



## The Legality of Electronic Signatures

### What you should know about E-Signature Law

The adoption of the Uniform Electronic Transactions Act (UETA) in most states and the passage of Electronic Signatures in Global and National Commerce Act (ESIGN) at the federal level in 2000 solidified the legal landscape for use of electronic records and electronic signatures in commerce.

#### Rule of General Validity

Both ESIGN and UETA establish that electronic records and signatures carry the same weight and legal effect as traditional paper documents and handwritten signatures, stating:

A document or signature cannot be denied legal effect or enforceability solely because it is in electronic form.

#### Intent to Sign

The electronic signature laws retain the rule that a signature is only valid if the signer intends to sign.

#### Signature Associated with the Record

In order to qualify as an electronic signature under ESIGN and UETA, the system that is used to capture the electronic transaction must either

(a) keep an associated record reflecting the process by which the signature was created or

(b) make a textual or graphic statement that is added to the signed record, reflecting the fact that it was executed with an electronic signature.

#### Consent to Do Business Electronically

Between businesses, the nature of the parties' consent to do business electronically can be established explicitly or by implication based on the parties' interactions.

However, consumers receive special protection under ESIGN and some state UETA enactments. Electronic records may be used to deliver Required Information to consumers only if the consumer

(a) receives certain disclosures (UETA Consumer Consent Disclosures);

(b) has affirmatively consented to use electronic records for the transaction; and

(c) has not withdrawn such consent.

#### Record Retention

UETA provides that legal effect, enforceability or validity requires that electronic signature records be:

(a) capable of being retained; and

(b) capable of being accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

## The Legality of Electronic Signatures

Contracts signed using enterprise-level electronic signature processes like DocuSign are completely secure and deliver a rigorous audit trail of who signed and when. This court-admissible audit trail includes the core elements required to successfully enforce and defend a contract.

## Beyond ESIGN – Best Practices

Compliance with the e-signature laws is a very basic step in selecting a system for electronic signature transactions. Like their paper counterparts, electronically signed documents can become the subject of a dispute.

In the event of a dispute regarding an electronically executed contract, merely complying with ESIGN is not enough. The signature process must provide enough proof to uphold the transaction.

Our comprehensive approach includes:

- Audit trail tracks all signer actions
- Secure encryption so documents can be read and signed only by designated users
- Unique Signatures created by each user, accessible only to that user, and stored securely online
- Sign Document Blocks so users can ‘initial’ and ‘sign’ specific areas of a document
- User Authentication leveraging email, access code, and/or third party ID check
- Time-Stamping of every step in the document process  
Transaction Summary provides complete document history

### Intent to Sign

A key convention in the paper world, precise signature placement is important criteria in establishing the signer’s intent. Similar considerations should be made when adopting an electronic signature process.

### Record Retention

Few organizations fine the requirements for record retention under UETA and ESIGN strict enough in comparison to their standards for mitigating risk. Most notably, the storage systems associated with any electronic signature system must be rigorously secure from a physical and technological standpoint.

### Admissibility into Evidence

The Federal Rules of Evidence and the Uniform Rules of Evidence generally allow for electronic records and their reproductions to be admissible into evidence.

This applies to electronic signatures stored in a computer or server, so that any printout or output readable by sight, shown to reflect the data accurately, is considered an original. In the case of an electronic signature, then, it is important to demonstrate to the satisfaction of the courts that:

- (a) the appropriate level and amount of information surrounding the signing process was retained, and
- (b) the system used to retain the information is itself reliable.

## About DocuSign

DocuSign, Inc. is the leading provider of on-demand software services for electronic signature. DocuSign empowers individuals, small business and global enterprises to operate faster and more efficiently with greater profitability, enhanced security and compliance. DocuSign is the only Web-based service to securely automate and control the entire electronic document signing process. To learn more, call 866.219.4318, email [sales@docusign.com](mailto:sales@docusign.com) or visit our Website at [www.docusign.com](http://www.docusign.com).

This white paper is for informational purposes only. DOCUSIGN MAKES NO REPRESENTATIONS or WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, AS TO THE INFORMATION IN THIS DOCUMENT.

©2009 DocuSign, Inc. Allrights reserved. DocuSign may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document.

Except as expressly provided in any written license agreement from DocuSign, the furnishing of this document does not give you any license or other rights to these patents, trademarks, copyrights, or other intellectual property.

DocuSign Inc.  
701 Fifth Avenue, Suite 4500  
Seattle, Washington 98104  
U.S.A.

Tel 866.219.4318  
Fax 206.622.0736  
[www.docusign.com](http://www.docusign.com)  
[sales@docusign.com](mailto:sales@docusign.com)