Sécurité, légalité et confidentialité des services Dropbox Sign

Dropbox Sign

Sommaire

Sommaire

Introduction

Les documents, contrats et accords que vous signez en tant qu'entreprise font partie des documents les plus importants en votre possession. Bon nombre de ces opérations impliquent une signature à valeur juridique et sont essentielles au bon fonctionnement d'une entreprise. En voici quelques exemples : documents servant au recrutement de nouveaux employés, contrats de vente, baux immobiliers, contrats de partenariat, contrats signés par les fournisseurs, etc. Ces documents contenant souvent des informations sensibles, leur sécurité est donc une préoccupation majeure. Avec les services Dropbox Sign, qui englobent Dropbox Sign, Dropbox Forms et Dropbox Fax, la protection de vos documents et des transactions associées est une priorité absolue. Nous nous engageons à garantir la confidentialité, la sécurité et la protection de tous les documents signés avec les services Dropbox Sign.

La sécurité couvre un large éventail de sujets, et ce livre blanc entend en donner une vue d'ensemble assez complète. Si en tant que client, vous achetez une valeur de contrat minimale, Dropbox peut collaborer avec vous sur des analyses de sécurité, des questionnaires et des évaluations personnalisés.

Équipe de sécurité dédiée et expérimentée

Toutes les personnes travaillant chez Dropbox se consacrent à la sécurité et à la protection des données des clients dans tout ce qu'elles font. Les services Dropbox Sign suivent les principes du programme de sécurité des informations établis sous la direction du responsable de la sécurité de Dropbox.

Les membres des équipes Dropbox font l'objet d'une vérification complète de leurs antécédents. Ils doivent également signer et respecter un code de conduite et une politique d'utilisation acceptable, mais aussi suivre une formation annuelle sur la confidentialité et de sensibilisation à la sécurité.

Fiabilité

Pour pouvoir développer votre activité, vous avez besoin que nous soyons à vos côtés. C'est la raison pour laquelle nous nous efforçons d'être le plus disponibles possible. Vous pouvez en permanence consulter notre disponibilité actuelle sur le **site indiquant l'état de nos services**.

Continuité d'exploitation et reprise d'activité

Notre entreprise a conscience qu'une catastrophe peut survenir à tout moment, quelle que soit la région ou quel que soit le site. Notre infrastructure a été conçue pour résister, et des plans d'urgence existent en cas d'événements susceptibles d'impacter les services. Nous utilisons Amazon Web Services (AWS), réparti sur plusieurs datacenters, afin de garantir la redondance des données et de leur traitement. Notre entreprise dispose d'un plan complet de continuité d'exploitation et de reprise d'activité pour garantir la disponibilité du système. Ce plan est révisé et testé tous les ans. Les données critiques concernant le système sont quant à elles sauvegardées tous les jours. Notre équipe d'ingénierie est informée en cas de défaillance du système de sauvegarde et elle prend les mesures qui s'imposent pour résoudre les problèmes constatés.

Authentification

Il est extrêmement important que nous puissions vérifier l'identité d'un utilisateur avant de l'autoriser à envoyer un document pour signature ou à apposer sa signature. À cette fin, nous disposons de plusieurs fonctionnalités qui garantissent une authentification forte des personnes.

Validation en deux étapes.
Les utilisateurs peuvent configurer la validation en deux étapes, qui oblige à saisir un code unique généré par Google Authenticator ou envoyé par SMS. Ce code doit être utilisé en plus de leur nom d'utilisateur et de leur mot de passe. Les administrateurs d'équipe peuvent déterminer la méthode à utiliser pour la validation en deux étapes.

- **Authentification unique** (disponible avec un compte Dropbox ou Google)
- **Authentification basée sur la clé API pour l'API**
- **Hachage et salage sécurisés de tous les mots de passe**

Les sessions expirent après un certain temps.

Le délai est d'une heure par défaut, mais il peut être étendu à 30 jours si l'utilisateur clique sur **Mémoriser** au moment de la connexion.

Fonctionnalités d'authentification spécifiques de Dropbox Sign :

- **Demandes de signatures protégées par un code d'accès.** Dans Dropbox Sign, les utilisateurs peuvent activer un "code d'accès du signataire" (une chaîne alphanumérique constituée de 4 à 12 caractères) que les signataires devront saisir pour pouvoir consulter un document.

- **OAuth**. Dropbox Sign API prend en charge OAuth, qui permet d'authentifier des appels d'API pour le compte d'un utilisateur.

- **SAML**. Dropbox Sign prend en charge SAML 2.0 pour l'authentification unique en entreprise.

Autorisations

Il est impératif que vous puissiez contrôler qui peut faire quoi au sein du système.

Produit Dropbox Sign

À chaque rôle, des droits d'accès différents (tant dans Dropbox Sign API que dans le produit de l'utilisateur final). Par exemple, les administrateurs contrôlent les paramètres de l'équipe, les informations de facturation et les rôles des autres utilisateurs.

- **Sécurité basée sur les rôles.** Différents niveaux d'autorisation peuvent être accordés aux différents membres d'une équipe. Cela va des droits d'administration aux autorisations de consultation des modèles ou d'émission de demandes de signature.

- **Codes d'accès des signataires.** Pour un niveau de sécurité supplémentaire, chaque signataire peut se voir attribuer un code d'accès qui permet de savoir qui signe.

Produit Dropbox Forms

- **Sécurité basée sur les rôles.** Différents niveaux d'autorisation peuvent être accordés aux différents membres d'une équipe. Cela va des droits d'administration aux autorisations d'accès limité aux fonctionnalités.

Chiffrement

Les documents sont stockés dans une infrastructure contrôlée de manière sécurisée. Ils sont également authentifiés sur la session de l'expéditeur chaque fois qu'une demande les concernant est effectuée. Nous appliquons les bonnes pratiques du secteur pour la transmission des données vers notre plateforme (protocole TLS, Transport Layer Security), et les données sont stockées dans des datacenters certifiés SOC 1 Type II, SOC 2 Type I et ISO 27001. Vos documents sont stockés et chiffrés au repos à l'aide du chiffrement AES 256 bits.

De plus, chaque document est chiffré au moyen d'une clé unique. Pour une protection supplémentaire, chaque clé est chiffrée à l'aide d'une clé principale qui change régulièrement. En d'autres termes, même si une personne parvenait à contourner la sécurité physique et à accéder à un disque dur, elle ne serait pas en mesure de déchiffrer vos données.

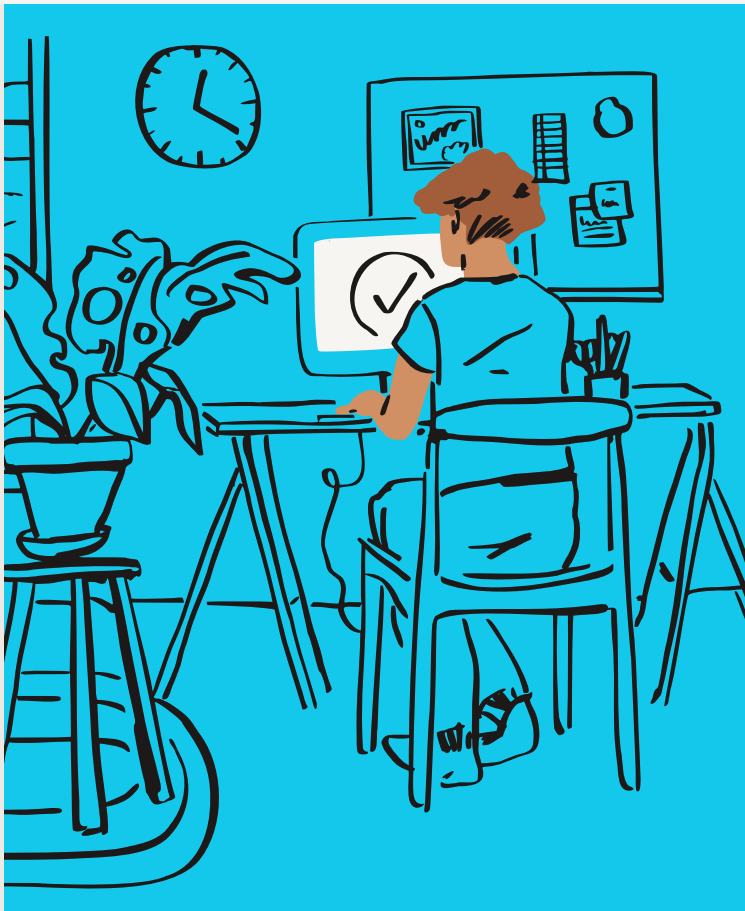
En résumé :

- Tous les documents sont chiffrés au repos à l'aide du chiffrement AES 256 bits.
- Chaque document est chiffré au moyen d'une clé unique, qui est elle-même chiffrée au moyen d'une clé principale.
- La clé principale change régulièrement.
- Les sauvegardes des documents sont chiffrées.
- Les documents en transit sont chiffrés au moyen du protocole TLS 1.2 ou ultérieur.
- L'application Web utilise un mécanisme HSTS pour veiller à la sécurité de la connexion.

Confidentialité

Chez Dropbox, nous partons du principe que vous êtes propriétaire de vos données et nous nous engageons à en protéger leur confidentialité. Notre **politique de confidentialité** stipule clairement la façon dont nous gérons et protégeons vos informations. Chaque année, nos auditeurs tiers indépendants testent nos contrôles de confidentialité et nous communiquent leurs rapports et recommandations, que nous pouvons partager avec vous sur simple demande. Pour en savoir plus sur la façon dont Dropbox s'engage à protéger vos données à caractère personnel, **cliquez ici**.

Pour signaler un problème de confidentialité, veuillez contacter privacy@dropbox.com.



Piste d'audit

Produit Dropbox Sign

Chaque signature ajoutée à un contrat est associée au document. Lorsque vous envoyez une demande de signature, Dropbox Sign annexe une page de piste d'audit au document lui-même. Cette piste d'audit contient un identificateur global unique (GUID) qui peut servir à rechercher un enregistrement dans notre base de données afin de savoir qui a signé un document et à quel moment. Pour en savoir plus, lisez notre **déclaration de légalité**.

Cette piste d'audit non modifiable garantit que chaque action sur vos documents est minutieusement consignée et horodatée, afin de fournir une preuve admissible d'accès, de lecture et de signature.

Voici une liste de certains des événements consignés dans la piste d'audit Dropbox Sign :

- Document envoyé
- Document consulté
- Document signé
- Refus de signature
- Nom/adresse e-mail du signataire mis à jour
- Pièce jointe importée
- Signature en personne activée
- Authentification du signataire via un code d'accès
- Consentement de document électronique et de signature électronique donné
- Demande de signature déléguée
- Demande de signature terminée
- Suite de la demande terminée

Pour obtenir une liste à jour de tous les événements consignés dans la piste d'audit, nous vous invitons à consulter notre **page sur la sécurité**.

Authenticité

Chaque signature ajoutée à un contrat est associée au document. Lorsque vous envoyez une demande de signature, Dropbox Sign annexe une page de piste d'audit au document lui-même. Cette piste d'audit contient un identificateur global unique (GUID) qui peut servir à rechercher un enregistrement dans notre base de données afin de savoir qui a signé un document et à quel moment. Pour en savoir plus, lisez notre déclaration de légalité.

Sécurité des applications

La sécurité des applications entrant dans le cadre des services Dropbox Sign fait partie intégrante du programme Dropbox Application Security. Nous utilisons notre processus d'admission pour analyser la conception et l'architecture des nouvelles fonctionnalités. L'ensemble du code des services Dropbox Sign est analysé à la recherche de problèmes de sécurité au moyen d'outils d'analyse du code statique comme Semgrep et CodeScan. Les services Dropbox Sign sont également couverts par notre programme Bug Bounty, qui cherche à détecter les failles de sécurité et les bugs permettant d'accéder aux données sensibles. L'accès s'effectue via Bugcrowd : **bugcrowd.com/dropbox**.

Surveillance de la sécurité

Les services Dropbox Sign utilisent les plateformes de sécurité cloud natives avec une remontée directe des alertes de sécurité. Dropbox surveille activement l'activité suspecte des utilisateurs et suit les accès aux composants critiques.

Sécurité, légalité et confidentialité des services Dropbox Sign

Infrastructure

Dropbox Sign fait appel à Amazon Web Service (AWS) en tant que fournisseur IaaS (infrastructure en tant que service), et les datacenters Amazon hébergent nos données aux États-Unis. Nous profitons également de l'implantation d'AWS dans l'Union européenne, au Royaume-Uni, au Japon, en Australie et au Canada.

Les services Dropbox Sign utilisent les fonctionnalités de sécurité d'Amazon comme Virtual Private Cloud (VPC), les groupes de sécurité, le chiffrement des disques, etc. pour garantir la confidentialité des données de nos clients dans le cloud.

Sécurité physique

Les services Dropbox Sign sont hébergés dans Amazon Web Services sur des sites de pointe certifiés SOC 1 Type II, SOC 2 et ISO 27001.

Sécurité du personnel

Les membres des équipes Dropbox font l'objet d'une vérification complète de leurs antécédents avant d'être embauchés. Tous les employés et sous-traitants doivent signer et respecter un code de conduite et une politique d'utilisation acceptable. Tous les employés doivent également suivre une formation sur la confidentialité et de sensibilisation à la sécurité. Cette formation a lieu au moment de leur embauche, puis tous les ans. Ils reçoivent de plus des newsletters et des notifications de sécurité pertinentes qui les sensibilisent en continu à la sécurité des informations.

Conformité

Dropbox Sign respecte les cadres, normes et réglementations suivants :

SOC 2 Type II

Les rapports SOC (Service Organization Controls) sont des cadres de référence établis par l'American Institute of Certified Public Accountants (AICPA) pour rendre compte des dispositifs de contrôle internes mis en place dans une entreprise. Les systèmes, les applications, les employés et les processus de Dropbox Sign sont certifiés par une série d'audits réalisés par Schellman Compliance LLC, un cabinet d'audit tiers indépendant.

Le rapport SOC 2 atteste de l'efficacité de nos contrôles auprès des clients et couvre les critères de fiabilité d'un service, à savoir la sécurité, la disponibilité et la confidentialité (TSP section 100). Il offre une description détaillée des processus de Dropbox Sign ainsi que des contrôles que nous avons mis en place pour protéger les données des clients (à savoir plus d'une centaine). Outre l'avis de notre auditeur tiers indépendant sur l'efficacité de nos contrôles, tant du point de vue de leur conception que de leur fonctionnement, ce rapport intègre également les procédures de test de cet auditeur et les résultats pour chaque contrôle. L'audit SOC 2 est disponible sur demande auprès de notre service commercial. Il suffit d'envoyer un e-mail à compliance-reports@hellosign.com.

ISO 27001 (Management de la sécurité de l'information)

ISO 27001 est l'une des normes relatives aux systèmes de management de la sécurité des informations (SMSI) les plus reconnues sur le plan international. Elle reprend également les bonnes pratiques de sécurité détaillées dans la norme ISO 27002. Pour mériter votre confiance, nous assurons pour Dropbox Sign une gestion et une amélioration continues et globales de nos mesures de contrôle physiques, techniques et juridiques. Notre cabinet d'audit, Schellman Compliance LLC, est accrédité ISO 27001 par **ANSI-ASQ National Accreditation Board (ANAB).** Consultez le **certificat ISO 27001** de nos solutions Dropbox Sign, Dropbox Fax et Dropbox Forms.

Sécurité, légalité et confidentialité des services Dropbox Sign

ISO 27018 (Protection des données personnelles dans le cloud)

ISO 27018 est une norme internationale relative à la protection et à la confidentialité des données. Elle s'applique aux fournisseurs de services cloud comme Dropbox Sign qui traitent des informations personnelles pour le compte de leurs clients. Elle sert de référence à nos clients pour comprendre les exigences contractuelles et réglementaires générales ou poser des questions. Nous adhérons à la norme ISO 27018 dans le cadre de notre certification ISO 27001. Consultez le **certificat ISO 27018** de nos solutions Dropbox Sign, Dropbox Fax et Dropbox Forms.

Nos produits Dropbox Sign et Dropbox Forms sont conformes à la loi HIPAA

Dropbox Sign se conforme aux dispositions des lois américaines HIPAA (Health Insurance Portability and Accountability Act) et HITECH (Health Information Technology for Economic and Clinical Health Act).

Ces lois visent à encourager la prolifération des technologies dans le domaine de la santé tout en mettant en place les protections nécessaires pour garantir la sécurité et la confidentialité des données de santé. Des organisations comme les hôpitaux, les cabinets médicaux et dentaires, mais aussi toute personne manipulant des informations médicales protégées (PHI), peuvent être soumises aux lois HIPAA/HITECH. Peuvent également être concernées les entreprises qui travaillent avec ces structures et qui sont en contact avec de telles données pour leur compte.

Dropbox Sign met à votre disposition un rapport sur la Règle de sécurité HIPAA et les exigences en matière de notification des brèches HITECH. Les clients souhaitant accéder à ces documents peuvent contacter notre service commercial en envoyant un e-mail à compliance-reports@hellosign.com.

ESIGN Act (loi des États-Unis sur les signatures électroniques de 2000)

L'Electronic Signatures in Global and National Commerce Act est une loi fédérale qui fournit une règle de validité générale pour les transactions impliquant des documents et des signatures électroniques. Entre autres choses, l'ESIGN Act des États-Unis oblige à démontrer l'intention de signer ainsi qu'elle oblige à fournir un avis de divulgation aux consommateurs et à conserver les enregistrements.

Uniform Electronic Transactions Act (UETA) de 1999

Adoptée en 1999 par la National Conference of Commissioners on Uniform State Laws, **l'Uniform Electronic Transaction Act** permet d'utiliser des transactions par communication électronique en accordant aux signatures électroniques la même valeur légale que les signatures manuscrites sur papier. L'UETA a été adoptée par tous les États des États-Unis, à l'exception de celui de New York.

Règlement IDAS – Règlement eIDAS pour l'Union européenne de 2016 (règlement UE n° 910/2014 qui remplace l'ancienne directive européenne 1999/93/CE)

Le règlement eIDAS définit trois types de signatures électroniques : signature électronique simple, avancée et qualifiée (SES, SEA et SEQ). Il s'applique à l'identification électronique et aux services de confiance, et concerne les transactions électroniques effectuées au sein du marché unique européen. Il établit un cadre juridique permettant aux personnes, aux entreprises (notamment aux PME) et aux administrations publiques d'accéder en toute sécurité aux services et d'effectuer des transactions numériques dans tous les États membres de l'UE. Dropbox Sign prend en charge les signatures électroniques standard (SES) et qualifiées (QES). Pour en savoir plus sur le règlement eIDAS, consultez notre **page sur la conformité**.

Privacy Shield

Dropbox respecte les cadres Privacy Shield établis entre les États-Unis et l'Union européenne et entre les États-Unis et la Suisse. Ces cadres ont été élaborés par le ministère du Commerce des États-Unis pour régir la collecte, l'utilisation et la conservation des données à caractère personnel transférées aux États-Unis à partir de l'Union européenne, de l'Espace économique européen et de la Suisse. Pour en savoir plus, consultez la **certification Privacy Shield** de Dropbox et le **site Web du Privacy Shield**.

Règlement général sur la protection des données (RGPD) de l'UE

Le Règlement général sur la protection des données 2016/679 (RGPD) est un règlement de l'Union européenne qui marque un changement significatif par rapport au cadre existant relatif au traitement des données à caractère personnel des individus au sein de l'UE. Le RGPD contient une série d'exigences (nouvelles ou améliorées) qui s'appliquent aux entreprises exploitant des données à caractère personnel (telles que Dropbox). Dropbox Sign respecte les principes du RGPD afin de permettre à nos clients d'utiliser la solution pour faciliter leur mise en conformité vis-à-vis du RGPD. Pour en savoir plus sur le **RGPD et la conformité de Dropbox Sign,** consultez notre Trust Center.

Pour accéder à nos audits et évaluations, veuillez nous contacter par e-mail à l'adresse compliance-reports@hellosign.com.

Lien vers des ressources importantes

Politique de confidentialité de Dropbox Sign

Trust Center Dropbox Sign

Sécurité de Dropbox Sign

Conformité de Dropbox Sign