Technische und organisatorische Maßnahmen

für Sicherheit und Schutz der Daten

yousign

Einführung

Yousign verpflichtet sich, die Vertraulichkeit Ihrer Daten und Ihre Privatsphäre zu wahren. Wir haben eine Vielzahl von technischen und organisatorischen Maßnahmen ergriffen, **um die Sicherheit der uns von Ihnen übermittelten personenbezogenen Daten zu gewährleisten.**
Diese Maßnahmen können sich ändern, wenn sich die Yousign-Lösung technisch weiterentwickelt und verbessert. Diesbezüglich kann Yousign andere geeignete Maßnahmen einführen.

Zertifizierungen und Audits

Als Vertrauensdiensteanbieter erfüllt Yousign die Anforderungen und verfügt über **eIDAS-Zertifizierungen für elektronische Signaturen, elektronische Stempel und Zeitstempel.**
Die gesamten technischen Unterlagen sind über diese Seite zugänglich:
Technischen Unterlagen

Verzeichnis der von Yousign eingehaltenen Normen:

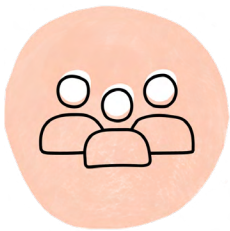
Elektronischer Stempel und fortgeschrittene Signatur	Qualifizierter Zeitstempel	Qualifizierte Stempel und Signaturzertifikate
EN 319 401 V2.2.1	EN 319 401 V2.2.1	EN 319 401 V2.2.1
EN 319 403 V2.2.2	EN 319 403 V2.2.2	EN 319 403 V2.2.2
EN 319 411-1 V1.2.2	EN 319 421 V1.1.1	EN 319 411-1 V1.2.2
		EN 319 411-2 V2.2.2

Unabhängig von der Signaturstufe verwendet Yousign einen HSM-Proteccio (Server, mit dem kryptographische Transaktionen gesichert werden können).
Das HSM ist zertifiziert laut:
- Generelle Kriterien auf EAL4+-Stufe;
- NATO SECRET-Zulassung;
- EU RESTRICTED-Zulassung;
- Verstärkte Qualifikation der französischen IT-Sicherheitsbehörde ANSSI.

Um sicherzustellen, dass unsere Compliance erhalten bleibt, führen wir regelmäßig Audits durch.

- Externe Sicherheits- und Compliance-Audits laut eIDAS;
- Interne Sicherheits- und Compliance-Audits laut eIDAS.

Personalmanagement und Rollen



Die Mitarbeiter von Yousign werden in Bezug auf die **Sicherheit und den Schutz personenbezogener Daten sensibilisiert.**

- Schulung zur Informationssicherheit und zum Schutz personenbezogener Daten für neue Mitarbeiter;
- Regelmäßige Kommunikationen an sämtliche Teams;
- Benennung von technischen Ansprechpartnern innerhalb der Teams, um die Umsetzung von bewährten Praktiken und internen Regeln zu gewährleisten.

Wir haben eine Richtlinie zum Rollenmanagement implementiert und beschränken somit den Zugriff auf die Rolle jedes Mitarbeiters nach dem Prinzip des geringsten Privilegs (engl. “principle of least privilege”). Eine Überprüfung der Rechteverwaltung wird vierteljährlich durchgeführt.

- Richtlinie zur Passwortverwaltung;
- Vertraulichkeitsverpflichtungen.

Infrastruktur und Zugangskontrolle

Yousign arbeitet mit Hosting-Partnern zusammen, um eine **optimale Sicherheit seiner Infrastrukturen** zu gewährleisten, und hat insbesondere eine Sicherheitspolitik für Informationssysteme implementiert, die die Anforderungen mehrerer Normen und Zertifizierungen erfüllt (PCI-DSS-Zertifizierung, ISO/IEC 27001-Zertifizierung, SOC 1 TYPE II- und SOC 2 TYPE II-Berichte, usw.).

Physische Zugangskontrolle

- Identitätsüberprüfung;
- Zentralisierte Verwaltung der Zugangstüren über ein Kartensystem;
- Ein-Personen-Schleuse;
- Überwachungsanlagen.

Logische Datenzugriffskontrolle

- Zweistufiger Authentifizierungsprozess;
- Richtlinie zur Passwortverwaltung;
- Firewall und Antivirenprogramme werden regelmäßig aktualisiert;
- Protokollierung und Richtlinie zur dokumentierten Zugriffskontrolle.

Transaktionssicherheit und Verschlüsselung

Die gesamte Transaktionskette ist durch **Verschlüsselung gesichert.** Yousign stützt sich auf moderne Verschlüsselungstechnologien, die den von der ANSSI festgelegten Standards entsprechen.

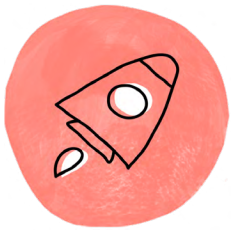
- Sicherung der Transaktionen über TLS-Verschlüsselung zu und von unseren Diensten;
- Verschlüsselung der ruhenden Dokumente vor und nach der Signatur mittels AES-256-Bit-Verschlüsselung;
- Verwendung von Schlüsseln mit einer Länge von mehr als 2.048 Bit und gesicherten Protokollen wie RSA.

Schwachstellen- und Vorfallmanagement

Richtlinien zum Management von Schwachstellen und Vorfällen sind vorhanden. Sie helfen, diese Ereignisse **zu verhindern, zu erkennen und zu beheben.**

- Schwachstellenscans;
- Pentest-Audit durch eine Fachfirma;
- Nachverfolgung der Erfassungen über ein Bug-Bounty-Programm;
- Warnungen und Schwachstellenüberwachung;
- Audits und Code-Reviews;
- Verfahren zur Benachrichtigung unserer Kunden und der zuständigen Behörden bei Verstößen.

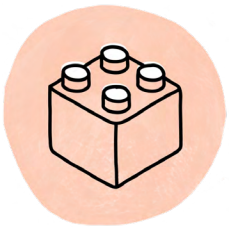
Verfügbarkeit und Kontinuität des Dienstes



Yousign unternimmt alle Anstrengungen, um eine **hohe Verfügbarkeit und Kontinuität der Dienste zu gewährleisten.**

- Redundante und skalierbare Infrastruktur;
- Prozesse zur Leistungsüberwachung;
- Regelmäßige Stresstests der Dienste;
- Schwachstellen- und Penetrationstests;
- Management der Sicherheitsinformationen und -ereignisse;
- Geschäftskontinuitätsplan;
- Disaster-Recovery-Plan.

Entwicklungssicherheit



Interne Entwicklungsprozesse sind für unsere Teams eingerichtet, um die sichere Entwicklung unserer Lösung zu gewährleisten.

- Überwachung der vom Open Web Application Security Project (OWASP) geforderten bewährten Praktiken;
- Security-by-Design-Ansatz;
- Automatische und manuelle Tests;
- Code-Reviews und -Änderungen;
- Peer-Review.


yousign