

# Privacidade e proteção de dados

## Introdução

Os dados pessoais desempenham um papel importante na sociedade e na economia. Cada vez mais, as pessoas estão buscando maior controle e clareza sobre como seus dados pessoais são usados e protegidos por organizações com as quais interagem.

No Dropbox, a confiança é a base do nosso relacionamento com milhões de pessoas e empresas ao redor do mundo. Apreciamos a confiança que você deposita em nós e assumimos a responsabilidade de proteger seus dados pessoais com seriedade.

## Nossos compromissos com você

Estamos comprometidos em proteger seus dados pessoais. Os [Termos de Serviço](#) do Dropbox descrevem suas responsabilidades ao usar nossos serviços. Nossa [Política de Privacidade](#) descreve nossos compromissos de privacidade com os usuários e explica como coletamos, usamos e tratamos seus dados pessoais quando você usa nossos serviços. Se você reside na América do Norte (Estados Unidos, Canadá e México), o Dropbox Inc. atua como seu provedor de serviços. Para todos os outros usuários, é o Dropbox International.

A Unlimited Company atua como controladora de seus dados pessoais.

Se você for usuário do Dropbox para empresas ou do Dropbox Education, sua organização atua como controladora de dados de quaisquer dados pessoais fornecidos ao Dropbox em conexão com seu uso do Dropbox para empresas ou do Dropbox Education. A controladora de dados determina o propósito e os meios de processamento de dados pessoais.

O Dropbox atua como o processador de dados, processando dados em nome de sua organização quando você usa o Dropbox para empresas ou o Dropbox Education, e nosso [Contrato do Dropbox para empresas](#) inclui compromissos relacionados a processamento de dados e transferência de dados internacional.

## Nosso registro de controle: Conformidade

A conformidade é uma maneira eficiente de validar a confiabilidade do serviço. Encorajamos e temos o prazer de fornecer verificação independente de que nossas práticas de segurança e privacidade estão em conformidade com as normas e regulamentos mais amplamente aceitos, como ISO 27001, ISO 27017, ISO 27018, ISO 27701, HIPAA/HITECH e SOC 1, 2 e 3.

Além disso, fomos um dos primeiros provedores de serviços em nuvem a obter a certificação ISO 27018, o padrão internacionalmente reconhecido para práticas líderes em privacidade de nuvem e proteção de dados. Nossos auditores terceirizados independentes testam nossos controles e fornecem seus relatórios e opiniões. Poderemos compartilhá-los com vocês, sempre que possível. Observe que, enquanto o escopo de nossas certificações

e relatórios de auditoria normalmente se referem ao Dropbox para empresas e ao Dropbox Education, a maioria de nossos controles são aplicáveis para os usuários do Dropbox Basic, Plus e Professional. Além disso, o Dropbox agora adere ao Código de conduta em nuvem da UE. Mais informações sobre as normas com as quais estamos em conformidade e como verificamos nossas práticas podem ser encontradas em nossa [página na web de conformidade](#).

# Arquitetura do Dropbox: Protegendo seus dados pessoais

No Dropbox, acreditamos que proteger seus dados pessoais começa com a manutenção de seus dados em segurança. O Dropbox é projetado com múltiplas camadas de proteção, incluindo transferência segura de dados de arquivo, criptografia e controles em nível de aplicativo, que são distribuídos através de uma infraestrutura segura e escalável.

## Nossa infraestrutura: Arquivos

A infraestrutura do Dropbox para arquivos é composta dos componentes descritos no diagrama abaixo.



## Servidores de metadados

Algumas informações básicas sobre dados de usuário, chamadas metadados, são mantidas em seu próprio serviço de armazenamento independente e funcionam como um índice para os dados das contas de usuários. Os metadados incluem informações básicas sobre a conta e o usuário, como endereço de e-mail, nome e nomes de dispositivos. Também incluem informações básicas sobre arquivos, inclusive nomes e tipos de arquivos, o que ajuda a viabilizar recursos como histórico de versões, recuperação e sincronização.

## Bancos de dados de metadados

Os metadados de arquivos são armazenados em serviços de banco de dados baseado em MySQL e são fragmentados e replicados conforme necessário para atender aos requisitos de desempenho e alta disponibilidade.

## Servidores em bloco

Por definição, o Dropbox oferece um mecanismo exclusivo de segurança que vai além da criptografia tradicional para proteger os dados de usuários. Os servidores em bloco processam arquivos dos aplicativos do Dropbox dividindo-os em blocos, criptografando cada bloco de arquivos usando uma cifra forte e sincronizando somente blocos que foram modificados entre as revisões. Quando um aplicativo do Dropbox detecta um novo arquivo ou alterações em um arquivo existente, o aplicativo notifica os servidores em bloco sobre a alteração e os blocos de arquivos novos ou modificados são processados e transferidos para os servidores de armazenamento.

## Servidores de armazenamento em bloco

O conteúdo real dos arquivos dos usuários é armazenado em blocos criptografados nos servidores de armazenamento em bloco. Antes da transmissão, o cliente do Dropbox separa os arquivos em blocos para prepará-los para o armazenamento. Os servidores de armazenamento em bloco funcionam como um sistema de Armazenamento de Conteúdo Endereçável (CAS), e cada bloco de arquivo criptografado individualmente é recuperado com base no seu valor de hash.

## Servidores de visualizações prévias

Os servidores de visualizações prévias são responsáveis pela criação de visualizações prévias de arquivos. A visualização prévia é uma renderização de um arquivo de usuário em um formato diferente, mais adequado para apresentação rápida em um dispositivo de usuário final. Os servidores de visualizações prévias recuperam blocos de arquivo dos servidores de armazenamento em bloco para gerar as visualizações prévias. Quando a visualização prévia de um arquivo é solicitada, os servidores de visualizações prévias recuperam a visualização prévia no cache de servidores de armazenamento de visualizações prévias anteriores e a transferem para os servidores em bloco. A visualização prévia é, então, mostrada para o usuário pelos servidores em bloco.

## Servidores de armazenamento de visualizações prévias

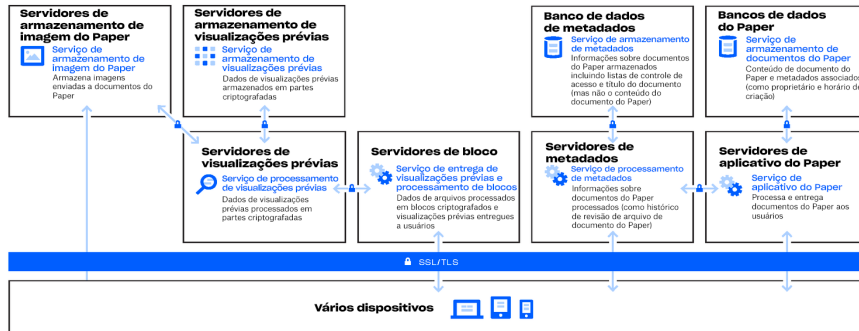
As visualizações prévias no cache estão armazenadas em um formato criptografado nos servidores de armazenamento de visualizações prévias.

## Serviço de notificações

Esse serviço separado monitora se houve ou não alterações nas contas do Dropbox. Nenhum arquivo ou metadado é armazenado aqui ou transferido para cá. Cada cliente estabelece uma conexão Long Poll com o serviço de notificação e aguarda. Quando ocorre alguma alteração em um arquivo no Dropbox, o serviço de notificação sinaliza uma mudança para os clientes relevantes, fechando a conexão Long Poll. O encerramento da conexão indica que o cliente deve se conectar aos Servidores de metadados de forma segura para sincronizar as alterações.

## Nossa infraestrutura: Paper

O Dropbox Paper (Paper) é um recurso do produto Dropbox. No entanto, o Paper usa um conjunto mais distinto de sistemas dentro do ambiente da infraestrutura do Dropbox. A infraestrutura do Paper é composta dos componentes descritos no diagrama abaixo.



### Servidores de aplicativos do Paper

Os servidores de aplicativos do Paper processam solicitações de usuários, renderizam a saída de documentos editados do Paper de volta ao usuário e operam serviços de notificação. Os servidores de aplicativos do Paper gravam edições de entrada do usuário nos bancos de dados do Paper, onde são colocadas em armazenamento persistente. As sessões de comunicação entre os servidores de aplicativos do Paper e os bancos de dados do Paper são criptografadas com cifras fortes.

### Bancos de dados do Paper

O conteúdo real de documentos do Paper dos usuários, bem como determinados metadados sobre esses documentos, são criptografados em armazenamento persistente nos bancos de dados do Paper. Isso inclui informações sobre um documento do Paper (como o título, associação e permissões, associações de pastas e projetos e outras informações), bem como o conteúdo do próprio documento do Paper, incluindo comentários e tarefas. Os bancos de dados do Paper são fragmentados e replicados conforme necessário para atender aos requisitos de desempenho e alta disponibilidade.

### Servidores de armazenamento de imagem do Paper

As imagens transferidas para os documentos do Paper são armazenadas e criptografadas em repouso nos servidores de imagem do Paper. A transmissão de dados de imagem entre o aplicativo do Paper e os servidores de imagem do Paper ocorre sobre uma sessão criptografada.

### Servidores de visualizações prévias

Os servidores de visualizações prévias produzem visualizações prévias tanto para as imagens enviadas para os documentos do Paper quanto para os hiperlinks incorporados aos documentos do Paper. Para as imagens transferidas para os documentos do Paper, os servidores de visualizações prévias buscam dados de imagem armazenados nos servidores de armazenamento de imagem do Paper, por meio de um canal criptografado. Para os hiperlinks incorporados aos documentos do Paper, os servidores de visualizações prévias buscam dados de imagens e fazem a renderização da visualização prévia, usando criptografia como especificado no link de origem. A visualização prévia é, então, mostrada para o usuário pelos servidores em bloco.

### Servidores de armazenamento de visualizações prévias

O Paper usa os mesmos servidores de armazenamento de visualizações prévias descritos no diagrama da infraestrutura do Dropbox para armazenar visualizações prévias do cache. Os blocos de visualizações prévias no cache são armazenados em um formato criptografado nos servidores de armazenamento de visualizações prévias.

# Controles do Dropbox: Nossas práticas internas

Tomamos medidas abrangentes para proteger nossa infraestrutura, rede e aplicativos. Algumas das medidas de segurança que temos em vigor incluem criptografia em repouso, criptografia em trânsito e exclusão permanente de arquivos. Também oferecemos treinamento robusto em privacidade e segurança para todos os nossos funcionários para construir uma cultura onde ser digno de confiança é uma prioridade. Detalhes de alguns de nossos controles estão descritos abaixo:

## Treinamento

Parte de manter os dados pessoais de nossos usuários seguros envolve cultivar e desenvolver uma cultura de conscientização de segurança e privacidade. Os colaboradores do Dropbox precisam concordar com as políticas de segurança, incluindo uma política de privacidade dos dados do usuário, antes de receber o acesso aos sistemas. Apenas os funcionários com uma necessidade específica têm acesso a esses sistemas. Os funcionários também participam anualmente do treinamento obrigatório de segurança e privacidade.

## Criptografia em trânsito

Para proteger dados de arquivos em trânsito entre um cliente Dropbox (atualmente desktop, dispositivo móvel, API ou web) e os servidores front-end do Dropbox, uma conexão criptografada é negociada para garantir uma entrega segura. Do mesmo modo, uma conexão criptografada é negociada para proteger os dados dos documentos do Paper em trânsito entre um cliente Paper (atualmente dispositivo móvel, API ou web) e os serviços hospedados. Essas conexões são criptografadas usando Secure Sockets Layer (SSL)/Transport Layer Security (TLS) para criar um túnel seguro protegido por padrões de criptografia Advanced Encryption Standard (AES) de 128 bits ou superior.

## Criptografia em repouso

Arquivos transferidos por usuários são armazenados nos servidores de armazenamento do Dropbox como blocos de arquivos independentes. Cada bloco é criptografado usando o padrão de criptografia Advanced Encryption Standard (AES) de 256 bits.

Apenas blocos que foram modificados entre as revisões são sincronizados. Do mesmo modo, os dados de documentos do Paper armazenados nos bancos de dados do Paper também são criptografados em repouso usando o padrão de criptografia Advanced Encryption Standard (AES) de 256 bits.

## Exclusão permanente de arquivos e documentos do Paper

Quando um usuário do Dropbox ou um administrador de uma equipe do Dropbox para empresas ou do Dropbox Education marca um arquivo para exclusão permanente, ele aciona um processo para excluir permanentemente o arquivo. Da mesma forma, quando um usuário ou um administrador de uma equipe do Dropbox para empresas ou do Dropbox Education marca um documento do Paper para exclusão permanente, há um processo semelhante para excluir permanentemente os dados de imagem e os dados do documento do Paper.

## Solicitações de acesso a dados pessoais

Para acessar dados pessoais além dos arquivos e documentos do Paper armazenados no Dropbox, os usuários podem acessar o site e ir para a [página de conta](#). A página da conta mostrará informações como o nome e o endereço de e-mail associados à conta. Os usuários também podem visualizar os endereços IP de sessões conectadas, computadores e dispositivos móveis; bem como aplicativos conectados às contas deles na [página de segurança](#) e da [página de aplicativos conectados](#).

Os usuários do Dropbox também têm a opção de solicitar acesso ou exclusão de outros dados pessoais que o Dropbox possa ter coletado sobre eles. Mais informações sobre esse processo podem ser encontradas na [Central de ajuda](#) do Dropbox.

## Governança de privacidade no Dropbox

A equipe de privacidade é responsável por operar o Programa de privacidade do Dropbox. Ela implementa nossas principais iniciativas de privacidade e defende a privacidade desde o início em nosso ciclo de vida de dados. O Programa de privacidade do Dropbox é ainda apoiado por várias subequipes jurídicas multifuncionais. Essas subequipes fornecem a experiência adicional necessária para operar e supervisionar as tarefas diárias do Programa de privacidade.

A equipe do DPO (do inglês Data Protection Officer, responsável pela proteção dos dados) opera separadamente das outras funções de privacidade e serve como conformidade e supervisão da privacidade, apoiando diretamente o responsável pela proteção de dados na execução de suas funções. O responsável pela proteção de dados pode ser contatado em [privacy@dropbox.com](mailto:privacy@dropbox.com).



## Princípios de solicitação

### de dados do governo

Entendemos que quando os usuários confiam a nós seus dados pessoais, esperam que nós mantenhamos esses dados confidenciais. Como a maioria dos serviços on-line, o Dropbox algumas vezes recebe solicitações de governos procurando informações sobre seus usuários.

Os princípios abaixo descrevem como lidamos com as solicitações de dados que recebemos do governo.

### Praticar a transparência

Acreditamos que os serviços on-line devem ter permissão para publicar o número e os tipos de solicitações recebidas do governo e para notificar as pessoas quando informações sobre elas forem solicitadas. Esse tipo de transparência capacita os usuários ajudando-os a entender melhor instâncias e

padrões de alcance do governo. Continuaremos a publicar informações detalhadas sobre essas solicitações e defender o direito de fornecer mais dessas importantes informações.

### Combater solicitações excessivamente abrangentes

As solicitações de dados por parte do governo devem ser limitadas a informações necessárias e estritamente ajustadas a pessoas específicas e investigações legítimas. Recusaremos solicitações excessivamente abrangentes.

### Oferecer serviços confiáveis

Os governos nunca deveriam instalar backdoors em serviços on-line ou comprometer a infraestrutura desses serviços para obter dados de usuários. Vamos continuar nos esforçando para proteger nossos sistemas e mudar as leis a fim de deixar clara a ilegalidade desse tipo de atividade.

### Proteger todos os usuários

Leis que dão às pessoas proteções diferentes com base em onde elas vivem ou sua cidadania são antiquadas e não refletem a natureza global dos serviços on-line. Continuaremos a defender a reforma dessas leis.

Esses princípios, juntamente com nosso relatório anual de transparência, ficam disponíveis ao público no site do Dropbox em: <https://www.dropbox.com/transparency>.

Para mais detalhes sobre nossos controles e nossa abordagem para proteger seus dados pessoais, consulte nosso [white paper Segurança do Dropbox para empresas](#).

## Outras pessoas trabalhando para e com o Dropbox

O Dropbox gerencia a maioria das atividades relacionadas ao provisionamento de nossos serviços; no entanto, utilizamos alguns terceiros confiáveis em relação aos nossos serviços (por exemplo, provedores de atendimento ao cliente e serviços de TI). Esses terceiros somente acessarão suas informações para realizar as tarefas em nosso nome em conformidade com nossa [Política de Privacidade](#), e nós permaneceremos responsáveis pela manipulação que eles fizerem de suas informações de acordo com nossas instruções.

Cada terceiro passa por um rigoroso processo de verificação, incluindo revisões de segurança e privacidade e revisões contratuais regulares, para avaliar sua capacidade de cumprir nossos compromissos de proteção de dados. Com base nesse processo de verificação, o Dropbox afirma que seus terceiros confiáveis se comprometem a cumprir a Lei de Proteção de Dados da UE aplicável em relação ao processamento de dados pessoais em nome do Dropbox. Os clientes podem monitorar os terceiros confiáveis do Dropbox, analisando as certificações ISO 27001 e 27018 do Dropbox e, sob

obrigações apropriadas de confidencialidade, revisando o relatório SOC 2 Tipo II do Dropbox. Em particular, os clientes podem monitorar terceiros confiáveis do Dropbox examinando os controles e os resultados da auditoria do Dropbox para os Critérios de Serviços de Confiança P6.1, P6.4 e CC.9.2 do Relatório SOC 2 Tipo II.

## Transferências de dados internacionais

Ao transferir dados da União Europeia, do Espaço Econômico Europeu, do Reino Unido e da Suíça, o Dropbox depende de uma variedade de mecanismos legais, como contratos com nossos clientes e afiliados, Cláusulas contratuais padrão e decisões de adequação da Comissão Europeia sobre determinados países, conforme aplicável.

O Dropbox está em conformidade com os Data Privacy Frameworks (padrões de privacidade de dados) entre União Europeia-EUA e Suíça-EUA, bem como a

Extensão do Reino Unido ao Data Privacy Framework entre União Europeia-EUA, conforme estabelecido pelo Departamento de Comércio dos EUA, referentes ao processamento de dados pessoais transferidos da União Europeia, da Área Econômica Europeia, do Reino Unido e da Suíça para os Estados Unidos. O Dropbox certificou ao Departamento de Comércio dos EUA que adere aos Data Privacy Frameworks com relação a esses dados, mas isso não inclui as partes dos Serviços referentes

ao DocSend nem ao Formswift.

Para saber mais sobre o Data Privacy Framework e visualizar a certificação do Dropbox, acesse [www.dataprivacyframework.gov](http://www.dataprivacyframework.gov).

Reclamações e disputas relacionadas à nossa conformidade com o Data Privacy Framework são investigadas e resolvidas através da JAMS, uma empresa terceira independente. Para saber mais, consulte nossa [Política de Privacidade](#).

## GDPR: Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados, ou GDPR, é um regulamento da UE que estabelece uma nova estrutura legal para proteção de dados pessoais de titulares de dados da UE. O GDPR é a legislação europeia de proteção de dados mais significativa desde a Diretiva de Proteção de Dados da UE (EU Data Protection Directive) de 1995, e muitas empresas, incluindo o

Dropbox, que fazem negócios na Europa, investiram intensivamente na conformidade com o GDPR. O GDPR harmoniza as leis de proteção de dados em toda a Europa e as atualiza com a rápida mudança tecnológica que ocorreu nas últimas duas décadas. Ele foi desenvolvido sobre as estruturas legais anteriores na UE, incluindo a Diretiva de Proteção de Dados da UE, e introduziu novas

obrigações e responsabilidades para as empresas que manipulam dados pessoais, bem como novos direitos para os indivíduos em relação a seus dados pessoais. As organizações estabelecidas na UE, bem como as organizações que processam dados pessoais de titulares de dados da UE, são obrigadas a cumprir o GDPR.

## A jornada do Dropbox rumo à conformidade com o GDPR

O Dropbox está comprometido com a conformidade ao GDPR. O respeito à privacidade e à segurança sempre esteve presente em nossos negócios desde o início e, conforme crescemos, nosso foco em manipular e proteger os dados que nossos clientes nos confiam continua sendo nossa prioridade. O Dropbox tem um histórico de estar à frente na curva da conformidade, conforme descrito acima, fomos um dos primeiros provedores de serviços de nuvem a conquistar a certificação ISO 27018 para nossos usuários empresariais. Devido a essa base sólida, o Dropbox vê a conformidade com o GDPR como uma evolução das práticas e controles já existentes e representa um conjunto contínuo e evolutivo de iniciativas para garantir que os dados pessoais de nossos usuários

estejam sempre protegidos. A jornada do Dropbox rumo à conformidade com o GDPR começou assim que o regulamento foi adotado em 2016. Nosso primeiro passo foi formar uma equipe multifuncional de especialistas em proteção de dados consistindo em consultores jurídicos, profissionais de segurança e conformidade e engenheiros de produto e infraestrutura. Nossa equipe, então, conduziu uma ampla avaliação de nossas práticas atuais de segurança e proteção de dados em relação aos requisitos do GDPR.

Nosso próximo passo foi realizar uma avaliação de nossas atividades de processamento de dados pessoais e traçar o ciclo de vida dos dados pessoais em nossos sistemas. Esses exercícios

algumas vezes são chamados de realização de Mapeamentos de dados e conclusão de Avaliações de Impacto de Proteção de Dados.

Desde então, continuamos a desenvolver nossos processos e procedimentos internos existentes para garantir o cumprimento dos princípios de prestação de contas de acordo com as exigências do GDPR, incluindo a manutenção de registros de processamento de acordo com o Artigo 30 do GDPR. Isso é importante, pois o GDPR coloca um foco maior nas decisões de documentação e práticas que afetam dados pessoais.

# Capacitação de nossos usuários em suas jornadas rumo à conformidade com o GDPR

O Dropbox fornece recursos de controle e visibilidade que podem ajudar você a gerenciar suas obrigações de proteção de dados, incluindo as obrigações de conformidade com o GDPR, mais facilmente. Claro, a conformidade com o GDPR em sua organização não começa nem termina com o relacionamento com seus fornecedores, como o Dropbox. Embora nossos recursos possam ajudar você a gerenciar suas obrigações, eles não podem garantir a conformidade por si mesmos. A conformidade com o GDPR requer pensar de modo mais amplo sobre como os dados circulam e são protegidos em sua organização. Cada organização deve dar seus próprios passos para entrar em conformidade, sendo os fornecedores parceiros importantes nessa jornada.

## Minimização de dados

Um elemento importante do requisito de Privacidade como padrão do GDPR é que as organizações devem projetar seus serviços de coleta de dados de forma minimizada. Isso significa ter boa visibilidade e controle dos dados em sua organização para poder gerenciá-los. O console do Dropbox para empresas é uma ferramenta útil para ajudar nessa empreitada, já que habilita você a monitorar a atividade da equipe, visualizar dispositivos conectados e auditar a atividade de compartilhamento.

Trabalhamos para incorporar os princípios de Privacidade como padrão em novos produtos e recursos.

## Proteção e restauração de dados

A proteção de dispositivos perdidos, o histórico de versões e a recuperação de arquivos podem ajudar você a se proteger contra perda acidental, dano ou destruição de dados pessoais e podem ajudar você também com a capacidade de restaurar a disponibilidade dos, e o acesso aos, dados pessoais de modo oportuno no caso de um incidente. A autenticação em dois passos é outra medida importante que encorajamos para ajudar na proteção de seus dados.

## Manutenção de registros

O GDPR também aumenta as obrigações das organizações de manter registros detalhados de suas atividades de processamento. Nossos registros de auditoria e nossos registros de atividade podem ajudar no melhor entendimento de suas atividades de processamento para atender sua manutenção de registros.

## Administração de acesso

No console do Dropbox, você gerencia facilmente o acesso de membros da equipe a arquivos, pastas e documentos do Paper. Para links de arquivos compartilhados, nosso recurso de permissões de link permite que você proteja os links compartilhados com senha, defina datas de validade para conceder acesso temporário e limite o acesso àqueles em sua organização. No caso de as responsabilidades mudarem entre usuários, nossa ferramenta de transferência de conta permite que você transfira facilmente arquivos e propriedade de documentos do Paper de um usuário para outro.

Os administradores também têm a capacidade de desativar o acesso de um

usuário à sua conta, preservando seus dados e compartilhando relacionamentos para manter as informações da sua organização seguras. Por fim, o recurso de exclusão remota permite que você exclua arquivos e documentos do Paper de dispositivos perdidos ou roubados.

## Infraestrutura da UE

Embora o GDPR não exija que dados pessoais sejam hospedados na UE, o Dropbox oferece aos clientes qualificados do Dropbox para empresas e do Dropbox Education a capacidade de armazenar arquivos (blocos) na UE. O armazenamento de arquivos baseado na UE é fornecido na infraestrutura da Amazon Web Services (AWS). Para saber mais sobre nossa infraestrutura da UE, [entre em contato com nossa equipe de vendas](#).



# Trabalho em conjunto para proteção de seus dados pessoais

O Dropbox trabalha com seus usuários para proteger seus dados pessoais. Tomamos medidas amplas para proteger nossa infraestrutura, rede e aplicativos, treinamos colaboradores com práticas de segurança e privacidade, construímos uma cultura em que ser digno de confiança é a maior prioridade e submetemos nossos

sistemas e práticas a rigorosos testes e auditorias de terceiros.

No entanto, os usuários também desempenham um papel fundamental na proteção de seus dados pessoais. O Dropbox permite que você configure, use e monitore sua conta de maneiras que atendam às necessidades de privacidade,

segurança e conformidade da sua organização. Nosso [guia de responsabilidade compartilhada](#) pode ajudar você a entender mais sobre o que fazemos para manter sua conta segura e o que você pode fazer para manter a visibilidade e o controle sobre seus dados pessoais.

## Resumo

Todos os dias, milhões de usuários depositam sua confiança no Dropbox. Para sermos merecedores dessa confiança, criamos e continuaremos a ampliar o Dropbox com ênfase na segurança e na privacidade. Nosso compromisso em proteger os dados pessoais de nossos usuários está no cerne de cada decisão que tomamos. Para mais informações, envie um e-mail para [privacy@dropbox.com](mailto:privacy@dropbox.com). Para mais informações sobre o GDPR, você também pode acessar nosso [centro de orientação sobre o GDPR](#).