

Privacidade e proteção de dados

Introdução

Dados pessoais são importantíssimos, tanto na sociedade quanto na economia. Cada vez mais, as pessoas buscam maior controle e clareza sobre como seus dados pessoais são usados e protegidos pelas 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 nossos usuários e explica como coletamos, usamos e lidamos com seus dados pessoais quando você usa nossos serviços. Se você reside na América do Norte (Estados Unidos, Canadá e México), a Dropbox, Inc. atua como seu provedor de serviços.

Para todos os outros usuários, a Dropbox International Unlimited Company age como um controlador de seus dados pessoais.

Se você é um usuário do Dropbox Business ou do Dropbox Education, sua organização atua como o controlador de dados para quaisquer dados pessoais fornecidos ao Dropbox em conexão com o uso do Dropbox Business ou do Dropbox Education. O controlador de dados

determina os propósitos e meios de processamento de dados pessoais. O Dropbox age como o processador de dados, processando dados em nome da sua organização quando você usa o Dropbox Business ou o Dropbox Education, e nosso [Acordo de negócios](#) inclui compromissos relacionados ao processamento de dados e de transferência de dados internacionais.

Nosso registro de rastreo: conformidade

Conformidade é uma forma eficaz de validar a confiabilidade de um 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, HIPAA/HITECH, Alemanha BSI C5 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. Podemos compartilhá-los com você sempre que possível.

Observe que, embora o escopo de nossas certificações e relatórios de auditoria geralmente se refira ao Dropbox Business e ao Dropbox Education, a maioria dos nossos controles também é aplicável aos usuários do Dropbox Basic, Plus e Professional. Mais informações sobre os padrões que cumprimos e como verificamos nossas práticas podem ser encontradas em nossa [página da web de conformidade](#).

Arquitetura do Dropbox: protegendo seus dados pessoais

No Dropbox, acreditamos que para proteger seus dados pessoais precisamos mantê-los em segurança. Para esse fim, o Dropbox é projetado com várias camadas de proteção, incluindo transferência segura de dados de arquivos, criptografia e controles em nível de aplicativo distribuídos em uma infraestrutura escalonável e segura.

Nossa infraestrutura: arquivos

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



Servidores de metadados

Determinadas informações básicas sobre os dados do usuário, chamadas metadados, são mantidas em serviço de armazenamento discreto próprio e atuam como um índice para os dados nas contas dos usuários. Os metadados incluem informações básicas sobre contas e usuários, como endereço de e-mail, nome e nomes de dispositivos. Os metadados também incluem informações básicas sobre arquivos, incluindo nomes e tipos de arquivos, que ajudam a dar suporte a recursos como histórico de versões, recuperação e sincronização.

Bancos de dados de metadados

Esses metadados de arquivo são armazenados em um serviço de banco de dados baseado em MySQL e são fragmentados e replicados conforme necessário para atender a requisitos de desempenho e alta disponibilidade.

Servidores de bloco

Desde a concepção, o Dropbox fornece um mecanismo de segurança único que vai além da criptografia tradicional para proteger dados do usuário. Servidores de bloco processam arquivos dos aplicativos Dropbox dividindo cada arquivo em blocos, que são criptografados usando uma cifra forte e sincronizando apenas os blocos que foram modificados entre as revisões. Quando um aplicativo Dropbox detecta um novo arquivo ou alterações em um arquivo existente, o aplicativo informa os servidores de arquivos sobre a mudança e os blocos de arquivo novos ou modificados são processados e transferidos para o servidor de armazenamento.

Servidores de armazenamento de blocos

O conteúdo real dos arquivos dos usuários é armazenado em blocos criptografados com os servidores de armazenamento de blocos. Antes da transmissão, o cliente Dropbox divide os arquivos em blocos de arquivos em preparação para o armazenamento. Os Servidores de armazenamento de blocos funcionam como um sistema CAS (Content-Addressable Storage), com cada bloco de arquivo criptografado individual recuperado com base em seu valor de hash.

Servidores de visualização prévia

Os Servidores de visualização prévia são responsáveis por produzir visualizações prévias de arquivos. As visualizações prévias são uma renderização do arquivo de um usuário em um formato de arquivo diferente, mais adequado para exibição rápida no dispositivo de um usuário final. Servidores de visualização prévia recuperam blocos de arquivos dos Servidores de armazenamento de blocos para gerar visualizações prévias. Quando a visualização prévia de um arquivo é solicitada, os servidores de visualização prévia recuperam a visualização em cache dos servidores de armazenamento de visualização prévia e a transferem para os servidores de bloco. As visualizações são enfim apresentadas aos usuários pelos servidores de bloco.

Servidores de armazenamento de visualização prévia

As visualizações prévias em cache são armazenadas em um formato criptografado nos Servidores de armazenamento de visualizações prévias.

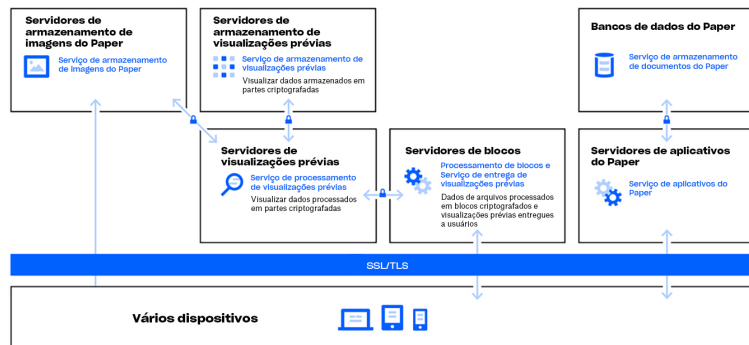
Serviço de notificação

Esse serviço separado é dedicado a monitorar 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 de qualquer 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 de sistemas predominantemente distinto no ambiente de infraestrutura do Dropbox. A infraestrutura do Paper é composta de componentes descritos no diagrama abaixo.



Servidores de aplicativo do Paper

Os servidores de aplicativo do Paper processam as solicitações dos usuários, bem como a saída de documentos do Paper editados de volta para os usuários e executam os serviços de notificação. Os servidores de aplicativo do Paper gravam as edições de usuários de entrada nos bancos de dados do Paper, onde são colocadas em armazenamento contínuo. As sessões de comunicação entre os servidores de aplicativo do Paper e os bancos de dados do Paper são criptografadas usando uma cifra forte.

Bancos de dados do Paper

O conteúdo real dos documentos do Paper dos usuários, bem como certos metadados sobre esses documentos, são criptografados em armazenamento contínuo nos bancos de dados do Paper. Isso inclui informações sobre um documento do Paper (como o título, assinatura e permissões compartilhadas, associações em pastas e projetos e outras informações), bem como o conteúdo no próprio documento do Paper, incluindo comentários e tarefas. Os bancos de dados do Paper são fragmentados e replicados conforme necessário para atender a requisitos de desempenho e alta disponibilidade.

Servidores de armazenamento de imagens do Paper

Imagens enviadas para documentos do Paper são armazenadas e criptografadas em repouso nos servidores de imagem do Paper. A transmissão dos dados de imagem entre o aplicativo do Paper e os servidores de imagem do Paper ocorre em uma sessão criptografada.

Servidores de visualização prévia

Os Servidores de visualização prévia produzem visualizações prévias de imagens enviadas a documentos do Paper, bem como hiperlinks incorporados em documentos do Paper. Para imagens enviadas a documentos do Paper, os Servidores de visualização prévia buscam dados de imagem armazenados nos Servidores de armazenamento de imagens do Paper por meio de um canal criptografado. Para hiperlinks incorporados em documentos do Paper, os Servidores de visualização prévia buscam os dados da imagem e renderizam uma visualização prévia da imagem usando criptografia, conforme especificado pelo link da origem. As visualizações são enfim apresentadas aos usuários pelos servidores de bloco.

Servidores de armazenamento de visualização prévia

O Paper usa os mesmos servidores de armazenamento de visualização prévia descritos no diagrama de infraestrutura do Dropbox para armazenar visualizações prévias de imagens em cache. As visualizações prévias em cache são armazenadas 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 a exclusão permanente de arquivos. Também oferecemos treinamento robusto de privacidade e segurança para todos os nossos funcionários, visando o desenvolvimento de uma cultura em que ser digno de confiança seja uma prioridade. Detalhes de alguns dos nossos controles estão descritos abaixo:

Treinamento

Parte da proteção dos dados pessoais de nossos usuários envolve a construção e o desenvolvimento de uma cultura de conscientização sobre segurança e privacidade. Os funcionários do Dropbox são obrigados a concordar com as políticas de segurança, incluindo uma política de privacidade de dados do usuário, antes de receber acesso aos sistemas. Somente os funcionários com necessidades específicas têm acesso a esses sistemas.

Os funcionários também participam de treinamentos obrigatórios de segurança e privacidade anualmente.

Criptografia de dados em trânsito

Para proteger os 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 a entrega segura. Da mesma forma, uma conexão criptografada é negociada para proteger os dados de documentos do Paper em trânsito entre um cliente do Paper (atualmente dispositivo móvel, API ou web) e o serviço hospedado. Essas conexões são criptografadas usando SSL (Secure Sockets Layer)/TLS (Transport Layer Security) para criar um túnel seguro protegido por criptografia AES (Advanced Encryption Standard) de 128 bits ou superior.

Criptografia de dados em repouso

Os arquivos enviados pelos usuários são armazenados nos Servidores de armazenamento do Dropbox como blocos de arquivos discretos. Cada bloco é criptografado usando a criptografia AES (Advanced Encryption Standard) de 256 bits. Somente blocos que foram modificados entre as revisões são

sincronizados. Da mesma forma, os dados de documentos do Paper armazenados em bancos de dados do Paper também são criptografados em repouso usando a criptografia AES (Advanced Encryption Standard) de 256 bits.

Exclusão permanente de arquivos e documentos do Paper

Quando um usuário do Dropbox ou um administrador de uma equipe do Dropbox Business 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 Business 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 acesso a dados pessoais além dos arquivos e documentos do Paper armazenados no Dropbox, os usuários podem entrar no site e acessar as [páginas](#) de sua conta. A página da conta mostrará informações como o nome e endereço de e-mail associado à conta. Os usuários também podem visualizar os endereços IP de sessões, computadores e dispositivos móveis conectados, bem como os aplicativos conectados a suas contas na página de segurança e na [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 do Programa de privacidade é responsável pela operação do Programa de privacidade do Dropbox. Ele implementa nossas principais iniciativas de privacidade e protege a privacidade desde a concepção em nosso ciclo de vida de dados. O Programa de privacidade do Dropbox é ainda apoiado por várias subequipes jurídicas multifuncionais. Essas subequipes fornecem o conhecimento adicional necessário para operar e supervisionar as tarefas diárias do Programa de privacidade.

A equipe do DPO opera separadamente das outras funções de privacidade e atua na conformidade e supervisão da privacidade, apoiando diretamente o DPO (responsável pela proteção de dados) no cumprimento de suas funções. O DPO é o representante local da UE e pode ser contatado em privacy@dropbox.com.



Princípios de solicitação de dados pelo governo

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

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

Ser transparente

Para nós os serviços on-line deveriam ter permissão de publicar a quantidade e os tipos de solicitações governamentais que recebem, e de notificar os indivíduos quando informações sobre eles são solicitadas. Esse tipo de transparência fortalece os usuários, permitindo que entendam melhor instâncias e padrões que

ultrapassam os limites governamentais. Continuaremos a publicar informações detalhadas sobre essas solicitações e a defender o direito de fornecer mais informações importantes desse tipo.

Recusar solicitações muito abrangentes

As solicitações de dados pelo governo deveriam ser limitadas às informações buscadas e centradas em pessoas específicas e investigações legítimas.

Resistiremos a solicitações muito abrangentes.

Oferecer serviços confiáveis

Os governos nunca devem instalar backdoors em serviços on-line ou comprometer a infraestrutura para obter os dados do usuário.

Continuaremos 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 oferecem às pessoas diferentes proteções, dependendo do local onde vivem ou qual 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 o nosso relatório anual de transparência, são disponibilizados publicamente no site do Dropbox em:

<https://www.dropbox.com/transparency>.

Para obter detalhes adicionais sobre nossos controles e nossa abordagem para proteger seus dados pessoais, consulte nosso [Whitepaper de Segurança do Dropbox Business](#).

Outros trabalhando para e com o Dropbox

O Dropbox gerencia a maioria das atividades relacionadas à prestação 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 tarefas em nosso nome em conformidade com nossa [Política de privacidade](#) e continuaremos responsáveis pelo tratamento de suas informações de acordo com nossas instruções.

Cada terceiro passa por um rigoroso processo de verificação, incluindo revisões de segurança e revisões contratuais regulares, para avaliar sua capacidade de cumprir nossos compromissos de proteção de dados.

Transferências de dados internacionais

O Dropbox conta com uma variedade de mecanismos legais para a sua transferência internacional de dados pessoais da UE para os Estados Unidos. Somos certificados nas políticas dos Privacy Shield Programs entre

UE-EUA e Suíça-EUA no que se refere à coleta, ao uso e à retenção de dados pessoais e a transferência dos mesmos da UE e da Suíça para os Estados Unidos. Além do Privacy Shield, o Dropbox também fornece fortes garantias contratuais em

torno da privacidade de seus serviços e implementou cláusulas contratuais-modelo da UE para cobrir suas transferências internacionais de dados.

RGPD: o Regulamento Geral de Proteção de Dados

O Regulamento Geral de Proteção de Dados, ou GDPR, é um regulamento da UE (União Europeia) que estabelece estrutura jurídica para proteção de dados pessoais de titulares de dados da UE.

O RGPD é a peça mais importante da legislação europeia de proteção de dados desde a Diretiva de Proteção de Dados de 1995 da UE, e muitas empresas, inclusive o Dropbox, que fazem negócios na Europa investiram pesadamente na conformidade com o RGPD.

O RGPD harmoniza as leis de proteção de dados em toda a Europa e as atualiza em relação às rápidas mudanças tecnológicas que ocorreram nas últimas duas décadas.

Baseia-se em estruturas jurídicas passadas da UE, incluindo a Diretiva de Proteção de Dados da UE, e introduz novas obrigações e responsabilidades para as organizações que lidam com dados pessoais, bem como novos direitos para os indivíduos em relação aos seus dados pessoais.

As organizações estabelecidas na UE, bem como as organizações que processam dados pessoais de titulares de dados da UE, devem cumprir o RGPD.

Jornada do Dropbox no cumprimento do GDPR

O Dropbox está comprometido com a conformidade com o RGPD. O respeito pela privacidade e segurança foi incorporado em nossos negócios desde o início e, conforme crescemos, nosso foco no tratamento e na proteção dos dados que nossos usuários confiam a nós continua sendo uma prioridade. O Dropbox tem um histórico de estar à frente da curva de conformidade, como descrito acima, fomos um dos primeiros provedores de serviços em nuvem a obter a certificação ISO 27018 para nossos usuários corporativos. Devido a essa sólida base, o Dropbox considera a conformidade com o RGPD uma evolução de nossas práticas e controles existentes e representa um conjunto de iniciativas em constante evolução para garantir que os dados pessoais de nossos usuários estejam sempre protegidos.

A jornada do Dropbox rumo à conformidade com o RGPD começou assim que o regulamento foi adotado em 2016. Nosso primeiro passo foi criar uma equipe multifuncional de especialistas em proteção de dados, formada por um conselho jurídico, profissionais de segurança e conformidade e engenheiros de produto e de infraestrutura. Nossa equipe, então, concluiu uma avaliação completa de nossas práticas atuais de segurança e proteção de dados em relação aos requisitos do RGPD.

Nosso próximo passo foi realizar uma avaliação de nossas atividades de processamento de dados pessoais e rastrear o ciclo de vida de dados pessoais em nossos sistemas. Esses exercícios são por vezes referidos como execução de Mapeamentos de dados e conclusão de Avaliações de impacto de proteção de dados

Mapeamentos de dados e preenchimento de Avaliações de impacto de proteção de dados.

Desde então, continuamos desenvolvendo nossos processos e procedimentos internos existentes para garantir que estejam de acordo os princípios de responsabilidade das exigências do RGPD. Isso é importante, pois o RGPD coloca um foco maior na documentação de decisões e práticas que afetam dados pessoais.

Capacitando nossos usuários em suas jornadas rumo ao RGPD

O Dropbox fornece recursos de controle e visibilidade que podem ajudá-lo a gerenciar suas obrigações de proteção de dados, incluindo as obrigações de conformidade com o RGPD, com mais facilidade. Obviamente, a conformidade com o RGPD em toda a sua organização não começa nem termina com o relacionamento com seus fornecedores, como o Dropbox. Embora nossos recursos possam ajudá-lo a gerenciar suas obrigações, eles não podem por si só garantir a conformidade. A conformidade com o RGPD exige uma consideração mais ampla sobre como os dados transitam e estão protegidos em sua organização. Cada organização deve dar seus próprios passos para alcançar a conformidade, tendo os fornecedores como parceiros importantes nessa jornada.

Minimização de dados

Um elemento importante do requisito de Privacidade desde a concepção do RGPD é que as organizações devem projetar seus serviços de uma maneira que minimize os dados. Isso significa ter boa visibilidade e controle dos dados em sua organização para ajudá-lo a gerenciá-los. O console do Dropbox Business é uma ferramenta útil para ajudá-lo nisso, pois permite monitorar a atividade da equipe, visualizar dispositivos conectados e auditar a atividade de compartilhamento. Trabalhamos para incorporar os princípios de Privacidade desde a concepção em novos produtos e recursos.

Proteção e restauração de dados

A proteção de dispositivo perdido, o histórico de versões e a recuperação de arquivos podem ajudá-lo na proteção contra perda acidental, danos ou destruição de dados pessoais e podem ajudá-lo na restauração da disponibilidade e do acesso a dados pessoais em tempo hábil no caso de um incidente. A autenticação em dois passos é outra medida importante que incentivamos para ajudá-lo na proteção de seus dados.

Manutenção de registros

O RGPD também aumenta as obrigações das organizações para manter registros detalhados de suas atividades de processamento. Nossos registros de auditoria e nossos registros de atividades podem ajudá-lo a entender melhor suas atividades de processamento para respaldar sua manutenção de registros.

Administração de acesso

No console do Dropbox Business, 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 a pessoas de dentro de sua organização. No caso de as responsabilidades mudarem entre os usuários, nossa ferramenta de transferência de conta permite que você transfira facilmente os arquivos e a propriedade dos documentos do Paper de um usuário para outro.

Os administradores também têm a capacidade de desabilitar o acesso de um usuário à própria conta, preservando seus dados e

compartilhando os relacionamentos para manter as informações da sua organização seguras. Por fim, o recurso de exclusão remota permite limpar arquivos e documentos do Paper de dispositivos perdidos ou roubados.

Infraestrutura UE

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



Trabalhando juntos para proteger seus dados pessoais

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

nossos sistemas e práticas para rigorosos testes e auditorias de terceiros.

No entanto, os usuários também desempenham um papel fundamental na proteção de seus dados pessoais. O Dropbox permite configurar, usar e monitorar sua conta de maneiras

que atendem às necessidades de privacidade, segurança e conformidade da sua organização. Nosso [guia de responsabilidade compartilhada](#) pode ajudá-lo 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 ser digno dessa confiança, desenvolvemos e continuaremos a desenvolver o Dropbox com ênfase em segurança e privacidade. Nosso compromisso em proteger os dados pessoais de nossos usuários está no centro de cada decisão que tomamos. Para mais informações, envie um e-mail para privacy@dropbox.com. Para obter mais informações sobre o RGPD, você também pode visitar o nosso [centro de orientação do RGPD](#).