Mesures techniques & organisationnelles

visant à la sécurité
et la protection des données

yousign

Introduction

Yousign a à cœur le respect de vos données et de votre vie privée. Nous avons mis en place une variété de mesures techniques et organisationnelles visant à **garantir la sécurité des données à caractère personnel que vous nous communiquez**. Ces mesures peuvent évoluer en fonction des progrès techniques et perfectionnements de la solution Yousign.
À cet égard, Yousign peut mettre en œuvre d'autres mesures adéquates.

Certifications et audits

En sa qualité de tiers de confiance, Yousign remplit les conditions et dispose des **certifications eIDAS en matière de signature électronique, de cachet électronique et d'horodatage**.
L'ensemble de la documentation technique est accessible sur notre site à la page Documentation technique des certifications.

Liste des normes respectées par Yousign :

Cachet électronique et signature avancée	Horodatage qualifié	Certificats qualifiés de cachet et de signature
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

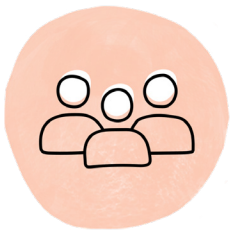
Quelque soit le niveau de signature, Yousign utilise un HSM proteccio (serveur permettant de sécuriser les transactions cryptographiques).
Le HSM est certifié :
- Critères Communs au niveau EAL4+ ;
- agrément NATO SECRET ;
- agrément EU RESTRICTED ;
- qualification renforcée par l'ANSSI.

Afin de s'assurer du maintien de notre conformité, nous réalisons des audits de façon régulière.

- Audits externes de sécurité et de conformité eIDAS ;
- Audits internes de sécurité et de conformité eIDAS.

Gestion du personnel et rôle

Les collaborateurs de Yousign sont **sensibilisés à la sécurité et à la protection des données à caractère personnel**.



- Formation à la sécurité de l'information et à la protection des données à caractère personnel pour les nouveaux collaborateurs ;
- Communications régulières à l'ensemble des équipes ;
- Désignation de référents techniques au sein des équipes pour assurer la mise en place des bonnes pratiques et des règles internes.

Nous avons mis en place une politique de gestion des rôles et, à ce titre, nous limitons les accès au rôle de chaque collaborateur dans le respect du principe du moindre privilège.
Une revue de la gestion des droits est réalisée de façon trimestrielle.

- Politique de gestion des mots de passe ;
- Engagements de confidentialité.

Infrastructure et contrôle d'accès

Yousign s'appuie sur des partenaires d'hébergement pour assurer une **sécurité optimale de ses infrastructures**, ayant notamment mis en place une politique de sécurité des systèmes d'information répondant aux exigences de plusieurs normes et certifications (certification PCI-DSS, certification ISO/IEC 27001, attestations SOC 1 TYPE II et SOC 2 TYPE II, etc.).

Contrôle d'accès physique

- Vérification d'identité ;
- Gestion centralisée des portes d'accès par un système de badge ;
- Sas unipersonnel ;
- Équipements de surveillance.

Contrôle d'accès logique aux données

- Processus d'authentification en deux étapes ;
- Politique de gestion des mots de passe ;
- Pare-feu & antivirus mis à jour régulièrement ;
- Journalisation & politique de contrôle d'accès documenté.

Sécurité des transactions et chiffrement

L'ensemble de la chaîne de transaction est **sécurisée par chiffrement**. Yousign s'appuie sur des technologies de chiffrement modernes et conformes aux standards édictés par l'ANSSI.

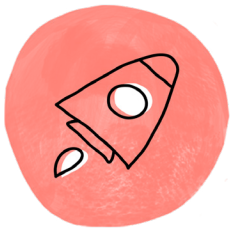
- Sécurisation des transactions via chiffrement TLS vers et depuis nos services ;
- Chiffrement au repos des documents avant et après signature via le chiffrement AES-256 bits ;
- Utilisation de clés supérieurs à 2048 bits et de protocoles sécurisés tel que le RSA.

Gestion des vulnérabilités et incidents

Des politiques de gestion des vulnérabilités et des incidents sont mises en place. Elles permettent de **prévenir, détecter et résoudre ces événements**.

- Scans des vulnérabilités ;
- Audit de pentest par une société spécialisée ;
- Suivi des détections via un programme de Bug bounty ;
- Alertes et veille des vulnérabilités ;
- Audits et revues de code ;
- Processus de notification des violations à nos clients et autorités compétentes.

Disponibilité et continuité du service

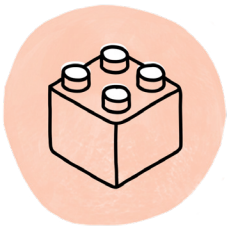


Yousign met tout en oeuvre pour garantir une **haute disponibilité et une continuité des services**.

- Infrastructure redondante et scalable ;
- Processus de suivi de performance ;
- Stress testing réguliers des services ;
- Tests de vulnérabilité et d'intrusion externe ;
- Gestion des informations et des événements de sécurité ;
- Plan de continuité d'activité ;
- Plan de reprise d'activité.

Sécurité du développement

Des processus internes de développement sont mis en place pour nos équipes afin de garantir un développement sécurisée de notre solution.



- Suivi des bonnes pratiques dictées par l'Open Web Application Security Project (OWASP) ;
- Approche "security by design" ;
- Tests automatiques et manuels ;
- Revues et modifications du code ;
- Évaluation par les pairs.


yousign