Dropbox

Confidentialité et protection des données

Introduction

Les données personnelles jouent un rôle essentiel dans la société et l'économie. Les utilisateurs demandent de plus en plus de clarté et de transparence sur la façon dont leurs données personnelles sont utilisées et sécurisées par les entreprises avec lesquelles ils interagissent. Ils souhaitent également que ces entreprises suivent des directives claires en matière de protection des données personnelles.

Chez Dropbox, les relations que nous entretenons avec des millions de particuliers et d'entreprises à travers le monde reposent sur la confiance. Nous sommes très reconnaissants de celle que vous nous accordez et nous prenons très au sérieux la responsabilité qui est la nôtre de protéger vos données personnelles.

Nos engagements

Nous nous engageons à protéger vos données personnelles. Les conditions d'utilisation de Dropbox décrivent vos responsabilités lorsque vous utilisez nos services. Notre politique de confidentialité décrit nos engagements de confidentialité envers nos utilisateurs et explique comment nous collectons, utilisons et gérons vos données personnelles lorsque vous recourez à nos services. Si vous résidez dans l'Union européenne (UE), vos données personnelles sont contrôlées par Dropbox International Unlimited Company, une société basée en Irlande.

Si vous utilisez Dropbox Business ou Dropbox Education, votre entreprise est responsable du traitement de toute donnée personnelle transmise à Dropbox dans le cadre de l'utilisation de Dropbox Business ou de Dropbox Education. En tant que responsable du traitement, vous déterminez dans quels buts et par quels moyens les données personnelles sont traitées. Dropbox agit en tant que sous-traitant pour le compte des entreprises utilisant Dropbox Business ou Dropbox Education. Notre Contrat Entreprises inclut d'ailleurs un certain nombre d'engagements relatifs au traitement des données et à leur transfert en dehors des frontières nationales.

Nos certifications en matière de conformité

La conformité est un bon moyen d'évaluer la fiabilité d'un service. Il est important pour nous de vous prouver, par le biais d'auditeurs indépendants, que nos pratiques de sécurité et de confidentialité sont conformes aux normes et réglementations les plus courantes, notamment ISO 27001, ISO 27017, ISO 27018, BSI C5 (Allemagne) et SOC 1, 2 et 3. Par exemple, nous étions l'un des premiers fournisseurs de services cloud à avoir obtenu la certification ISO 27018. Cette norme reconnue à l'échelle mondiale régit la confidentialité et la protection des données dans le cloud. Des auditeurs tiers indépendants testent nos contrôles et nous communiquent leurs rapports et recommandations, que nous partageons avec vous le plus régulièrement possible.

Notez que, même si nos certifications et rapports d'audit concernent généralement Dropbox Business et Dropbox Education, la majorité de nos contrôles s'appliquent également à Dropbox Basic, Dropbox Plus et Dropbox Professional. Vous trouverez plus d'informations sur les normes que nous respectons et sur la validation de nos pratiques sur notre page Web relative à la conformité.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

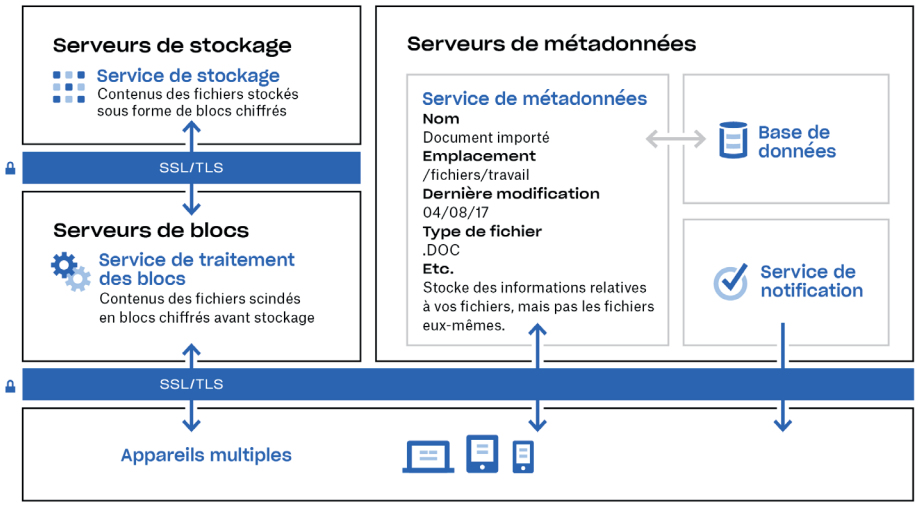
Dropbox

Notre infrastructure protège vos données personnelles

Chez Dropbox, nous sommes convaincus que la protection de vos données est le premier pas vers la sécurité de vos données personnelles. De par sa conception, Dropbox intègre plusieurs niveaux de protection, comme le transfert sécurisé des données, le chiffrement et les contrôles au niveau des applications, qui sont répartis sur une infrastructure sécurisée à grande échelle.

Infrastructure de fichiers

L'infrastructure de fichiers Dropbox comporte les éléments suivants :



Serveurs de blocs

Pour protéger les données des utilisateurs, Dropbox intègre un dispositif de sécurité unique qui va bien au-delà des systèmes de chiffrement traditionnels. Les serveurs de blocs traitent les fichiers issus des applications Dropbox en les scindant en plusieurs blocs, en chiffrant chacun d'eux à l'aide d'un algorithme renforcé et en synchronisant uniquement les blocs modifiés entre les révisions. Lorsqu'une application Dropbox détecte la présence d'un nouveau fichier ou d'un fichier modifié, elle le signale aux serveurs de blocs. Les blocs de fichiers nouveaux ou modifiés sont ensuite traités et transférés vers les serveurs de stockage.

Service de notification

Ce service indépendant permet de détecter les modifications apportées aux comptes Dropbox. Il n'implique aucun stockage ni transfert de fichiers ou de métadonnées. Chaque client établit une connexion d'interrogation longue avec le service de notification. En cas de modification d'un fichier dans Dropbox, le service de notification en informe le ou les clients concernés en fermant cette connexion. La fermeture de la connexion indique que le client doit se connecter aux serveurs de métadonnées de manière sécurisée afin de synchroniser les modifications.

Serveurs de métadonnées

Certaines informations de base, que l'on appelle également "métadonnées", sont stockées par un service de stockage dédié. Ce service sert également d'index pour les données stockées dans les comptes des utilisateurs. Toutes les métadonnées Dropbox sont stockées dans un service de base de données MySQL. Elles sont partitionnées et répliquées autant de fois que nécessaire pour atteindre les performances et les niveaux de disponibilité attendus. Les métadonnées comprennent les informations de base sur les comptes et les utilisateurs, telles que les adresses e-mail, les noms d'utilisateur ou les noms d'appareil. Elles incluent également des informations de base sur les fichiers, telles que leur nom et leur type, et sont notamment utilisées par les fonctionnalités d'historique des versions, de récupération et de synchronisation.

Serveurs de stockage

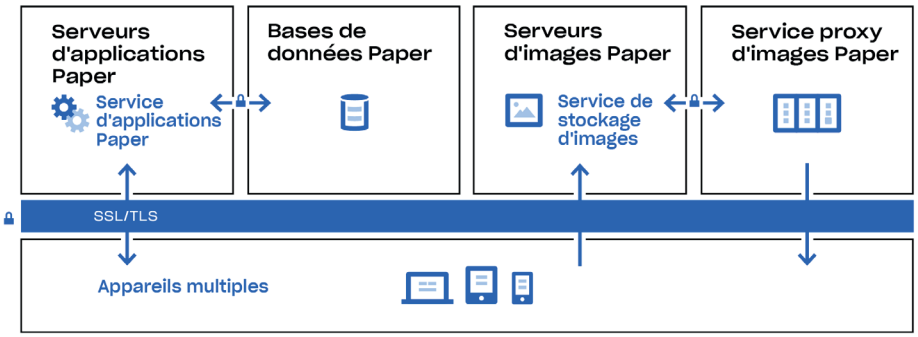
Une fois les fichiers scindés en blocs et chiffrés par les serveurs de blocs, le contenu de ces blocs de fichiers est stocké sur les serveurs de stockage. Ce service fonctionne comme un système de stockage CAS (Content-Addressable Storage), chaque bloc de fichier chiffré étant récupéré en fonction de sa valeur de hachage.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

Infrastructure Paper

Dropbox Paper (Paper) est un produit Dropbox. Toutefois, Paper se base presque essentiellement sur des systèmes distincts au sein de l'infrastructure Dropbox. L'infrastructure de Paper est constituée des éléments suivants :



Serveurs d'applications Paper

Les serveurs d'applications Paper traitent les demandes des utilisateurs, effectuent le rendu des documents Paper modifiés et assurent les services de notification. Ils écrivent les modifications utilisateur entrantes dans les bases de données Paper, où elles sont placées sur du stockage persistant. Les sessions de communication entre les serveurs d'applications et les bases de données Paper sont chiffrées à l'aide d'un algorithme renforcé.

Service proxy d'images Paper

Le service proxy d'images Paper affiche un aperçu des images ajoutées dans les documents Paper et des liens hypertexte qui y sont intégrés. Pour les images ajoutées dans les documents Paper, le service proxy d'images Paper récupère les données d'image stockées sur les serveurs d'images Paper via un canal chiffré. Pour les liens hypertexte ajoutés dans les documents Paper, le service proxy d'images récupère les données d'image depuis le lien source et affiche un aperçu de l'image via HTTP ou HTTPS, en fonction de ce que le lien indique.

Bases de données Paper

Le contenu des documents Paper des utilisateurs, ainsi que certaines métadonnées sur ces documents, sont chiffrés dans le stockage persistant des bases de données Paper. Cela inclut les informations sur le document Paper (son titre, ses autorisations, les utilisateurs avec qui il est partagé, les dossiers associés, etc.), ainsi que le contenu du document Paper en lui-même, y compris les commentaires et les tâches. Les bases de données Paper sont partitionnées et répliquées autant de fois que nécessaire pour atteindre les performances et les niveaux de disponibilité attendus.

Serveurs d'images Paper

Les images ajoutées dans les documents Paper sont stockées et chiffrées au repos sur les serveurs d'images Paper. La transmission des données d'image entre l'application Paper et les serveurs d'images Paper s'effectue dans le cadre d'une session chiffrée.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

Contrôles Dropbox : nos pratiques internes

Nous prenons des mesures exhaustives visant à protéger notre infrastructure, notre réseau et nos applications ; nous formons nos employés aux pratiques de sécurité et de confidentialité ; nous créons une culture accordant une priorité absolue à la confiance. Certains de nos contrôles sont décrits ci-dessous :

Formation

L'une des méthodes mises en œuvre pour protéger les données personnelles de nos utilisateurs consiste à sensibiliser nos employées aux problématiques de sécurité et de confidentialité. Les employés de Dropbox doivent accepter nos règles de sécurité, y compris notre politique de confidentialité des données, avant de se voir accorder un accès aux systèmes. Ils doivent également suivre une formation obligatoire sur la sécurité et la confidentialité lors de leur embauche, ainsi que des formations complémentaires tous les ans. Par ailleurs, les employés sont régulièrement sensibilisés aux questions de sécurité par le biais d'e-mails informatifs, de présentations et de ressources disponibles sur notre intranet.

Chiffrement des données en transit

Pour protéger les blocs de fichiers en transit entre un client Dropbox (client de bureau, application mobile, API ou site Web) et les serveurs frontaux de Dropbox, une connexion chiffrée est négociée afin de garantir une livraison sécurisée. De même, une connexion chiffrée est négociée pour protéger les données des documents Paper en transit entre un client Paper (application mobile, API ou site Web) et le service hébergé. Ces connexions sont chiffrées à l'aide du protocole SSL/TLS (Secure Sockets Layer/Transport Layer Security) afin de créer un tunnel sécurisé protégé par un chiffrement AES (Advanced Encryption Standard) d'au moins 128 bits.

Chiffrement des données au repos

Les fichiers transférés par les utilisateurs sont stockés sur les serveurs de stockage Dropbox sous forme de blocs de fichiers séparés. Chaque bloc est protégé par un chiffrement AES (Advanced Encryption Standard) de 256 bits. Seuls les blocs modifiés d'une révision à une autre sont synchronisés. Les données des documents Paper stockées dans les bases de données Paper sont, elles aussi, protégées par un chiffrement AES (Advanced Encryption Standard) de 256 bits.

Suppression permanente de fichiers et de documents Paper

Lorsqu'un utilisateur Dropbox, ou l'administrateur d'une équipe Dropbox Business ou Dropbox Education, marque un fichier en vue d'une suppression définitive, il déclenche un processus de suppression définitive. De même, lorsqu'un utilisateur, ou l'administrateur d'une équipe Dropbox Business ou Dropbox Education, marque un document Paper en vue d'une suppression définitive, il déclenche un processus similaire pour les données d'image et les données des documents Paper.

Demandes d'accès aux données personnelles

Pour obtenir des informations autres que les fichiers et les documents Paper stockés dans Dropbox, les utilisateurs peuvent se connecter au site Web et accéder à leur compte. La page de compte affiche des informations telles que le nom et l'adresse e-mail qui y sont associés. Les utilisateurs peuvent également consulter les adresses IP des sessions, ordinateurs et appareils mobiles connectés, ainsi que les applications connectées à leurs comptes à partir de la page de sécurité et de la page des applications connectées.

Les utilisateurs Dropbox peuvent demander d'avoir accès à d'autres informations personnelles que nous aurions recueillies à leur sujet ou de les supprimer. Pour en savoir plus, consultez cet article du centre d'assistance Dropbox.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

Principes relatifs aux demandes émanant des autorités

Nous savons que lorsque les utilisateurs nous confient leurs données personnelles, ils veulent que ces données restent confidentielles. Comme la plupart des services en ligne, Dropbox reçoit parfois des demandes émanant des autorités, qui souhaitent obtenir des informations sur ses utilisateurs.

Les principes ci-dessous expliquent la façon dont nous gérons ces demandes.

Faire preuve de transparence

Nous pensons que les services en ligne devraient pouvoir publier le nombre et le type de demandes qu'ils reçoivent de la part des autorités, et notifier les individus concernés par ces demandes. Ce type de transparence permet aux utilisateurs de mieux comprendre les demandes abusives de certaines administrations. Nous continuerons à publier des informations détaillées sur ces demandes et à plaider pour le droit à fournir davantage de ces informations importantes.

Lutter contre les demandes trop vagues

Les demandes de données émanant des autorités devraient être limitées aux informations recherchées, ainsi qu'à des personnes spécifiques et à des enquêtes justifiées. Nous lutterons contre les demandes non ciblées et trop vagues.

Fournir des services de confiance

Les gouvernements ne devraient jamais être autorisés à installer des portes dérobées sur les services en ligne ni compromettre l'infrastructure pour obtenir des données sur les utilisateurs. Nous continuerons à faire tout notre possible pour protéger nos systèmes et faire modifier la législation afin d'établir clairement que ce type d'activité est illégal.

Protéger tous les utilisateurs

Les lois accordant différentes protections aux individus en fonction de leur pays de résidence ou de leur citoyenneté sont obsolètes et ne reflètent pas la nature internationale des services en ligne. Nous continuerons de plaider pour la réforme de ces lois.

Ces principes, tout comme notre rapport de transparence annuel, sont accessibles sur le site Web de Dropbox : https://www.dropbox.com/transparency.

Pour en savoir plus sur nos contrôles et notre approche de la protection des données personnelles, consultez notre livre blanc sur la sécurité Dropbox Business.

Intervention de tiers

Dropbox gère la majorité des activités associées à la fourniture de nos services. Il nous arrive toutefois de faire appel à certains tiers de confiance (par exemple, des fournisseurs de services informatiques et d'assistance client). Ces tiers accèdent à vos informations uniquement pour effectuer certaines tâches à notre place tout en respectant notre politique de confidentialité et nous demeurons responsables de la façon dont ils gèrent vos informations conformément à nos instructions. Chaque tiers est soumis à un examen rigoureux, notamment des contrôles de sécurité et des contrôles contractuels réguliers, pour évaluer sa capacité à répondre à nos engagements en termes de protection des données.

Transferts internationaux de données

Dropbox s'appuie sur différents mécanismes juridiques pour ses transferts internationaux de données personnelles entre l'Union européenne et les États-Unis. Nous respectons l'accord Privacy Shield entre l'Union européenne et les États-Unis, ainsi qu'entre la Suisse et les États-Unis, pour ce qui concerne la collecte, l'utilisation et la conservation des données personnelles et leur transfert depuis l'Union européenne et la Suisse à destination des États-Unis. En plus du Privacy Shield, Dropbox offre également des garanties contractuelles solides concernant la confidentialité de ses services et s'appuie sur les clauses contractuelles types de la Commission européenne pour encadrer ses transferts internationaux de données.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

RGPD : Règlement général sur la protection des données

Le Règlement général sur la protection des données (RGPD) est le nouveau texte de référence européen qui régit la protection des données à caractère personnel des résidents de l'Union européenne. Le RGPD est le texte juridique européen le plus important en termes de protection des données depuis la directive de l'UE de 1995, et de nombreuses entreprises ayant des activités en Europe (dont Dropbox) ont beaucoup investi pour s'y conformer.

Le RGPD a pour objectif d'harmoniser les lois sur la protection des données en Europe et de les aligner sur l'évolution technologique des deux dernières décennies. Il repose sur d'anciens cadres juridiques européens, notamment la directive de l'UE sur la protection des données, et établit de nouvelles obligations et responsabilités pour les entreprises qui traitent des données personnelles, et de nouveaux droits pour les individus. Les entreprises établies dans l'Union européenne, ainsi que celles qui traitent les données personnelles des résidents de l'Union européenne, doivent se conformer au RGPD.

Mise en conformité de Dropbox avec le RGPD

Dropbox s'engage à respecter le RGPD. Le respect de la confidentialité et de la sécurité est inscrit dans les gènes de Dropbox. Ainsi, malgré la croissance de nos activités, une chose est restée immuable : la façon dont nous traitons et protégeons les données que nous confient nos clients, qui est toujours au centre de nos priorités. Dropbox a toujours su rester à l'avant-garde de la conformité. Comme indiqué ci-dessus, nous avons été l'un des premiers fournisseurs de services cloud à obtenir la certification ISO 27018 pour nos utilisateurs professionnels. C'est pourquoi, pour Dropbox, la conformité avec le RGPD est la simple évolution des pratiques et contrôles déjà en place.

La mise en conformité de Dropbox avec le RGPD a commencé dès son adoption en 2016. Nous avons commencé par constituer une équipe pluridisciplinaire de spécialistes de la protection des données composée de conseillers juridiques et de professionnels de la sécurité et de la conformité, ainsi que d'ingénieurs produit et infrastructure. Notre équipe a ensuite évalué l'ensemble de nos méthodes de sécurité et de protection des données en les comparant aux exigences du RGPD. L'étape suivante a consisté à passer en revue nos modes de traitement des données personnelles et à suivre leur cycle de vie dans nos systèmes. Ces procédures sont parfois désignées sous le nom d'évaluation des données et d'études d'impact pour la protection des données.

Depuis lors, nous avons continué de miser sur nos processus internes et procédures existants afin de garantir le respect des exigences du RGPD. Ceci est important, car le RGPD nous incite fortement à documenter les décisions et pratiques qui affectent les données personnelles.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

Comment nous aidons nos clients à se mettre en conformité

Dropbox fournit des fonctionnalités de contrôle et de gestion de la visibilité qui peuvent vous aider à gérer plus facilement vos obligations en matière de protection des données, y compris celles relatives à la mise en conformité avec le RGPD. Cependant, la mise en conformité avec le RGPD au sein de votre entreprise ne dépend pas uniquement de la nature de votre relation avec vos fournisseurs tels que Dropbox. Si nos fonctionnalités peuvent vous aider à gérer vos obligations, elles ne peuvent pas garantir leur respect. La mise en conformité avec le RGPD exige une réflexion plus globale quant à la manière dont les données circulent et sont protégées au sein de votre entreprise. Chaque entreprise doit appliquer ses propres mesures en vue de la mise en conformité, les fournisseurs jouant un rôle essentiel à cet égard.

Minimisation des données

Dans le cadre du nouveau principe de protection des données dès la conception du RGPD, il est demandé aux entreprises de concevoir leurs services en limitant au maximum le volume de données collectées. Cela requiert une visibilité et un contrôle complets sur les données de votre entreprise afin d'en assurer une bonne gestion. Via le tableau de bord d'administration Dropbox, vous pouvez notamment surveiller les activités au sein des équipes, afficher les appareils connectés et contrôler les partages.

Protection et restauration des données

L'effacement à distance en cas de perte d'un appareil, l'historique des versions et la récupération des fichiers offrent une protection contre les risques de perte, de détérioration ou de destruction accidentelles de données personnelles, et peuvent rétablir la disponibilité et l'accès à ces données dans les plus brefs délais en cas d'incident. Nous encourageons par ailleurs l'activation de la validation en deux étapes pour mieux protéger vos données.

Conservation des informations

Le RGPD exige également des entreprises qu'elles conservent désormais des données détaillées sur leurs activités de traitement. Nos journaux d'audit et nos journaux d'activité vous permettent de mieux comprendre vos activités de traitement.

Gestion des accès

Le tableau de bord d'administration Dropbox vous permet de gérer facilement l'accès des membres d'équipe aux fichiers, dossiers et documents Paper. Nos différents contrôles vous permettent de protéger vos liens partagés par mot de passe, de définir des délais de validité pour accorder un accès temporaire à ces liens partagés, ou encore de limiter l'accès à ces liens aux membres de votre entreprise. En cas de changement de poste d'un membre de l'équipe, notre outil de transfert de compte permet de transférer facilement des fichiers et la propriété des documents Paper d'un utilisateur à un autre. Les administrateurs peuvent également désactiver l'accès d'un utilisateur à son compte tout en conservant ses données et relations de partage afin de protéger les données de l'entreprise. Enfin, la fonctionnalité d'effacement à distance vous permet d'effacer des fichiers et documents Paper sur les appareils perdus ou volés.

Infrastructure européenne

Même si dans la plupart des cas, le RGPD n'exige pas que les données personnelles soient hébergées au sein de l'Union européenne, Dropbox offre aux utilisateurs de Dropbox Business et de Dropbox Education la possibilité de stocker leurs fichiers (blocs) dans l'UE. Pour ce faire, nous faisons appel à l'infrastructure Amazon Web Services (AWS). Pour en savoir plus sur notre infrastructure européenne, contactez notre équipe commerciale.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.

Dropbox

Protégeons ensemble vos données personnelles

Dropbox travaille en collaboration avec ses utilisateurs afin de protéger leurs données personnelles. Nous mettons tout en œuvre pour protéger notre infrastructure, nos réseaux et nos applications, mais aussi pour former nos employés aux pratiques de sécurité et de confidentialité, bâtir une culture centrée sur notre volonté d'être dignes de confiance et soumettre nos systèmes et nos pratiques aux tests et audits externes les plus rigoureux.

Toutefois, nos clients jouent également un rôle clé dans la protection de leurs données personnelles. Dropbox vous permet de configurer, d'utiliser et de contrôler votre compte de façon à répondre aux exigences de conformité, de confidentialité et de sécurité de votre entreprise. Notre guide consacré à la responsabilité partagée peut vous permettre de mieux comprendre ce que nous faisons pour assurer la sécurité de votre compte et ce que vous pouvez faire pour bénéficier d'une visibilité et d'un contrôle adéquats sur vos données personnelles.

Résumé

Chaque jour, des millions d'utilisateurs accordent leur confiance à Dropbox. Pour être dignes de cette confiance, nous avons conçu et continuerons de développer Dropbox en mettant l'accent sur la sécurité et la confidentialité. Notre engagement à protéger les données personnelles de nos utilisateurs est au cœur de chacune de nos décisions. Pour en savoir plus, envoyez un e-mail à l'adresse privacy@dropbox.com. Pour plus d'informations sur le RGPD, consultez notre guide de préparation au RGPD.

Pour en savoir plus sur les fonctionnalités et les politiques de sécurité Dropbox, lisez le livre blanc sur la sécurité de Dropbox Business ou envoyez un e-mail à l'adresse sales@dropbox.com.