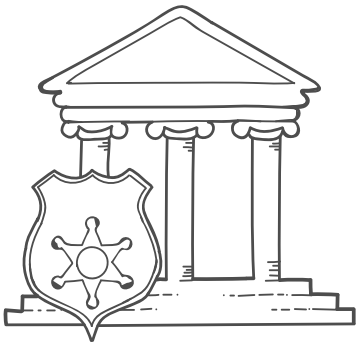
Signable

Electronic Signature
Legality Guide



Court legal? ✓

General Business use ✓

How do we ensure legal compliance?

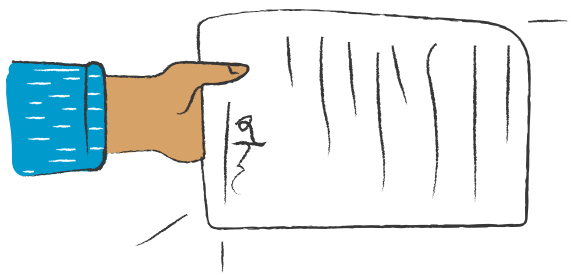
- eIDAS compliant (eu esignature law)
- UK eSign compliant
- Post-Brexit law information available
- Full Audit Trail
- IP address tracking
- Unique fingerprint per document
- Geotracking
- SSL 256-bit AES/RSA encryption
- Main infrastructure is hosted in the Amazon AWS

Breakdown of the law

Under UK law, a written signature is not necessarily required for a valid contract - contracts are generally valid if legally competent parties reach an agreement, whether they agree verbally, electronically or in a physical paper document.

To prove a valid contract, parties sometimes have to present evidence in court. Digital transaction management solutions can provide electronic records that are admissible in evidence under s7(1) Electronic Communications Act 2000 ("ECA 2000"), to support the existence, authenticity and valid acceptance of a contract.

A.K.A: An Audit Trail or legality certificate that Signable attaches to every document sent with us.



The eIDAS Regulation or trust services for electronic transactions regulation, came into effect on the 1st of July 2016. Meaning all eSignature providers have to comply with it for their contracts to be leagally binding. It applies to all 28 members of the EU.

Article 25(1) basically says that an electronic signature can't be denied as evidence in legal proceedings solely on the grounds that it's electronic.

Brexit law

Experts say the laws governing electronic signatures won't change drastically, and will likely be replicated by the government for the UK esignature legislation. They say there will likely be regulations for businesses that send contracts overseas and to the EU. We'll update you with more information as we find out - follow us on Twitter to be the first to know.

For more detailed Post-Brexit information see here: Brexit & Your Electronic Documents

Data Storage

All data stored and processed within Signable stays within the EU. We host the majority of our data in Amazon's AWS data centre in London, which is used by most of the top Internet companies. It's also fully compliant with all the major certifications.

More information on its compliance can be found here.
We also have backup facilities in Ireland which access is restricted to and is only used for data recovery or restoration. Our backups are taken every hour for both the database and the documents themselves.
Minimising the chance of any lost data.

Encryption

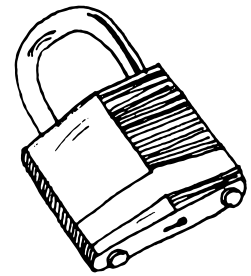
All data stored by Signable is encrypted at every point. Data shared between internal systems is also encrypted. In short wherever your information appears it's encrypted so no one can snoop.

Data access

Access to the data that we hold on behalf of our customers is tightly controlled and regulated by an auditable system and process.

Your data is never exposed to third parties and you fully control who is allowed to access your company data. What's more every action is logged and recorded.

Internally, members of the Signable team are unable to access the documents from within your account. If you do require support and assistance which relates to a specific document, you must first grant permission for us to access your documents. Until then, access is locked down and restricted.



Third party access

Your data, including names, address details and the documents itself are never exposed to third parties. Where third party contractors are used, we heavily vet and regulate them and if data is required for them perform their role, sample data is provided.

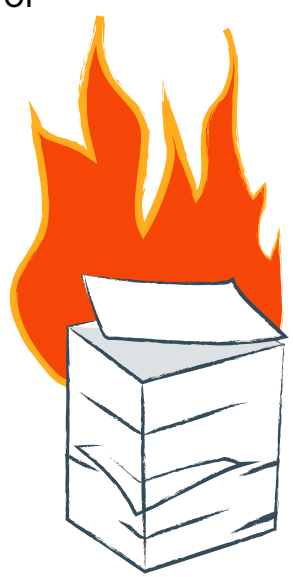
Disaster recovery
Depending on the type of disaster we have plans to handle the procedure when dealing with unexpected issues. All include the following:

- Prompt and effective communication to customers on the situation, communicated via Signable's status page
- Key people assigned as 'in charge' of coordinating the response and reaction.

- Effective gathering of data and logs required to determine the root cause to help diagnose the problem and work towards a solution.

- Feedback loops in place at every stage so learnings can be made for future events.

- For issues that affect the availability of the Signable service, we communicate them via our status page.
We have the ability to regenerate our whole infrastructure, within a different AWS region within a few minutes with backups taken from our backup facilities. (as mentioned in Data Storage)



Penetration testing
The Signable infrastructure is scanned on a daily basis against the OWASP top 10 security issues and any issues highlighted to the Signable development team. Our infrastructure is also scanned on a quarterly basis to comply with our PCI-DSS certification.

"End of business" plans
In the highly unlikely event that Signable is unable to continue trading, all previously signed documents will be provided in an archive file along with any information required to prove that the documents were signed legally and correctly.