yousign.com

Technische en organisatorische maatregelen

voor de beveiliging en bescherming van gegevens

yousign

Inleiding

Yousign hecht veel waarde aan het beschermen van de vertrouwelijkheid van uw gegevens en uw privacy. We hebben verschillende technische en organisatorische maatregelen genomen om de **veiligheid van de persoonsgegevensdie u ons verstrekt, te waarborgen**. Deze maatregelen kunnen veranderen naarmate de oplossing van Yousign technisch evolueert en verbetert. In dit verband kan Yousign andere passende maatregelen nemen.

Certificeringen en audits

Als vertrouwde derde partij voldoet Yousign aan de eisen en beschikt het over **eIDAS-certificaten voor elektronische handtekeningen, elektronische stempels en tijdstempels**. Alle technische documentatie is toegankelijk op de pagina: Technische documentatie van certificeringen.

Lijst van normen die door Yousign worden nageleefd:

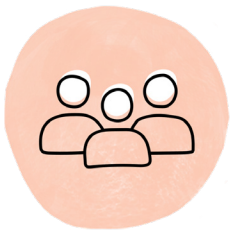
Elektronische stempel en geavanceerde handtekening	Gekwalificeerde tijdstempels	Gekwalificeerde stempel- en handtekeningcertificaten
EN 319 401 V2.2.1	EN 319 401 V2.2.1	EN 319 401 V2.2.1
EN 319 403 V2.2.2	EN 319 403 V2.2.2	EN 319 403 V2.2.2
EN 319 411-1 V1.2.2	EN 319 421 V1.1.1	EN 319 411-1 V1.2.2
		EN 319 411-2 V2.2.2

Ongeacht het niveau van de handtekening gebruikt Yousign een HSM-proteccio (een server die het mogelijk maakt om cryptografische transacties te beveiligen).
De HSM is gecertificeerd :
- *Gemeenschappelijke* criteria op EAL4+-niveau;
- NATO SECRET-goedkeuring;
- EU RESTRICTED-goedkeuring;
- kwalificatie versterkt door de ANSSI.

Om ervoor te zorgen dat onze compliance wordt gehandhaafd, voeren we regelmatig audits uit:

- externe veiligheids- en conformiteitsaudits eIDAS;
- interne veiligheids- en conformiteitsaudits eIDAS.

Personeels- en rollenbeheer



De medewerkers van Yousign zijn zich **bewust van de veiligheid en bescherming van persoonsgegevens**:

- opleiding in informatiebeveiliging en bescherming van persoonsgegevens voor nieuwe werknemers;
- regelmatige communicatie naar alle teams;
- aanwijzing van technische aanspreekpunten binnen de teams om de toepassing van goede praktijken en interne regels te garanderen.

We hebben een rolmanagementbeleid ingevoerd en beperken als zodanig de toegang tot de rol van elke werknemer in overeenstemming met het principe van “least privilege”. Elk kwartaal wordt een revisie van het rechtenbeheer uitgevoerd.

- beleid voor het beheer van wachtwoorden;
- vertrouwelijkheidsverplichtingen.

Infrastructuur en toegangscontrole

Yousign vertrouwt op zijn hostingpartners **om optimale beveiliging van zijn infrastructuren te garanderen en heeft** met name een veiligheidsbeleid voor informatiesystemen geïmplementeerd dat voldoet aan de eisen van verschillende normen en certificeringen (PCI-DSS-certificering, ISO/IEC 27001-certificering, SOC 1 TYPE II en SOC 2 TYPE II-certificering, etc.).

Fysieke toegangscontrole

- identiteitscontrole;
- gecentraliseerd beheer van toegangsdeuren via een badgesysteem;
- eenpersoons-draaideur;
- bewakingsapparatuur.

Logische controle op de toegang tot de gegevens

- tweestapsauthenticatieproces;
- beleid voor het beheer van wachtwoorden;
- regelmatig bijgewerkte firewall en antivirusprogramma;
- gedocumenteerd logboek- en toegangscontrolebeleid.

Transactiebeveiliging en encryptie

De hele transactieketen **is beveiligd door middel van encryptie**. Yousign maakt gebruik van moderne encryptietechnologieën die voldoen aan de door ANSSI gestelde normen:

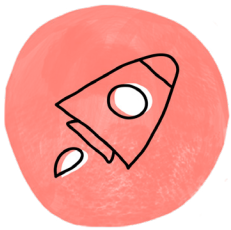
- beveiligde transacties via TLS-codering van en naar onze diensten;
- encryptie van documenten voor en na het ondertekenen via AES-256-bits encryptie;
- gebruik van sleutels die groter zijn dan 2048 bits en veilige protocollen zoals RSA.

Beheer van gevoelige punten en incidenten

Er zijn beleidsregels ingevoerd voor het beheren van gevoelige punten en incidenten.
Ze helpen deze gebeurtenissen te voorkomen, op te sporen en op te lossen.

- scans van gevoelige punten;
- spentest-audits door een gespecialiseerd bedrijf;
- sopvolging van detecties via een Bug Bounty-programma;
- swaarschuwingen voor kwetsbare punten;
- saudits en code reviews;
- sproces voor het melden van overtredingen voor onze klanten en bevoegde instanties.

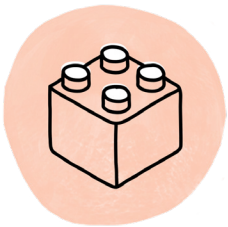
Beschikbaarheid en continuïteit van de dienstverlening



Yousign stelt alles in het werk om een **hoge beschikbaarheid en continuïteit van de diensten te garanderen**:

- redundante en schaalbare infrastructuur;
- prestatiebewaking;
- regelmatige stresstesten van diensten;
- controles op lekken en externe aanvallen;
- beheer van beveiligingsinformatie en -gebeurtenissen;
- bedrijfscontinuïteitsplanning;
- rampenplan.

Ontwikkeling van de beveiliging



Interne ontwikkelingsprocessen worden opgezet voor onze teams om de veilige ontwikkeling van onze oplossing te garanderen:

- monitoring van goede praktijken opgelegd door het Open Web Application Security Project (OWASP);
- beveiliging door middel van een "security by design";
- automatische en handmatige testen;
- codewijzigingen en -reviews;
- peer reviews.


yousign