação da parte remetente, o Foxit eSign pode entrar em contato com o remetente em nome do signatário e facilitar a exclusão, mas o remetente deverá compartilhar a prova de que as tentativas de envio fracassaram.

¹ O Foxit eSign mantém os data centers confiáveis nos EUA e na Europa com instalações SSAE16 que estão em conformidade com o SOC 2 Tipo 2 e o PCI. Nos Estados Unidos, os data centers estão localizados no norte da Virgínia (Leste dos EUA), Ohio (Leste dos EUA) e Norte da Califórnia (Oeste dos EUA). Na Europa, os data centers estão localizados em Frankfurt, na Alemanha.

POR SETOR



HIPAA (SAÚDE)

O Foxit eSign é certificado em conformidade com HIPAA e pode ajudar a garantir que você e a documentação confidencial e sensível do seu paciente estejam sempre dentro da regulamentação. Para manter as informações de identificação pessoal (PII), o Foxit eSign fornece campos seguros para mascarar essas informações. Usamos criptografia e tokenização para evitar vazamentos de dados PII. Todos os dados são criptografados em repouso e em movimento. Cada transação do Foxit eSign Signature contém uma trilha de auditoria totalmente rastreável e inviolável e recebe um Certificado de conclusão.

Os documentos armazenados em nossos data centers auditados pelo SOC2 são criptografados com o padrão AES 256 no nível do aplicativo para documentos do cliente para garantir total confidencialidade.

O Foxit eSign oferece Contratos de Associado Comercial (BAA) (BAA) nos planos Pro e Enterprise.

Além disso, o Foxit eSign está em conformidade com os regulamentos HIPAA através de:

- Assinaturas eletrônicas juridicamente vinculativas (de acordo com UETA e E-SIGN) que serão mantidas em tribunais
- Adesão estrita aos padrões de segurança e proteção eletrônica da HIPAA
- Padrões detalhados de documentação que incluem verificação de origem e identidade, chaves de criptografia, algoritmos de hash para bloquear documentos e outras tecnologias de assinatura que dão suporte à conformidade
- Auditoria completa que rastreia o movimento e a assinatura de cada documento



21 CFR PARTE 11 (CIÊNCIAS DA VIDA)

Para aqueles que aderem à conformidade com a 21 CFR Parte 11 da FDA, o Foxit eSign apoia a conformidade com este regulamento aderindo ao código de regulamentos estabelecido pela FDA para utilização de assinaturas eletrônicas e fornecendo os recursos e ferramentas necessários para atender aos requisitos. A identidade do signatário é verificada no momento da assinatura e cada iniciação, fornecendo a senha de login no mínimo após as verificações iniciais de identidade no acessar ao documento para assinatura. Depois da assinatura do documento pelos destinatários, ele é

armazenado eletronicamente com um certificado de conclusão contendo a imagem da assinatura, os carimbos de data e hora dos principais eventos e o endereço IP do assinante.

O Foxit eSign está em conformidade com a 21 CFR Parte 11 através de:

- Métodos de verificação de identidade
- Trilhas de auditoria detalhadas
- Proteção contra adulteração de documentos, evidências de adulteração
- Carimbos de data e hora
- Certificado de conclusão para documentos assinados



FERPA (EDUCAÇÃO)

O Foxit eSign facilita o cumprimento dos requisitos da FERPA por educadores e administradores, mantendo os dados seguros e acessíveis para acomodar os requisitos de 45 dias para atender às solicitações de registros. Além disso, o Foxit eSign oferece suporte à conformidade FERPA da seguinte forma:

- Fornecendo uma maneira eletrônica para os alunos assinarem os formulários de liberação exigidos pela FERPA mantendo a segurança e a integridade dos registros através de recursos invioláveis e à prova de adulteração
- Fornecendo às escolas uma maneira segura e fácil de coletar permissões assinadas de alunos e pais para liberar registros de alunos
- Fornecendo soluções juridicamente vinculativas compatíveis com E-SIGN e UETA
- Através de recursos de auditoria detalhados, certificados de conclusão de assinatura e chaves de assinatura digital que permitem que as escolas evitem assinaturas fraudulentas e garantam a validade de forma eficaz, atendendo aos requisitos da FERPA para validação de assinaturas eletrônicas
- O Foxit eSign fornece campos seguros para mascarar informações de identificação pessoal (PII) e utiliza criptografia e tokenização para evitar vazamentos de dados de PII
- Todos os dados são criptografados em repouso e em movimento



FINRA (FINANÇAS)

O Foxit eSign oferece suporte à conformidade com a Regra 4512 da FINRA, incluindo a Emenda 19-13 do Aviso Regulatório da FINRA 2019 e os requisitos de retenção de documentos da Regra 17a-4(f), o que significa que você tem a garantia de que o envio e a assinatura dos documentos estejam sempre em conformidade com os regulamentos do setor. O Foxit eSign oferece suporte à conformidade FINRA da seguinte forma:

- Fornecendo soluções juridicamente vinculativas reconhecidas por todos os principais bancos em conformidade com ESIGN e UETA
- Através da emissão de assinaturas digitais à prova de adulteração e de violação com criptografia de 256 bits garantindo que em caso de tentativa de alteração de um documento, exista uma prova registada
- Através de auditoria e conformidade rigorosas do SOC 2 Tipo 2 e estrita adesão aos 5 Princípios de Serviço de Confiança desenvolvidos pelo AICPA
- Fornecendo auditoria completa e detalhada que exhibe todas as ações realizadas por remetentes e signatários, incluindo datas, horários e locais
- Fornecendo um certificado detalhado de conclusão para todos os documentos
- Através do fornecimento de opções de métodos de verificação de identidade, como autenticação de dois fatores (2FA) e autenticação baseada em conhecimento (KBA)
- Permitindo que os usuários salvem e baixem os documentos assinados preenchidos para retenção de registros



PCI DSS

O Padrão de Segurança de Dados da Indústria de Cartão de Pagamento (PCI DSS) é um padrão de segurança da informação para as organizações que lidam com cartões de crédito das principais bandeiras de cartões para aumentar os controles de gerenciamento de dados do titular do cartão e reduzir as fraudes. O Foxit eSign mantém a conformidade com o PCI DSS 3.2.1, atendendo e superando os requisitos para proteger o manuseio dos dados do titular do cartão de crédito. Além disso, o Foxit eSign é testado regularmente contra riscos de segurança de alto nível, incluindo aqueles encontrados no OWASP Top 10.