FOXIT ESIGN: PANORAMICA SULLA CONFORMITÀ

Alcune organizzazioni sono soggette a una serie di requisiti normativi specifici, e Foxit eSign può fungere da componente essenziale per soddisfare gli obblighi di conformità. Questo documento illustra varie normative, sia per regione sia per settore, per le quali Foxit eSign supporta la conformità.

WHITEPAPER

SOMMARIO

Per regione 3

Stati Uniti 3

California Consumer Privacy Act (CCPA) 3

Unione Europea 4

GDPR 4

Per settore 6

HIPAA (Sanità) 6

21 CFR Parte 11 (Scienze biologiche) 6

FERPA (Istruzione) 7

FINRA (Finanza) 8

PCI DSS 8

PER REGIONE

STATI UNITI

Foxit eSign è compatibile al 100% con tutte le normative sulla conformità U.S. ESIGN Act e UETA e fornisce strumenti importanti per garantire che i documenti siano legalmente vincolanti.

- Registri di associazione e attribuzione di firma (audit trail) chiari
- Criteri definiti di conservazione dei documenti
- Certificato di compilazione fornito per ciascun documento firmato
- Facili metodi per gli utenti per dimostrare il chiaro intento di firmare ed effettuare business in formato elettronico

È importante tenere presente che mentre il software Foxit eSign può aiutare nella conformità con le leggi ESIGN e UETA, potrebbe non essere sufficiente per i tuoi requisiti locali, statali, dei mercati internazionali o industriali. Verifica sempre le linee guida corrispondenti.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Foxit eSign è conforme al California Consumer Privacy Act (CCPA) definito dallo stato della California e riguardante il diritto di conoscere, il diritto di accesso, il diritto di eliminare, il diritto di rifiutare esplicitamente e il diritto di non discriminazione delle informazioni personali, relativi al consumatore e in riferimento a qualsiasi azienda che svolga attività di business e trasferisce dati per i consumatori della California.

Foxit eSign ha certificato di aderire strettamente al CCPA in relazione a tali dati. Invieremo una notifica al cliente per qualsiasi richiesta dei relativi clienti e lavoreremo per intraprendere le azioni necessarie nel rispetto della legge e in base al consenso del cliente come richiesto.

UNIONE EUROPEA

Facciamo rispettare rigorosamente il Regolamento europeo per l'identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (Electronic Identification, Authentication, and Trust Services, eIDAS) come stabilito dai regolamenti UE per le transazioni nel Mercato europeo comune.

La normativa eIDAS n. 910/2014 definisce tre livelli principali di firma elettronica: Conformità di base, firme digitali avanzate (AES) e firme digitali avanzate qualificate (QES o QAES).

Conformità di base: le firme che rientrano in questo livello consistono in genere di caselle di controllo o nella digitazione del nome e non richiedono ulteriori protocolli tecnologici.

Firme digitali avanzate (AES): con le firme digitali di livello avanzato, la firma del firmatario è collegata direttamente al documento, tutte le modifiche sono monitorate e documentate, e viene utilizzato un processo di certificazione digitale per convalidare la firma.

Firme digitali avanzate qualificate (QES o QAES): questo rappresenta il livello di firma elettronica più alto e qualificato. Questo livello garantisce una chiave di firma privata, assicura che i dati usati nella creazione della firma possano essere utilizzati una sola volta, protegge da contraffazione e consente al firmatario di mantenere pieno controllo del processo di firma. Le firme qualificate non possono essere alterate, duplicate o riprodotte e rimangono sotto la supervisione di un fornitore di servizi di attendibilità qualificato.

Foxit eSign è conforme ai requisiti definiti da firma elettronica avanzata (AES) e la firma elettronica qualificata (QES).*

*Foxit eSign offre QES mediante ZealiD. ZealiD aderisce a una strategia di sicurezza dei dati basata su servizi di attendibilità certificati eIDAS, su standard ETSI designati eIDAS e su regolamenti di identificazione a distanza all'avanguardia dell'UE.

GDPR

In qualità di cliente Foxit eSign, usufruisci dei seguenti diritti definiti dalla legge sul GDPR e protetti da Foxit eSign:

- Il diritto di richiedere la conferma del trattamento dei tuoi dati personali.
- Il diritto alla correzione di dati imprecisi e il completamento di dati personali incompleti.
- In alcune circostanze, il diritto all'eliminazione dei tuoi dati personali senza ritardi

ingiustificati.

- In alcune circostanze, il diritto a limitare il trattamento dei tuoi dati personali.
- Il diritto di opporti al nostro trattamento dei tuoi dati personali per motivi legati alla tua situazione particolare, ma solo nella misura in cui la base giuridica del trattamento è che tale trattamento è necessario per: l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di qualsiasi autorità ufficiale a noi conferita; o gli scopi dei legittimi interessi perseguiti da noi o da un terzo.
- Il diritto di opporti al trattamento dei tuoi dati personali per scopi di marketing diretto.
- Il diritto di opporti al trattamento dei tuoi dati personali per scopi di ricerca scientifici o storici oppure per scopi statistici su basi correlate alla tua particolare situazione a meno che tale trattamento non sia necessaria per l'esecuzione di un'attività eseguita nel pubblico interesse.

Foxit eSign offre le seguenti funzioni per aiutare i clienti a conformarsi con il GDPR:

Accesso[1]: alla maggior parte delle informazioni personali relative a un Utente o a un Firmatario, il soggetto stesso può accedervi direttamente tramite l'interfaccia utente di Foxit eSign e tramite la parte autorizzata dell'organizzazione che ha richiesto le informazioni durante la firma dei documenti.

Correzione: tutte le informazioni personali raccolte sugli utenti o sui firmatari sono disponibili attraverso l'interfaccia utente. Se è necessario effettuare modifiche, l'utente e il firmatario possono effettuare modifiche dirette durante la firma del documento. Le modifiche possono essere apportate dal firmatario dopo la firma di qualsiasi documento, richiedendo al Firmatario autorizzato una revisione o un aggiornamento dei propri registri o l'avvio di un'altra richiesta di firma.

Eliminazione: sono previste diverse azioni a seconda del ruolo dell'utente nell'evento di firma. Un Utente che invia un contratto deve inviare la richiesta di eliminazione all'azienda presso cui è dipendente. Foxit eSign non controlla i dati che il datore di lavoro ha raccolto durante la transazione. Il processo di firma raccoglie le seguenti informazioni relative a un firmatario durante un evento di firma: nome e cognome, indirizzo e-mail e indirizzo IP. Queste informazioni sono archiviate con il contratto assieme alla firma e sono controllate dall'azienda che ha inviato il contratto. Se un Firmatario necessita di informazioni che riguardano le informazioni personali raccolte con il contratto, dovrà contattare il Mittente del contratto. Foxit eSign non può fornire informazioni al Firmatario relative al contratto o all'azienda che gli ha inviato il contratto. Se il firmatario pensa che non ci sia cooperazione dalla parte del mittente, Foxit eSign può contattare il Mittente a nome del firmatario e chiedere l'eliminazione, ma il Mittente deve condividere la prova che i tentativi verso il Mittente non sono andati a buon fine.

---

[1] Foxit eSign mantiene data center attendibili negli Stati Uniti e in Europa con strutture SSAE16 conformi a SOC 2 Type 2 e a PCI. Negli Stati Uniti, i data center sono situati in Virginia del Nord (USA orientali), Ohio (USA orientali) e Nord California (USA occidentali). In Europa, i data center si trovano a Francoforte, in Germania.

PER SETTORE

HIPAA (SANITÀ)

Foxit eSign è conforme alla certificazione HIPAA e può garantire che la tua documentazione privata e riservata e quella del tuo paziente siano sempre a norma. Per mantenere informazioni personali che consentono l'identificazione (PII), Foxit eSign fornisce campi sicuri per mascherare tali informazioni. Utilizziamo crittografia e token per impedire perdite di dati PII. Tutti i dati sono crittografati sia in archiviazione sia in movimento. Ciascuna transazione con firma Foxit eSign contiene audit trail a prova di contraffazione e pienamente tracciabili, ottenendo inoltre un Certificato di compilazione.

I documenti archiviati nei nostri data center controllati SOC2 sono crittografati con lo standard AES 256 a livello di applicazione in modo da assicurare una piena riservatezza ai documenti del cliente.

Foxit eSign offre contratti di società in affari (BAA) in base ai piani Pro ed Enterprise.

In aggiunta, Foxit eSign è conforme alle normative HIPAA nei modi seguenti:

- firme digitali legalmente vincolanti (in accordo con UETA ed ESIGN) ritenute ammissibili nei tribunali
- Rigoroso rispetto degli standard di protezione e sicurezza elettronica HIPAA
- Standard di documentazione dettagliati che includono verifica di origine e identità, chiavi di crittografia, algoritmi di hash per bloccare i documenti, e altra tecnologia di firma che supporta la conformità
- Auditing approfondito che traccia il movimento e la firma di ciascun documento

21 CFR PARTE 11 (SCIENZE BIOLOGICHE)

Per coloro che aderiscono alla conformità allo standard 21 CFR Parte 11 della FDA, Foxit eSign supporta la conformità con questa normativa rispettando il codice delle normative definito dalla FDA per l'utilizzo della firma elettronica e fornendo le funzioni e gli strumenti necessari per rispettarne i requisiti. L'identità del firmatario viene verificata al momento della firma e di ciascuna iniziale fornendo la password di accesso come minimo dopo le verifiche dell'identità iniziali durante l'accesso al documento per la firma. Una volta che i destinatari hanno firmato il documento, questo verrà archiviato in formato elettronico assieme a un certificato di compilazione contenente l'immagine della firma, i timestamp degli eventi importanti e l'indirizzo IP del firmatario.

Foxit eSign è conforme allo standard 21 CFR Parte 11 nei modi seguenti:

- Metodi di verifica dell'identità
- Audit trail dettagliati
- Protezione da contraffazione dei documenti, prova di contraffazione
- Timestamp
- Certificato di compilazione fornito per i documenti firmati

FERPA (ISTRUZIONE)

Foxit eSign facilita a educatori e amministratori la conformità con i requisiti FERPA mantenendo i dati protetti e accessibili in modo sicuro, allo scopo di garantire i requisiti di 45 giorni nel rispetto delle richieste dei registri. In aggiunta, Foxit eSign supporta la conformità con lo standard FERPA nei modi seguenti:

- Fornendo una modalità elettronica agli studenti per la firma dei moduli di rilascio richiesti dallo standard FERPA, la quale mantiene la sicurezza e l'integrità dei registri attraverso funzioni a prova di contraffazione e che offrono evidenza di eventuali manomissioni
- Fornendo alle scuole una modalità sicura e semplice di raccogliere autorizzazioni firmate da studenti e genitori per rilasciare i registri degli studenti
- Fornendo soluzioni legalmente vincolanti compatibili con ESIGN e UETA
- Tramite funzioni di auditing dettagliate, certificati di compilazione delle firme e chiavi di firma digitali che consentono alle scuole di impedire firme fraudolente, oltre che assicurare la validità in modo efficace soddisfacendo nel contempo i requisiti FERPA per convalidare le firme digitali
- Foxit eSign offre campi sicuri per mascherare informazioni personali che consentono l'identificazione (PII) e utilizza crittografia e token per impedire perdite di dati PII
- Tutti i dati sono crittografati sia in archiviazione che in movimento

FINRA (FINANZA)

Foxit eSign supporta la conformità con lo standard FINRA Regola 4512, incluso l'Emendamento di avviso normativo 19-13 FINRA 2019 e i requisiti di mantenimento dei documenti della Regola 17a-4(f), il che significa che puoi essere certo che l'invio e la firma del tuo documento siano sempre compatibili con le normative industriali. Foxit eSign supporta la conformità con lo standard FINRA nei modi seguenti:

- Fornendo soluzioni legalmente vincolanti, riconosciute da tutte le principali banche, compatibili con ESIGN e UETA
- Attraverso l'emissione di firme digitali a prova di contraffazione e che offrono evidenza di eventuali manomissioni, con crittografia a 256 bit che assicura una prova registrata nel caso in cui ci sia un qualsiasi tentativo di alterare un documento
- Attraverso rigorosi auditing e conformità con lo standard SOC 2 Type 2, nonché un rigoroso rispetto dei 5 Trust Service Principles sviluppati da AICPA
- Fornendo un auditing completo e dettagliato che visualizza tutte le azioni intraprese da mittenti e firmatari, incluso date, ore e località
- Fornendo un dettagliato certificato di compilazione disponibile per tutti i documenti
- Attraverso l'offerta di opzioni del metodo di verifica dell'identità, quali l'autenticazione a due fattori (2FA) e l'autenticazione basata sulla conoscenza (KBA)
- Consentendo agli utenti di salvare e scaricare il documento firmato compilato per conservarlo nei registri

PCI DSS

Il Payment Card Industry Data Security Standard (PCI DSS) è uno standard di sicurezza delle informazioni per le organizzazioni che gestiscono carte di credito delle marche dei principali circuiti di pagamento, allo scopo di aumentare i controlli relativi alla gestione dei dati del possessore della carta e ridurre le frodi. Foxit eSign mantiene la conformità con lo standard PCI DSS 3.2.1, rispettando e superando i requisiti allo scopo di proteggere la gestione dei dati del possessore della carta di credito. In aggiunta, Foxit eSign viene regolarmente testato nei riguardi dei rischi di sicurezza di alto livello, inclusi quelli presenti nella top 10 di OWASP.

© Foxit Software Incorporated. Tutti i diritti riservati.