Dropbox

プライバシーとデータ保護

はじめに

個人のデータは社会活動や経済活動において重要な役割を果たします。最近では、企業や組織は、ユーザーから入手した個人データに対する管理の厳格化、利用方法と保護方法の明確化がより求められるようになりました。

Dropbox は、信頼という基盤の上に、世界中にいる数億人ものユーザーや企業との関係を築いています。皆様にご利用いただいていることを誇りとし、個人データ保護の責任を第一に考えています。

お客様へのコミットメント

Dropbox は、お客様の個人データを保護することをお約束します。お客様が Dropbox のサービスをご使用になる際のお客様の責任については、Dropbox のサービス規約をご覧ください。ユーザーへの Dropbox のプライバシー コミットメントと、お客様が Dropbox のサービスをご使用になる際にお客様の個人データが収集、仕様、および処理される方法の説明については、Dropbox のプライバシー ポリシーをご覧ください。北米（米国、カナダ、メキシコ）にお住まいのお客様には Dropbox Inc. がサービスを提供します。その他すべてのお客様の個人データは、Dropbox International Unlimited Company によって管理されます。

Dropbox Business または Dropbox Education をご利用中に Dropbox に提供したすべての個人データの管理者は、Dropbox Business または Dropbox Education のユーザーである企業や組織です。個人データの処理の目的と手段を判断するのはデータ管理者です。

Dropbox はデータ処理者であり、お客様が Dropbox Business または Dropbox Education を利用される際に、お客様の企業や組織の代わりにデータを処理します。データの処理と国際転送に関連する Dropbox のコミットメントについては、Dropbox Business 契約書をご覧ください。

Dropbox の実績：コンプライアンス

コンプライアンスは、サービスの信頼性を検証する際の有効な手段です。Dropbox では、セキュリティおよびプライバシーに対する活動が、ISO 27001、ISO 27017、ISO 27018、ISO 27701、HIPAA/HITECH、SOC 1、2、3 など広く受け入れられている基準や規制に適合していることを独立機関を通じて積極的に検証し、その結果を提供しています。

さらに、Dropbox は、クラウド プライバシーとデータ保護に関する主要な実践として国際的に認められている ISO 27018 を初めて取得したクラウド サービス プロバイダの 1 つです。独立した第三者機関による監査法人が Dropbox の管理機能をテストし、レポートと見解を発表しています。そのレポートと見解は、発表され次第、公開いたします。Dropbox に関する認証と監査レポートは、通常、Dropbox Business と Dropbox Education を対象にしていますが、Dropbox Basic、Plus、Professional のユーザーにもほぼ同様の管理を行っています。さらに、Dropbox は現在、EU クラウド行動規範を遵守しています。Dropbox が遵守している基準とその実践を実証する方法の詳細については、Dropbox のコンプライアンスに関するウェブ ページをご覧ください。

Dropbox アーキテクチャ：お客様の個人データの保護

Dropbox は、お客様の個人データの保護はお客様のデータを安全に保つことから始まると考えています。このため、Dropbox では、セキュリティで保護されたファイル データ転送や暗号化を導入し、拡張可能で安全なインフラストラクチャ全体にアプリケーション レベルの管理機能を割り当てるなど、幾重もの安全対策を講じています。

Dropbox のインフラストラクチャ：ファイル

下の図は、ファイル関連の Dropbox のインフラストラクチャを構成するコンポーネントを示したものです。

メタデータ サーバー

ユーザー データに関する特定の基本情報はメタデータと呼ばれ、独立したストレージ サービスに保管されています。メタデータは、ユーザー アカウントのデータに対するインデックスとして機能します。メタデータには、メール アドレス、ユーザー名、デバイス名などの基本的なアカウント情報とユーザー情報が含まれます。また、ファイル名 やファイル形式などファイルに関する基本情報も含まれ、バージョン履歴やファイルの復元、同期などの機能をサポートします。

メタデータ データベース

ファイルのメタデータは MySQL ベースのデータベース サービスに保管され、パフォーマンスと高可用性に関する要件を満たすために、必要に応じてシャード化/複製されます。

ブロック サーバー

Dropbox は、従来の暗号化を超えて設計された独自のセキュリティの仕組みを利用して、ユーザーのデータを保護しています。ブロック サーバーでは、Dropbox アプリケーションからのファイルをブロックに分け、強力な暗号を使用して各ファイル ブロックを暗号化し、リビジョン間で変更のあったファイル ブロックのみを同期します。Dropbox アプリケーションが新しいファイルや既存ファイルに対する変更を検知すると、変更があったことをブロック サーバーに通知します。新規または変更されたファイル ブロックは、前述のように処理されてストレージ サーバーに転送されます。

ブロック ストレージ サーバー

ユーザーのファイルに含まれる実際のコンテンツは、暗号化されたブロックの状態でブロック ストレージ サーバーを使用して保管されます。Dropbox クライアントはデータを転送する前に、ストレージに合わせてファイルをファイル ブロックに分割します。ブロック ストレージ サーバーは Content-Addressable Storage（コンテンツ アドレス ストレージ：CAS）システムとして機能し、暗号化された各ファイル ブロックはそのハッシュ値に基づいて取得されます。

プレビュー サーバー

プレビュー サーバーは、ファイルのプレビューを作成します。プレビューとは、エンド ユーザーが自分のデバイスですぐに確認できるよう、ユーザーのファイルを別のファイル形式でレンダリングしたものです。プレビュー サーバーは、ブロック ストレージ サーバーからファイル ブロックを取得してプレビューを生成します。ファイルのプレビューが要求されると、まずプレビュー サーバーがプレビュー ストレージ サーバーからキャッシュされたプレビューを取得してブロック サーバーに転送します。最終的にユーザーにプレビューを提供するのはブロック サーバーです。

プレビュー ストレージ サーバー

キャッシュ化されたプレビューは、暗号化された形式でプレビュー ストレージ サーバーに保管されます。

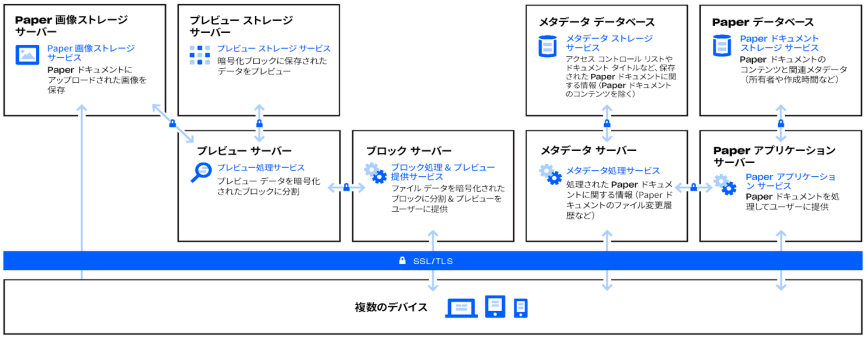
通知サービス

Dropbox アカウントに対して変更があったかどうかをモニタリングするための専用サービスです。ファイルやメタデータがこのサービスに保管または転送されることはありません。各クライアントは、通知サービスに対してロング ポーリング接続を確立して待機します。Dropbox のファイルが変更されると、通知サービスはロング ポーリング接続を終了することによって、関連するクライアントに変更を通知します。ロング ポーリング接続の終了を検知したクライアントは、メタデータ サーバーに安全に接続して、ファイルの変更を同期する必要があります。

Dropbox

Dropbox のインフラストラクチャ：Paper

Dropbox Paper（Paper）は、Dropbox 製品の 1 つの機能ですが、Dropbox インフラストラクチャ環境内でほとんど別個のシステムを使用しています。下の図は、Paper のインフラストラクチャを構成するコンポーネントを示したものです。



Paper アプリケーション サーバー

Paper アプリケーション サーバーは、ユーザーからの要求の処理、編集された Paper ドキュメントの出力の表示、および通知サービスを実行します。Paper アプリケーション サーバーは、ユーザーが行った編集を永続的なストレージに配置されている Paper データベースに書き込みます。Paper アプリケーション サーバーと Paper データベース間の通信セッションは、強力な暗号化が行われています。

Paper データベース

Paper ドキュメントに関する一部のメタデータとユーザーの Paper ドキュメントの実際のコンテンツは、Paper データベースの永続的なストレージ上で暗号化されています。Paper ドキュメント内のコンテンツだけでなく、その Paper ドキュメントについての情報（タイトル、共有メンバーシップとアクセス許可、プロジェクトとフォルダの関連付け、その他の情報など）もその対象に含まれます。また、これにはコメントとタスクも含まれています。Paper データベースは、パフォーマンスと高可用性に関する要件を満たすために、必要に応じてシャード化/複製されます。

Paper 画像ストレージ サーバー

Paper ドキュメントにアップロードした画像は、Paper 画像サーバーで暗号化されて保存されます。Paper アプリケーション サーバーと Paper 画像サーバー間の画像データの転送は、暗号化されたセッションを介して行われます。

プレビュー サーバー

プレビュー サーバーは、Paper ドキュメントにアップロードされた画像、および Paper ドキュメントに埋め込まれたハイパーリンクのプレビューを生成します。Paper ドキュメントにアップロードされた画像の場合は、暗号化チャネル経由で Paper 画像ストレージ サーバーに保存されている画像データを取り出します。Paper ドキュメントに埋め込まれたハイパーリンクの場合は、画像データを取り出し、ソースのリンクで指定された暗号化方式を使用して画像のプレビューを表示します。最終的にユーザーにプレビューを提供するのはブロック サーバーです。

プレビュー ストレージ サーバー

Paper は、Dropbox のインフラストラクチャ図にあるものと同じプレビュー ストレージ サーバーを使用して、画像プレビューのキャッシュを保存します。キャッシュ化されたプレビューのチャンクは、暗号化された形式でプレビュー ストレージ サーバーに保管されます。

Dropbox

Dropbox の管理：Dropbox の 内部慣行

Dropbox は、インフラストラクチャ、ネットワーク、アプリケーションなどを保護するための包括的な対策を講じています。このセキュリティ対策には、ファイル保管時の暗号化、転送時の暗号化、ファイルの完全削除などがあります。また、信頼に応えることを最優先する社風を構築するため、全社員を対象としてプライバシーとセキュリティに関する万全なトレーニングも実施しています。以下に、Dropbox の管理慣行のいくつかを詳細に説明します。

トレーニング

セキュリティとプライバシーを重視する文化の構築と醸成は、Dropbox におけるユーザーの個人データを保護する対策の一部を占めています。そのため、Dropbox の社員は、ユーザー データ プライバシー ポリシーを含むセキュリティ ポリシーに同意していなければ、システムへのアクセスを許可されません。そのシステムには、特定のニーズを持つ社員だけがアクセスできます。また、社員は年に一度、セキュリティとプライバシーに関する必須トレーニングを受講しています。

転送中の暗号化

Dropbox クライアント（現状ではデスクトップ/モバイル/API/ウェブ）と Dropbox のフロント エンド サーバー間では暗号化された接続が確立されて安全な配信が確保され、転送中のファイル データが保護されます。同様に、Paper クライアント（現状ではモバイル/API/ウェブ）とホストされているサービスとの間でも暗号化された接続が確立され、転送中の Paper ドキュメントのデータが保護されます。これらの接続では、Secure Sockets Layer（SSL）/Transport Layer Security（TLS）を使用して暗号化することによって、128 ビット以上の Advanced Encryption Standard（AES）暗号化で保護された安全なトンネルを確立しています。

保管中の暗号化

ユーザーがアップロードしたファイルは、不連続のファイル ブロックとして Dropbox のストレージ サーバーに保存されます。各ブロックは 256 ビットの Advanced Encryption Standard（AES）を使用して暗号化されます。

ファイルの編集中に変更されたブロックのみが同期対象になります。Paper データベースに保存されている Paper ドキュメント データも同様に、256 ビットの Advanced Encryption Standard（AES）によって暗号化されます。

ファイルと Paper ドキュメントの完全削除

Dropbox ユーザー、あるいは Dropbox Business または Dropbox Education のチーム管理者がファイルを完全削除の対象として指定すると、そのファイルを完全に削除する処理がトリガーされます。同じように、ユーザー、あるいは Dropbox Business または Dropbox Education のチーム管理者が Paper ドキュメントを完全削除の対象として指定すると、Paper ドキュメントのデータと画像データを完全削除するための同様の処理が行われます。

個人データへのアクセスのリクエスト

Dropbox に保存されているファイルや Paper ドキュメント以外の個人データは、ウェブサイトにログインし、アカウント ページにアクセスすることで確認できます。アカウント ページには、アカウントに付随する名前やメール アドレスなどの情報が表示されます。また、セキュリティ ページやリンク済みアプリのページには、アカウントにリンクされているセッション、パソコン、モバイル デバイス、アプリが表示されます。

Dropbox ユーザーは、Dropbox が収集したその他の個人データへのアクセスや、それらの情報の削除をリクエストすることもできます。このプロセスの詳細については、Dropbox ヘルプセンターをご覧ください。

Dropbox のプライバシー ガバナンス

プライバシー チームは、Dropbox プライバシー プログラムの運用を担当しています。プライバシーに関する Dropbox の主な取り組みを実施し、データ ライフサイクルにおけるプライバシー バイ デザインを推進しています。さらに Dropbox プライバシー プログラムは、部門の枠を超えたいくつかの法務サブチームによってもサポートされています。プライバシー プログラムの日々の業務を運営、監督するために必要な専門知識はこれらのサブチームが補っています。

データ保護責任者（DPO）のチームは他のプライバシー関連部門とは別に運営されており、データ保護責任者の職務遂行を直接サポートするプライバシー コンプライアンスと監督の役割を果たしています。データ保護責任者（DPO）への連絡は privacy@dropbox.com までお送りください。

Dropbox

政府データ 要請原則

ユーザーが個人データを Dropbox に委ねるのは、Dropbox がそのデータの機密性を守ることを期待しているからであり、それを Dropbox は理解しています。他のオンライン サービス企業と同じく、Dropbox では、政府機関からユーザーに関する情報の提供を要請されることがあります。

政府機関からデータの提供を要請された際の対処の原則について、以下に説明します。

透明性の維持

オンライン サービス企業は、政府機関から受け取った要請の数と種類を公開すること、さらには個人情報の提供が要請された際に本人にそのことを通知することが許されるべきであると、Dropbox は考えます。この種の透明性を高めることは、政府による行き過ぎた行為の事例やパターンに関するユーザーの理解を深めるための一助となります。Dropbox は継続的に、こういった提供要請に関する詳細な情報を公開し、これらの重要情報を提供する権利を主張していきます。

過度に広範な要請に応じない

政府機関によるデータ提供要請は、必要とする情報に限定され、特定のユーザーに的を絞り、合法な調査に基づいて行われるべきです。Dropbox は、包括的かつ過度に広範な要請には応じません。

信頼されるサービスの提供

政府はユーザー データを取得するためにオンライン サービスにバックドアを設置してはならず、インフラストラクチャを危険にさらすべきでもありません。Dropbox は、このような活動が違法であることを明確にするため、弊社システムの保護と法律改定に取り組み続けています。

すべてのユーザーの保護

居住地と市民権の存在する場所に応じて異なる方法で人を保護する法律は、時代に沿わなくなっており、グローバルに展開されるオンライン サービスの可用性を阻害する可能性があります。Dropbox は、これらの法律の改定に取り組み続けています。

これらの原則と年次透明性レポートは、Dropbox ウェブサイト（https://www.dropbox.com/transparency）でご覧になれます。

お客様の個人データの保護に関する Dropbox の管理とアプローチの詳細については、Dropbox Business のセキュリティ ホワイトペーパーをご覧ください。

Dropbox のパートナー

Dropbox では、サービスの提供に関連する活動のほとんどを自社で管理していますが、一部のサービスについては信頼できるサード パーティ（カスタマー サポートや IT サービスのプロバイダなど）に業務を委託しています。これらのサード パーティがお客様の情報にアクセスするのは、Dropbox のプライバシー ポリシーの遵守の下で、Dropbox に代わってタスクを実行する場合に限定されます。また、Dropbox はこれらのサード パーティが Dropbox の指示に従ってお客様の情報を処理することについて、引き続き責任を持ちます。

各サード パーティは、セキュリティ レビューや定期的な契約レビューなど厳格な事前審査プロセスを通して、Dropbox のデータ保護コミットメントを満たす能力があると評価されています。Dropbox はこの事前審査プロセスに基づき、信頼できるサード パーティが Dropbox に代わって個人データを処理する際に、適用される EU データ保護法が確実に遵守されることを確認しています。お客様は、Dropbox が ISO 27001 認証および 27018 認証を受けていることを確認し、適切な守秘義務を遵守したうえで Dropbox の SOC 2 タイプ II レポートを確認することで、Dropbox が信頼するサード パーティを監視することができます。特に、SOC 2 タイプ II レポートにおいて、Dropbox の制御と監査に関する Trust サービス基準 P6.1、P6.4、CC.9.2 の結果を調べることで、Dropbox が信頼するサード パーティを監視することができます。

Dropbox

国際データ転送

Dropbox は、欧州連合、欧州経済地域、英国、およびスイスからデータを転送する場合、当社のお客様や関連会社との契約、標準的契約条項、特定の国の適切性に関する欧州委員会の決定など、該当するさまざまな法的枠組みを遵守しています。

Dropbox は、EU 加盟国、欧州経済地域、英国ならびにスイスから米国に転送される個人データの処理に関して、米国商務省により定められている EU/米国間およびスイス/米国間のデータ プライバシー フレームワークと、EU/米国間データ プライバシー フレームワークの英国拡張版に準拠しています。Dropbox は当該データに関してこれらのデータ プライバシー フレームワークを順守する旨を米国商務省に対して保証していますが、本サービスの DocSend と Formswift に関してはこれに含まれません。

データ プライバシー フレームワークと Dropbox の認定について詳しくは、www.dataprivacyframework.gov をご覧ください。

Dropbox のデータ プライバシー フレームワークのコンプライアンスに関する苦情と申し立ては、独立した第三者機関である JAMS を通して調査と解決が行われます。詳細については、Dropbox のプライバシー ポリシーをご覧ください。

GDPR：一般データ保護規則

一般データ保護規則（GDPR）は、EU 域内のデータ主体の個人データ保護に関する法的枠組みを定めた EU の規則です。GDPR は 1995 年以降の EU データ保護指令を置き換える欧州データ保護法令の最も重要な部分で、Dropbox をはじめ欧州で事業を展開する多数の企業が GDPR コンプライアンスに多大な投資をしています。GDPR は、EU 域内のデータ保護法を調和させ、過去 20 年間に起こった急速な技術変革に対応させています。GDPR は、EU データ保護指令を含む過去の法的枠組みに基づいて構築されており、個人情報を取り扱う企業や組織に対して新たな義務と責任を導入しつつ、個人データに関する個人の新しい権利についても触れています。EU 域内の企業や組織、および、EU 域内のデータ主体の個人データを処理する企業や組織は、GDPR の遵守を求められます。

Dropbox の GDPR コンプライアンスへの取り組み

Dropbox は、GDPR の遵守に取り組んでいます。プライバシーとセキュリティの重視は Dropbox 設立時からの社是であり、企業成長の過程においても、ユーザーから委ねられたデータの取り扱いと保護に注力することは常に高い優先順位を保ってきました。Dropbox はコンプライアンス曲線を上回る実績があり、上記のように、ビジネス ユーザー向けに ISO 27018 認証をいち早く取得したクラウド サービス プロバイダでもあります。このような強固な基盤があることから、GDPR のコンプライアンスは、Dropbox がすでに行っている慣行と管理の進化形であり、ユーザーの個人データを常に保護するための継続的な取り組みをさらに発展させたものであると Dropbox は考えています。Dropbox の GDPR コンプライアンスへの取り組みは、2016 年に規制が採択された直後に始まりました。Dropbox は、法律顧問、セキュリティとコンプライアンスの専門家、製品とインフラストラクチャのエンジニアで構成されるデータ保護の専門家チームを組織することから取り組みを始め、その専門家チームにより、現状のセキュリティおよびデータ保護慣行の GDPR 要件に対する評価をすべて完了しました。

次のステップとしたのは、Dropbox が扱う個人データ処理活動の評価を行い、Dropbox のシステム全域での個人データのライフサイクルを追跡することでした。このような実地での検証を、データ マッピングの実行およびデータ保護影響評価の完全実施と呼ぶこともあります。

それ以来 Dropbox では、既存のプロセスをベースとして、GDPR 要件下での責任原則を確実に満たす内部プロセスと手順を構築し続けてきました。これには GDPR 第 30 条に従って処理の記録を維持することなどが含まれます。GDPR では個人データに影響を与える決定と慣行を文書化することに重点を置いているため、これは重要です。

Dropbox ユーザーの GDPR への取り組みを支援

Dropbox は、GDPR での遵守義務を含むデータ保護義務の管理がより簡単になる制御と可視化の機能を提供します。当然ながら、ユーザーの企業や組織全体での GDPR の遵守と、Dropbox などのサプライヤーとの関係の開始や終了とは無関係です。Dropbox の機能はユーザーの企業や組織が果たすべき義務の管理に役立ちますが、義務の遵守自体を保証するものではありません。GDPR を遵守するためには、組織内でのデータの移動と保護の状況について、より広範に検討する必要があります。GDPR コンプライアンスを達成するため、それぞれの企業や組織は重要なパートナーであるサプライヤーと協力して、独自の手順を確立し実行する必要があります。

データの最小化

企業や組織は利用するデータを最小限に抑えてサービスを設計する必要がある、という点が、プライバシー バイ デザイン（計画的なプライバシー対策）の要件に関する GDPR の重要な要素です。つまり、組織におけるデータの可視性の高さが、容易なデータ管理につながる、ということです。Dropbox Business 管理者用ダッシュボードは、チームのアクティビティの監視、接続デバイスの表示、共有アクティビティの監査を可能にする便利なツールで、そういった高い可視性の実現に役立ちます。Dropbox は、新製品や新機能にプライバシー バイ デザインの原則を反映させるべく取り組んでいます。

データの保護と復元

紛失したデバイスの保護、バージョン履歴、およびファイルの復元は、個人データの偶発的な紛失、破損、破壊からの保護と、インシデントが発生した場合の速やかな可用性の回復、個人データへのアクセスを可能にするものです。データを保護するために推奨されるもう 1 つの重要な手段は、2 段階認証です。

記録の保存

GDPR により、処理アクティビティの詳細な記録を企業や組織が保持する義務も増加します。Dropbox の監査ログとアクティビティ ログは記録保持に役立ち、処理アクティビティがより理解しやすくなります。

アクセス管理

Dropbox Business 管理者用ダッシュボードを利用することで、チーム メンバーのファイル、フォルダ、Paper ドキュメントへのアクセス管理が容易になります。共有ファイル リンクに対しては、リンク許可機能を使用することで、共有リンクのパスワード保護、有効期限を設定した一時アクセス許可、組織内のアクセス制限が実現できます。ユーザー間で責任が変更された場合は、アカウント移行ツールを使用すれば、ユーザー間でファイルと Paper ドキュメントの所有権を簡単に移行できます。

管理者は、ユーザーのデータと共有関係を維持しつつユーザーのアカウントへのアクセスを無効にすることで、企業や組織の情報を守ることができます。また、遠隔削除機能を使用すれば、紛失したデバイスや盗難に遭ったデバイスからファイルや Paper ドキュメントを消去できます。

EU 域内でのインフラストラクチャ

GDPR では、個人データを EU 域内でホストすることは必須ではありませんが、Dropbox Business および Dropbox Education のお客様が EU 域内でのファイル（ブロック）の保存をご希望の場合、保存が可能です。EU ベースのファイル ストレージは、Amazon Web Services（AWS）インフラストラクチャによって提供されます。EU 域内でのインフラストラクチャの詳細については、セールス担当にお問い合わせください。

Dropbox

お客様と共に取り組む個人データ保護

Dropbox は、お客様と協力して個人データの保護に取り組んでいます。インフラストラクチャ、ネットワーク、アプリケーションの保護、セキュリティとプライバシー対策に関する社員トレーニング、信頼に応えることを最優先する社風の構築、システムと実践内容に対する厳格な第三者機関によるテストと監査など、Dropbox は包括的なセキュリティ対策を講じています。

もちろん、お客様も個人データの保護で重要な役割を担います。Dropbox を使用することで、企業や組織のプライバシー、セキュリティ、コンプライアンスのニーズに合致した方法でアカウントの設定、使用、監視できます。Dropbox の共有責任ガイドをご覧になることで、お客様のアカウントを安全に保ち、個人データの可視性と管理性を維持するために、Dropbox をどのように利用すればよいかをご理解いただきやすくなります。

まとめ

日々、数億ものユーザーに Dropbox を信頼してご利用いただいています。Dropbox では、その信頼にお応えするためにセキュリティとプライバシーを重視したシステムの構築と成長を続けてまいります。ユーザーの個人データを保護することは、Dropbox の行動規範です。詳細については、privacy@dropbox.com までお問い合わせください。GDPR の詳細については、Dropbox の GDPR ガイダンス センターをご覧ください。