FOXIT ESIGN COMPLIANCE OVERVIEW

Some organizations are subject to a range of specific regulatory requirements, and Foxit eSign can serve as a key component for meeting your compliance obligations. This document outlines various regulations, both by region and industry, which Foxit eSign supports compliance with.

WHITE PAPER

TABLE OF CONTENTS

BY REGION

UNITED STATES

Foxit eSign is 100% compliant with all U.S. ESIGN Act and UETA compliance regulations and provides you with important tools to help ensure your documents are legally binding.

- Clear signature association records and signature attribution (audit trails)
- Defined document retention policy
- Certificate of completion provided for each signed document
- Easy methods for users to demonstrate clear intent to sign and conduct business electronically

It's important to keep in mind that while Foxit eSign software can help you comply with ESIGN and UETA laws, it may not be enough for your local, state, international markets, or industry requirements. Always check corresponding guidelines.

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

Foxit eSign complies with the California Consumer Privacy Act (CCPA) as set forth by the state of California regarding the consumer's right to know, right to access, right to delete, right to opt out, right to non-discrimination of their personal information from any companies conducting business, and transfers data for California consumers.

Foxit eSign has certified that it strictly adheres to the CCPA with respect to such data. We will notify the customer of any request from their clients and will make provisions to take the necessary action as per law upon customer consent as required.

EUROPEAN UNION

We enforce strict compliance with the Electronic Identification, Authentication, and Trust Services (eIDAS) as set forth by EU regulations for transactions in the European Single Market.

The eIDAS regulation No. 910/2014) defines three primary levels of e-signatures: Basic Compliance, Advanced Electronic Signatures (AES), and Qualified Advanced Electronic Signatures (QES or QAES).

Basic Compliance: Signatures that fall into this level usually consist of checkboxes or typing your name and do not require any further technological protocols.

Advanced Electronic Signatures (AES): With advanced-level electronic signatures, the signer's signature is tied directly to the document, all changes are monitored and documented, and a digital certification process is used to validate the signature.

Qualified Advanced Electronic Signatures (QES or QAES): This is the highest and most qualified electronic signatures level. This level guarantees a private signing key, ensures data used in signature creation can only be used once, protects against forgery, and allows the signee to retain full control of the signature process. Qualified signatures cannot be altered, duplicated, or reproduced and remain under the supervision of a qualified trust provider.

Foxit eSign conforms to the prerequisites set by Advanced Electronic Signatures (AES) and Qualified Electronic Signatures (QES).*

*Foxit eSign offers QES via ZealiD. ZealiD adheres to a data security strategy based on eIDAS certified trust services, eIDAS designated ETSI standards, and cutting-edge EU distant identification regulations.

GDPR

As a Foxit eSign customer, you have the following rights as set forth by GDPR law and protected by Foxit eSign:

- The right to confirm the processing of your personal data.
- The right to have inaccurate data corrected and incomplete personal data completed.
- In some circumstances, the right to the erasure of your personal data without undue delay.
- In some circumstances, the right to restrict the processing of your personal data.

- The right to object to our processing of your personal data on grounds relating to your particular situation, but only to the extent that the legal basis for the processing is that the processing is necessary for: the performance of a task carried out in the public interest or in the exercise of any official authority vested in us; or the purposes of the legitimate interests pursued by us or by a third party.
- The right to object to our processing of your personal data for direct marketing purposes.
- The right to object to our processing of your personal data for scientific or historical research purposes or statistical purposes on grounds relating to your particular situation unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Foxit eSign offers the following features to help customers comply with GDPR:

Access[1] – Most personal information about a User or a Signer can be accessed directly by that individual through Foxit eSign's user interface and by the authorized party from the organization who requested information while signing documents.

Correction – All of the personal information that is collected on users or signers is available through the user interface. If changes need to be made, the user and signer can make direct changes while signing the document. Changes can be initiated by the signer after signing any document by requesting the authorized Sender for a review/update on their records or reinitiating another signature request.

Deletion – There are different actions depending on the role of the user in the signing event. A User that sends the agreement must make the deletion request to the company they are employed by. Foxit eSign does not control the data the employer has collected during the transaction. The signing process collects the following information about a signer during the signing event: name, e-mail address, and IP address. This information is stored with the agreement with their signature and is controlled by the company that sent the agreement. If a Signer needs information that pertains to the personal information collected with that agreement, they need to contact the Sender of the agreement. Foxit eSign cannot provide any information to the Signer about the agreement or the company that sent them the agreement. If the signer feels that there is no cooperation from the sending party, Foxit eSign can contact the Sender on the signer's behalf and facilitate deletion, but the Sender must share proof that attempts to Sender have not been successful.

[1] Foxit eSign maintains trusted US and European data centers with SSAE16 facilities that are SOC 2 Type 2 compliant and PCI compliant. In the United States, data centers are located in N. Virginia (US East), Ohio (US East), and Northern California (US West). In Europe, data centers are located in Frankfurt, Germany.

BY INDUSTRY

HIPAA (HEALTHCARE)

Foxit eSign is certified HIPAA compliant and can help ensure you and your patient's private and sensitive documentation are always within regulation. To maintain personally identifiable information (PII), Foxit eSign provides secure fields to mask this information. We use encryption and tokenization to prevent PII data leaks. All data is encrypted at rest and in motion. Each Foxit eSign Signature transaction contains a fully traceable, tamper-proof audit trail and is given a Certificate of Completion.

Documents stored in our SOC2 audited data centers are encrypted with the AES 256 standard at the application level for customer documents to ensure full confidentiality.

Foxit eSign offers Business Associate Agreements (BAA) under Pro and Enterprise plans.

Additionally, Foxit eSign complies with HIPAA regulations through the following:

- Legally binding electronic signatures (in accordance with UETA and ESIGN) that will hold up in court
- Strict adherence to HIPAA electronic safety and security standards
- Detailed documentation standards that include source and identity verification, encryption keys, hash algorithms to lock documents, and other signature technology that supports compliance
- Thorough auditing that tracks each document's movement and signing

21 CFR PART 11 (LIFE SCIENCES)

For those who adhere to the FDA's 21 CFR Part 11 compliance, Foxit eSign supports compliance with this regulation by adhering to the code of regulations established by the FDA for electronic signature usage and by providing the features and tools needed to meet requirements. The signer's identity is verified at the time of signature and each initial by providing the login password at a minimum after initial identity checks while accessing the document for signing. Once recipients have signed the document, it is then stored electronically with a certificate of completion containing the signature image, key event timestamps and the signer's IP address.

Foxit eSign complies with 21 CFR Part 11 through the following:

- Identity verification methods
- Detailed audit trails
- Document tampering protection, tamper evidence
- Timestamps
- Certificate of completion provided for signed documents

FERPA (EDUCATION)

Foxit eSign makes it easy for educators and administrators to comply with FERPA requirements by keeping data safe and securely accessible to accommodate 45-day requirements for satisfying records requests. Additionally, Foxit eSign supports FERPA compliance with the following:

- By providing an electronic way for students to sign FERPA required release forms that maintain the security and integrity of the records through tamper-proof and tamper-evident features
- By providing schools a secure and easy way to collect signed permissions from students and parents to release student records
- By providing legally binding solutions that are compliant with ESIGN and UETA
- Through detailed auditing features, signature completion certificates, and digital signing keys that allow schools to prevent fraudulent signing and ensure validity effectively while meeting FERPA requirements to validate electronic signatures
- Foxit eSign provides secure fields to mask personally identifiable information (PII) and uses encryption and tokenization to prevent PII data leaks
- All data is encrypted at rest and in motion

FINRA (FINANCE)

Foxit eSign supports compliance with FINRA Rule 4512, including FINRA 2019 Regulatory Notice Amendment 19-13 and document retention requirements of Rule 17a-4(f), meaning you can ensure your document sending and signing is always compliant with industry regulations. Foxit eSign supports FINRA Compliance with the following:

- By providing legally binding solutions recognized by all major banks that are compliant with ESIGN and UETA
- Through the issuing of tamper-proof and tamper-evident digital signatures with 256-bit encryption that ensures if any attempt is made to alter a document, there is recorded proof
- Through Stringent SOC 2 Type 2 auditing and compliance and strict adherence to the 5 Trust Service Principles as developed by the AICPA
- By providing thorough and detailed auditing that displays all actions taken by senders and signers, including dates, times, and locations
- By providing a detailed certificate of completion provided for all documents
- Through providing identity verification method options, such as two-factor authentication (2FA) and knowledge-based authentication (KBA)
- By allowing users to save and download the completed signed document for their record retention

PCI DSS

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes to increase controls around cardholder data management and reduce fraud. Foxit eSign maintains compliance with PCI DSS 3.2.1, meeting and exceeding the requirements to safeguard the handling of credit card holder data. In addition, Foxit eSign is tested regularly against top-level security risks, including those found in the OWASP Top 10.