yousign.com

Technical & organisational measures

for data security and data protection

yousign

Introduction

Yousign is committed to protecting your data and respecting your privacy. We have put in place a variety of technical and organisational measures to **ensure the security of the personal data you provide to us**. These measures may change depending on the technical progress of and improvements to the Yousign solution. In this regard, Yousign may implement other appropriate measures.

Certifications & audits

As a trust service provider, Yousign meets the conditions and has **eIDAS certifications for electronic signature, electronic seal and time stamping**. All technical documentation can be accessed from the following page: Technical documentation of certifications.

List of standards met by Yousign:

Electronic seal and advanced signature	Qualified time stamp	Qualified seal and signature certificates
EN 319 401 V2.2.1	EN 319 401 V2.2.1	EN 319 401 V2.2.1
EN 319 403 V2.2.2	EN 319 403 V2.2.2	EN 319 403 V2.2.2
EN 319 411-1 V1.2.2	EN 319 421 V1.1.1	EN 319 411-1 V1.2.2
		EN 319 411-2 V2.2.2

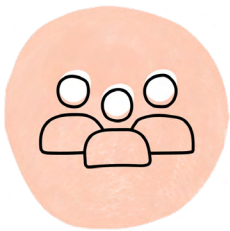
Whatever the signature level, Yousign uses a Proteccio HSM (server to secure cryptographic transactions).
The HSM is certified:
- *Common Criteria* at EAL4+;
- NATO SECRET approval;
- EU RESTRICTED approval;
- qualification reinforced by ANSSI [French National Agency for the Security of Information Systems].

To ensure continued compliance, we conduct audits on a regular basis.

- External eIDAS security and compliance audits;
- Internal eIDAS security and compliance audits.

Staff management & role

Yousign's employees are **aware of personal data security and protection**.



- Training on information security and protection of personal data for new employees;
- Regular communications to all teams;
- Appointment of technical consultants within the teams to ensure the implementation of good practices and internal rules.

We have put in place a role management policy and, as such, we limit access to each employee's role in accordance with the principle of least privilege. A review of the management of rights is carried out quarterly.

- Password management policy;
- Confidentiality undertakings.

Infrastructure & Access control

Yousign relies on hosting partners to ensure **optimal security of its infrastructure**, having in particular put in place an information system security policy that meets the requirements of several standards and certifications (PCI-DSS certification, ISO/IEC 27001 certification, SOC 1 TYPE II and SOC 2 TYPE II certification, etc.).

Physical access control

- Identity verification;
- Centralised management of access doors by a badge system;
- One-person double entrance security door;
- Surveillance equipment.

Control of logical access to data

- Two-step authentication process;
- Password management policy;
- Firewall & antivirus regularly updated;
- Logging & documented access control policy.

Transaction security & encryption

The entire transaction chain is **secured by encryption**. Yousign draws on modern encryption technologies that comply with the standards laid down by ANSSI.

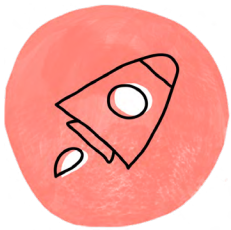
- Securing transactions via TLS encryption to and from our services;
- Encryption of documents at rest before and after signature via AES-256 bit encryption;
- Use of keys of more than 2048 bits and secure protocols such as RSA.

Management of vulnerabilities & Incidents

Vulnerability and incident management policies are in place. They **prevent, detect and resolve these events**.

- Vulnerability scans;
- Penetration testing by a specialised company;
- Monitoring detections via a Bug Bounty program;
- Vulnerability alerts and monitoring;
- Audits and code reviews;
- Process of notifying breaches to our customers and competent authorities.

Service availability & continuity

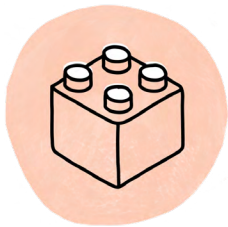


Yousign makes every effort to ensure **high service availability and service continuity**.

- Redundant and scalable infrastructure;
- Performance monitoring process;
- Regular stress testing of services;
- External vulnerability and intrusion tests;
- Management of security information and events;
- Business continuity plan;
- Business recovery plan.

Development Security

Internal development processes are in place for our teams to ensure the secure development of our solution.



- Monitoring of best practices laid down by the Open Web Application Security Project (OWASP);
- Security by design approach;
- Automatic and manual tests;
- Reviews of and changes to the code;
- Peer review.


yousign