



## What You Should Know about E-Signature Law

These days international borders are becoming less and less of a hurdle to conducting business. Particularly in industrialized countries, the law recognizes that business accelerators such as electronic signatures are essential to remaining competitive in the global economy. An understanding of the law regarding electronic signatures in the European Union and DocuSign's strong adherence to these laws, as follows, provides businesses with the confidence to conduct business and get signatures electronically anywhere in the world.

The adoption of the European Directive 1999/93/EC of 13 December 1999 establishes a Community framework for the use of electronic signatures on electronic contracts in the EU. Thirty European countries (EU-27, Croatia, Turkey and Liechtenstein) have already implemented the Directive 1999/93/EC. Electronic signatures are actively in use in Europe, and worldwide, and DocuSign's **advanced signature** is ready and legal to accelerate the speed of business.

### Summary of EU Directive 1999/93/EC

First, let's dive into the detail of European laws surrounding electronic signatures.

### Electronic Signature Definitions

Laying the groundwork for the legality of electronic signatures, the Directive provides three important definitions:

- The **"electronic signature"** is simply data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication.
- The **"advanced electronic signature"** defines a process that does not describe a particular technology, but rather a process that creates an enforceable electronic signature if the signature:
  - is uniquely linked to the signatory;
  - is capable of identifying the signatory;
  - is created using means that the signatory can maintain under their sole control;
  - is linked to the data to which it relates in such a manner that any subsequent change in the data is detectable.
- The **"qualified certificate"** defines a process which must in particular include specific technology:
  - an indication that it is issued as a qualified certificate;
  - the identification of the certification service provider;
  - the name of the signatory;
  - provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;
  - signature-verification data corresponding to signature-creation data under the control of the signatory;
  - an indication of the beginning and end of the period of validity of the certificate;
  - the identity code of the certificate;
  - the advanced electronic signature of the issuing certification service provider.



## Same Legal Effect as Pen and Paper Signatures

Using these definitions, the Directive goes on to establish the criteria that form the basis for legal recognition of electronic signatures to carry the same weight and legal effect as a traditional paper document with a pen and ink signature. It ensures that no matter what form of electronic signature is used, the electronic signature will be valid—as long as a recognized process is followed.

An electronic signature may **not** legally be refused simply because:

- it is in electronic form;
- it is not based on a qualified certificate;
- it is not based upon a qualified certificate issued by an accredited certification service provider;
- it is not created by a secure signature-creation device.

## Making Sense of the Definitions

An **advanced signature** is generally taken to be a specific type of **electronic signature** that meets an additional set of criteria for signer identification. The main purpose of an advanced electronic signature is **authentication**, i.e. to give added assurance that the individual signing the message really is the person that he or she claims to be. Ostensibly, any electronic signature mechanism that captures the signer's intent to adopt the signature and his affixing that signature to a record would meet this requirement if the record is at some point provisioned with a tamper-evident seal.

A **qualified certificate** is not an electronic signature per se; it is a technical mechanism for establishing the source of an electronic message. When affixed or associated with an advanced electronic signature, the combination of the two is given an elevated status and becomes the "functional equivalent" of a handwritten signature. This has caused much confusion, because in many jurisdictions (common law countries in particular), there is no legal distinction between different "tiers" of signatures.

Court cases illustrate that courts will accept the use of electronic communication, including electronic signatures, as evidence, so they can constitute the basis of binding contracts.

Please note that even a simple **electronic signature** is recognized under the Directive as valid and enforceable. This aspect of the law, which closely resembles the United States federal E-SIGN law, is the governing principle behind the vast majority of electronic contracts currently executed in Europe. The Directive simply enables parties to an agreement to enhance the transaction with additional measures of security if desired.


## DocuSign's Support of the Advanced Electronic Signature

DocuSign has elected to support the Advanced Signature model, primarily because it affords a reasonable range of identification and authentication of the parties without requiring the added expense and inconvenience of obtaining a qualified certificate.

DocuSign Supports Advanced Electronic Signatures by:

### Uniquely identifying the signer

DocuSign provides the secure and auditable process for the signer to adopt their own electronic signature. Through email authentication, IP address and additional authentication methods the DocuSign service can uniquely link the signer to the electronic signature.

DocuSigned by:  
  
1D9F2F4F70954F4...

## Identifying the signer

DocuSign provides multiple levels of authentication that can identify the signer. This includes email address, IP address and additional authentication levels such as:

1. **Access Code** – A shared word or phrase that is given to the signer by the sender over the phone, which is needed to unlock the envelope before the signer can sign. The DocuSign Service will store this in the audit trail of the transaction. This is also known as “out of band” authentication.
2. **Phone Authentication** – The signer will be shown a code on their screen with a button that will dial their phone. They will be asked to key or say the number, as well as their name. The DocuSign service will store this in the audit trail of the transaction. This is known as “2 Factor, Biometric” Authentication.
3. **Portal Authentication** – Many of our customers have a portal that the signer must log into before they are able to sign the documents. DocuSign will accept this authentication and store this in the audit trail of the transaction.

## Assuring the Electronic Signature is under the signer’s sole control

The DocuSign Service allows the signer to create their electronic signature in a secure and auditable manner. After the signing process is completed, the signer can securely maintain their electronic signature by protecting their signature account with a password that they create and maintain under their sole control.

## Locking the signed document so that subsequent changes in the data is detectable

After the documents have been electronically signed, the DocuSign Service holds the documents in a tamper-proof state (using hashing and encryption) for the parties to retrieve at a later time. Each access to the documents is written to the audit trail. When any party to the transaction downloads the documents, the DocuSign Service will apply a Global Digital Certificate, which creates a tamper-evident seal around the documents.

## Electronic Signature Best Practices

In the event of a dispute regarding an electronically executed contract, merely complying with the EU Directive is not enough. Much like their paper counterparts, electronically signed documents can become the subject of a dispute. The signature *process* must provide enough proof to uphold the transaction. For this reason, compliance with the EU Directive is an important step in selecting an electronic signature platform.

### DocuSign’s comprehensive approach includes:

- Audit trail time/date stamps on all signer actions.
- Secure encryption so the document can be read and signed by only designated users.
- Unique Signatures created by each user, accessible only to that user, and stored securely online.
- Signature Areas (Stick-eTabs) are required so signers can initial and sign in specific parts of the document.
- Selectable user authentication methods to be commensurate with the transaction’s security requirements.

## Intent to Sign

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

## Signing Artifacts

Contracts signed using an enterprise-level electronic signature platform like DocuSign are completely secure and deliver a rigorous audit trail of who signed and when. We call it the Certificate of Completion. The Certificate of Completion and “digitally sealed” signed documents are key elements to successfully enforce and defend a contract.

## Admissibility into Evidence

EU countries generally allow for electronic records and their reproductions to be admissible into evidence. In the case of electronic signature, then, it is important to demonstrate to the satisfaction of the courts that:

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

By following the Directive and continually optimizing our solution based on legal developments, DocuSign is fully legal for electronic signature in 30 countries in Europe. Businesses can be confident in using DocuSign everywhere in the world, and DocuSign customers have sent out of more than 40 countries. That number is growing quickly, as more and more businesses trust DocuSign to make it easy to finish business fast worldwide.

## About DocuSign

DocuSign is the market leader and global standard for electronic signature. DocuSign provides the world's largest and fastest growing electronic signature platform that empowers businesses to complete transactions quickly and securely online while improving compliance and dramatically reducing processing costs. With more than 7 million unique signers processing millions of transactions per year, DocuSign is trusted by more people, more companies, more times than any other electronic signature vendor in the world.

Disclaimer: 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.