E-Signature Guideline

At Beneva, we pride ourselves on our high standards of document compliance. We regularly review all internal procedures in order to simplify your business with us and ensure the legal security of all parties involved.

This level of compliance is to provide maximum security and minimize litigation and non-compliance risks, both for us and for our distribution networks. In essence, our document compliance guideline is in place to protect our clients, our brokers, our MGA partners and Beneva.

The electronic signature solutions listed below have been reviewed and approved by Beneva, provided they are used correctly. Note that a number of these solutions comprise settings that could have an impact on a document's compliance and signatures. Accordingly, use of one of these solutions alone does not guarantee acceptance of the document by Beneva.

Solutions

- Adobe Sign
- Authentisign
- DocHub
- DocuSign
- Dropbox Sign
- eSign
- eZsign
- Formstack Sign
- Foxit eSign
- iGeny
- Notarius
- OneSpan
- Zoho

Please note that use of an electronic signature platform that does not meet our security criteria may result in rejection of the document.

When Beneva examines the compliance of any electronic signature, we look at the following aspects:

Authenticity

Is the signature authentic? How can we demonstrate that the document was really signed by the signatory?

By demonstrating that no one other than the client could have signed the document, such as with the email address provided by the client on the form or through SMS-based two-factor authentication.

Document integrity and document locking

Has the document been altered either between signature(s) or after it has been signed? Can the document be altered after it was signed? Has the format of the document been altered?

This can be checked when the electronic signature solution affixes a security seal to the document following receipt of all the signatures.

Proof of authenticity and integrity

Does the electronically signed document come with all the metadata (IP address, time stamp and identification information) that is required should we need to prove the authenticity of the signatures or the integrity of the documents? Has the metadata been altered? Should a separate evidence document showing the metadata accompany the document?

Security

Does the electronic signature solution ensure information security? Verify that the eSignature platform uses strong encryption of data in transit and at rest and stores data within an encrypted database volume to ensure an encrypted channel for all communications.

We will be updating and improving our corporate eSignature guideline as well as this document, so be sure to refer back to it regularly. Thank you for your partnership and continued support.

For more information, read The Ultimate eSignature Security Checklist.

Beneva Management Team