Data Security of e-signatures

The security of your data is our top priority

How we ensure your data protection

ISO 27001

SignRequest is ISO 27001 certified. The ISO 27001 certification is a global standard for information security. With this certificate, SignRequest shows its commitment to information security. You can review our certificate and statement of applicability here.

GDPR

SignRequest supports compliance with GDPR. The General Data Protection Regulation is a regulation in EU law about data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas. Review our data processing agreement here.

Data Processing Activities

SignRequest uses Subprocessors to support its data processing activities in accordance with our Privacy Notice.

Third party due diligence

SignRequest has a responsible disclosure program through HackerOne, find out more about HackerOne on their website.

Digital signature security measures

Secure Socket layer

All communications with SignRequest use Secure Sockets Layer (SSL) 256 bit encrypted endpoints to ensure the security of your electronic signatures and e-signed documents.

Monitoring and alerting

Our application and underlying infrastructure components are monitored 24/7. Critical bugs are sent to our development team immediately, who are informed and available 24 hours a day, 7 days a week and 365 days a year. Monitor status

Storage

SignRequest infrastructure is hosted and stored on the highly available and robust architecture of Amazon Web Services (AWS).

SignRequest's digital certificate

All SignRequests are sealed with our digital certificate. The seal shows as a green checkmark when the completed document is opened in Adobe Acrobat. If the document is changed after signing, that seal is broken and it will show that the signature is invalid. Read more

Signing log

Every completed SignRequest is accompanied by a signing log. The signing log is uniquely linked to the signatory and the document with a hash code. Optionally, we can activate the use of signature stamps. These make it easier to link the signed document to the signing log thanks to a clearly visible document ID in the signed document. Read more

Hash codes

SignRequest creates hash codes of the signed document and the signing log. Hash codes are unique for each document. With the hash codes, the integrity of the e-signed document is ensured, because it is impossible to change the document without changing the hash code.Read more.