FOXIT ESIGN: DESCRIPCIÓN GENERAL DE CUMPLIMIENTO

Algunas organizaciones están sujetas a un rango de requerimientos regulatorios específicos, por lo que Foxit eSign puede servir como un componente clave para llevar a cabo sus obligaciones de cumplimiento. Este documento describe varias regulaciones, tanto por región como por industria, con las que Foxit eSign apoya el cumplimiento.

DOCUMENTO TÉCNICO

ÍNDICE

Por región 3

Estados Unidos 3

Ley de Privacidad del Consumidor de California (California Consumer Privacy Act, CCPA) 3

Unión Europea 4

GDPR 4

Por industria 6

HIPAA (servicios de salud) 6

21 CFR Parte 11 (ciencias de la vida) 6

FERPA (educación) 7

FINRA (finanzas) 8

PCI DSS 8

POR REGIÓN

ESTADOS UNIDOS

Foxit eSign es 100% compatible con todas las regulaciones de cumplimiento de las normas UETA y de la ley ESIGN de EE. UU.; además, le proporciona importantes herramientas para ayudarle a asegurar que sus documentos sean legalmente vinculantes.

- Registros de asociación de firmas claros y atribución de firmas (pistas de auditoría)
- Política de retención de documentos definida
- Se proporciona un certificado de finalización por cada documento firmado
- Métodos sencillos para que los usuarios demuestren su clara intención de firmar y realizar negocios por medio electrónico

Es importante tener en cuenta que, si bien el software Foxit eSign puede ayudarle a cumplir con las leyes ESIGN y UETA, tal vez no sea suficiente para los requerimientos de sus mercados locales, estatales, internacionales o de la industria. Revise siempre los lineamientos correspondientes.

LEY DE PRIVACIDAD DEL CONSUMIDOR DE CALIFORNIA (CALIFORNIA CONSUMER PRIVACY ACT, CCPA)

Foxit eSign cumple con la Ley de Privacidad del Consumidor de California (California Consumer Privacy Act, CCPA) según lo establecido por el estado de California con respecto al derecho del consumidor de saber, de acceder a, de eliminar, de exclusión, de la no discriminación de su información personal por parte de cualquier empresa que realice actividades comerciales y transfiera los datos para los consumidores de California.

Foxit eSign ha certificado que se adhiere de manera estricta a la CCPA con respecto a dichos datos. Notificaremos al consumidor sobre cualquier solicitud de parte de sus clientes y adoptaremos las disposiciones para tomar la acción necesaria según la ley con base en el consentimiento del consumidor según se requiera.

UNIÓN EUROPEA

Exigimos el estricto cumplimiento de los Servicios electrónicos de identificación, autenticación y confianza (eIDAS) según lo establecido por las regulaciones de la UE para las transacciones en el mercado individual europeo.

La regulación No. 910/2014 de eIDAS define tres niveles principales de firmas electrónicas: Cumplimiento básico, Firmas electrónicas avanzadas (AES) y Firmas electrónicas avanzadas cualificadas (QES o QAES).

Cumplimiento básico: Las firmas que se encuentran en este nivel consisten por lo general de casillas de verificación o escribir su propio nombre, por lo que no requieren protocolos tecnológicos adicionales.

Firmas electrónicas avanzadas (AES): Con las firmas electrónicas avanzadas, la firma del firmante se enlaza directamente al documento, todos los cambios se monitorean y documentan, y se usa un proceso de certificación digital para validar la firma.

Firmas electrónicas avanzadas cualificadas (QES o QAES): Este es el nivel de firmas electrónicas más alto y cualificado. Este nivel garantiza una clave de firma privada, asegura que los datos que se utilicen en la creación de la firma puedan usarse solo una vez, protege contra la falsificación y permite al firmante conservar el completo control del proceso de firma. Las firmas cualificadas no pueden alterarse, duplicarse o reproducirse y se mantienen bajo la supervisión de un proveedor de confianza cualificado.

Foxit eSign cumple con los requisitos previos establecidos por las Firmas electrónicas avanzadas (AES) y las Firmas electrónicas cualificadas (QES).*

*Foxit eSign ofrece QES a través de ZealiD. ZealiD se adhiere a la estrategia de seguridad de los datos basada en los servicios de confianza certificados de eIDAS, las normas ETSI designadas por eIDAS y las avanzadas normativas de identificación a distancia de la UE.

GDPR

Como cliente de Foxit eSign, tiene los siguientes derechos según lo establecido por la ley GDPR y por la protección de Foxit eSign:

- El derecho de confirmar el procesamiento de sus datos personales.
- El derecho de corregir los datos imprecisos y de completar los datos personales incompletos.
- En algunas circunstancias, el derecho de borrar sus datos personales sin ningún retraso indebido.

- En algunas circunstancias, el derecho de restringir el procesamiento de sus datos personales.
- El derecho a objetar el procesamiento de sus datos personales por razones de su situación particular, pero solo en la medida en que la base legal del procesamiento sea que dicho procesamiento es necesario para: el desempeño de una tarea que se lleva a cabo por el interés público o en el ejercicio de cualquier autoridad oficial que se nos confiera; o para los fines de los intereses legítimos nuestros o de un tercero.
- El derecho a objetar el procesamiento de sus datos personales para fines de marketing directo.
- El derecho a objetar el procesamiento de sus datos personales para fines de investigación científicos o históricos, o para fines estadísticos relacionados con su situación particular, a menos que el procesamiento sea necesario para desempeñar una tarea que se lleve a cabo por motivos de interés público.

Foxit eSign ofrece las siguientes características para ayudar a que los clientes cumplan con GDPR:

Acceso[1]: un usuario o firmante puede acceder directamente a la mayoría de su información personal a través de la interfaz de usuario de Foxit eSign; una parte autorizada también puede acceder a dicha información de la organización que solicitó la información durante la firma de documentos.

Corrección: toda la información personal que se recolecta sobre los usuarios o firmantes está disponible a través de la interfaz de usuario. Si hay que realizar cambios, el usuario y el firmante pueden realizar los cambios directamente durante la firma del documento. El firmante puede iniciar los cambios después de firmar un documento al solicitar que el emisor autorizado haga una revisión/actualización de sus registros o se reinicie otra solicitud de firma.

Eliminación: hay distintas acciones dependiendo del rol del usuario en el evento de firma. Un usuario que envíe el acuerdo debe realizar la solicitud de eliminación a la empresa para la que trabaja. Foxit eSign no controla los datos que el empleado haya recolectado durante la transacción. El proceso de firma recolecta la siguiente información sobre un firmante durante el evento de firma: nombre, dirección de correo electrónico y dirección IP. Esta información se guarda con el acuerdo con su firma y lo controla la empresa que envió dicho acuerdo. Si un firmante necesita información que pertenezca a la información personal recolectada con dicho acuerdo, necesita contactar al emisor del acuerdo. Foxit eSign no puede proveer información al firmante sobre el acuerdo o la empresa que les envió dicho acuerdo. Si el firmante siente que no hay cooperación de la parte emisora, Foxit eSign puede contactar al emisor en representación del firmante y facilitar la eliminación, pero el emisor debe compartir una prueba de que los intentos con el emisor no fueron exitosos.

[1] Foxit eSign mantiene centros de datos de confianza en EE.UU. y Europa con instalaciones SSAE16 que cumplen con los estándares SOC 2 tipo 2 y PCI. En Estados Unidos, los centros de datos se encuentran en Virginia del Norte (Este de EE. UU.), Ohio (Este de EE. UU.) y el norte de California (Oeste de EE. UU.). En Europa, los centros de datos se encuentran en Frankfurt, Alemania.

POR INDUSTRIA

HIPAA (SERVICIOS DE SALUD)

Foxit eSign está certificado como compatible con HIPAA y puede ayudar a asegurar que tanto su información privada y confidencial como la de su paciente estén siempre dentro de la regulación. Para mantener la información de identificación personal (PII), Foxit eSign provee campos seguros para enmascarar dicha información. Utilizamos encriptación y tokenización para evitar fugas de datos de PII. Todos los datos se encriptan almacenados y en tránsito. Cada transacción de firma de Foxit eSign contiene una pista de auditoría completamente rastreable y a prueba de alteraciones; además se proporciona un Certificado de finalización.

Los documentos almacenados en nuestros centros de datos auditados por SOC2 y se encriptan con el estándar AES 256 a nivel de aplicación, para asegurar la completa confidencialidad de los documentos de los clientes.

Foxit eSign ofrece Acuerdos de Socio Comercial (BAA) bajo los planes Pro y Enterprise.

Además, Foxit eSign cumple con las regulaciones de la HIPAA a través de lo siguiente:

- Firmas electrónicas legalmente vinculantes (de conformidad con UETA y ESIGN) que serán válidas en los juzgados
- Estricta adherencia a los estándares electrónicos de protección y seguridad de la HIPAA
- Estándares de documentación detallados que incluyen la verificación de fuente e identidad, claves de encriptado, algoritmos hash para bloquear documentos y demás tecnología de firma que apoye el cumplimiento
- Auditoría minuciosa que rastrea el movimiento y la firma de cada documento

21 CFR PARTE 11 (CIENCIAS DE LA VIDA)

Para quienes se adhieren al cumplimiento con 21 CFR Parte 11 de la FDA, Foxit eSign soporta el cumplimiento con esta regulación al adherirse al código de regulaciones establecido por la FDA para el uso de firmas electrónicas y al proporcionar las características y herramientas necesarias para cumplir con los requerimientos. La identidad del firmante se verifica al momento de la firma y cada inicial al proveer la contraseña de inicio de sesión como mínimo después de las verificaciones de identidad iniciales al acceder el documento para la firma. Una vez que los receptores firman el documento, este se almacena en forma electrónica con un certificado de

finalización que contiene la imagen de la firma, las etiquetas de hora y fecha de los eventos clave y la dirección IP del firmante.

Foxit eSign cumple con 21 CFR Parte 11 a través de lo siguiente:

- Métodos de verificación de identidad
- Pistas de auditoría detalladas
- Protección contra alteración de documentos, evidencia de alteración
- Etiquetas de hora y fecha
- Se proporciona un certificado de finalización para los documentos firmados

FERPA (EDUCACIÓN)

Foxit eSign facilita a los educadores y administradores el proceso de cumplir con los requerimientos de la FERPA, al mantener los datos protegidos y accesibles en forma segura para adaptarse a los requerimientos de 45 días y cumplir con las solicitudes de los registros. Además, Foxit eSign soporta el cumplimiento de la FERPA mediante lo siguiente:

- Al proveer una forma electrónica para que los estudiantes firmen los formularios de liberación requeridos por la FERPA, que mantienen la seguridad e integridad de los registros mediante características a prueba de alteraciones y que hacen evidentes las alteraciones
- Al proveer a las escuelas una forma fácil y segura de recolectar permisos firmados de los estudiantes y padres para liberar los registros estudiantiles
- Al proveer soluciones legalmente vinculantes que cumplan con ESIGN y UETA
- Mediante características de auditoría detalladas, certificados de finalización de firmas y claves de firma digitales que permitan a las escuelas evitar firmas fraudulentas y asegurar una validez de manera efectiva, al tiempo que cumplan con los requerimientos de la FERPA para validar firmas electrónicas
- Foxit eSign proporciona campos protegidos para enmascarar la información de identificación personal (PII) y usa el encriptado y la tokenización para evitar fugas de datos de PII
- Todos los datos se encriptan almacenados y en tránsito

FINRA (FINANZAS)

Foxit eSign admite el cumplimiento con la FINRA Regla 4512, incluida la Enmienda de aviso regulatorio 19-13 de la FINRA 2019, y los requerimientos de retención de documentos de la Regla 17a-4(f), lo que significa que puede asegurar que el envío y la firma de su documento siempre cumplirá con las regulaciones industriales. Foxit eSign admite el cumplimiento de la FINRA mediante lo siguiente:

- Al proveer soluciones legalmente vinculantes reconocidas por los principales bancos, que sean compatibles con ESIGN y UETA
- Mediante la emisión de firmas digitales a prueba de alteraciones y que hagan evidentes las manipulaciones mediante el encriptado de 256 bits, el cual asegura que, si se intenta alterar un documento, habrá una prueba registrada
- A través de una estricta auditoría de SOC 2 Tipo 2 y del cumplimiento y la estricta adherencia a los 5 principios de servicio de confianza, según lo desarrollado por la AICPA
- Al proveer una auditoría minuciosa y detallada que muestre todas las acciones realizadas por los emisores y firmantes, incluidas fechas, horas y ubicaciones
- Al proveer un certificado detallado de finalización, el cual se incluye en todos los documentos
- Mediante opciones de métodos de verificación de identidad, como la autenticación de dos factores (2FA) y la autenticación basada en el conocimiento (KBA)
- Al permitir que los usuarios guarden y descarguen el documento firmado completo para la retención de su registro

PCI DSS

La Norma de seguridad de los datos de la industria de tarjetas de pago (PCI DSS) es una norma de seguridad de información para organizaciones que manipulan tarjetas de crédito de marca de los principales esquemas de tarjetas, para incrementar los controles en torno a la gestión de datos del tarjetahabiente y reducir el fraude. Foxit eSign mantiene el cumplimiento con PCI DSS 3.2.1; cumple y excede los requerimientos para salvaguardar la manipulación de los datos de los poseedores de tarjetas de crédito. Además, Foxit eSign se prueba de manera regular contra riesgos de seguridad de nivel superior, incluidos los que se encuentran en la lista OWASP Top 10.

© Foxit Software Incorporated. Todos los derechos reservados.