Dropbox が GDPR に準拠するまで

Dropbox

はじめに

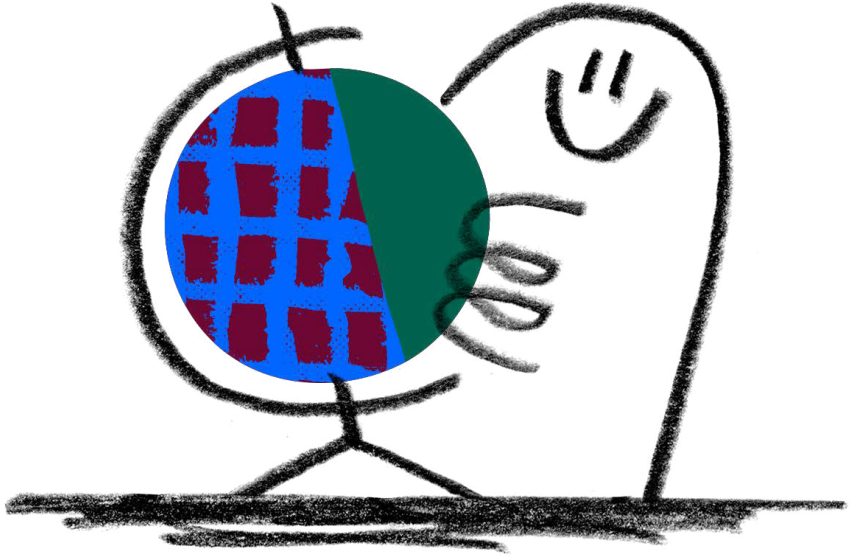
一般データ保護規則（GDPR）は欧州連合の規則であり、EU 居住者の個人データの取り扱いに関して、新たに統合された枠組みです。2018 年 5 月 25 日より適用が開始されました。

本規則の発効を受けて、お客様の間でも欧州における新しいデータ保護の枠組みが具体的にどのような影響を及ぼすのか注目が集まりつつあります。

Dropbox は GDPR に完全に対応していますが、お客様からのご意見を受けて、この度、GDPR 準拠のプロセスをご紹介することになりました。

Dropbox にとっての GDPR の意味

Dropbox と世界中にいる数億人もの Dropbox ユーザーや企業との関係性を構築しているのは信頼です。皆様にご利用いただいていることを誇りとし、情報保護の責任を第一に考えています。

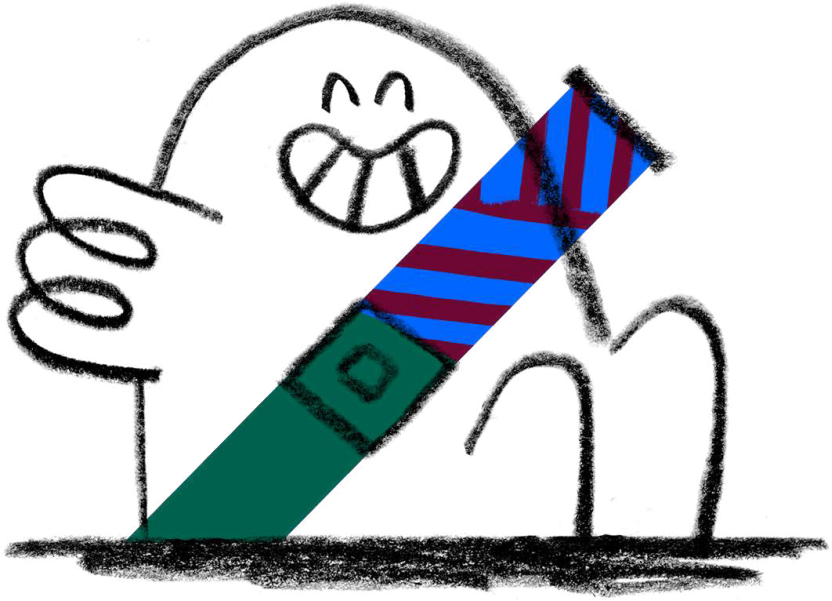


データのプライバシーと安全性を最優先

- Dropbox には、専門家向けツールを駆使するセキュリティ専門チームと、Dropbox の開発と保守のために用意されたエンジニアリング手法があり、何重ものセキュリティ対策を通じて、お客様のファイルを保護しバックアップしています。
- Dropbox のセキュリティ対策は、ISO 27001、ISO 27017、ISO 27018、HIPAA/HITECH、ドイツ BSI C5、SOC 1、2、3 などの広く認められた規格や規制に準拠しています。また、独立した第三者監査機関が Dropbox の管理機能をテストし、レポートと見解を提供しています。
- Dropbox が準拠している各種基準および弊社のセキュリティ対策の検証方法については、コンプライアンスに関するウェブページで詳細をご覧ください。
- Dropbox Business セキュリティ ホワイト ペーパーには、弊社のセキュリティへの取り組みが、あらゆる角度から詳しく記載されています（インフラストラクチャ、ネットワーク、アプリケーション、物理環境、情報など）。

データ保護に関する確固とした実績

- Dropbox には、データ保護を何よりも重要と捉え、率先してコンプライアンスを満たしてきた実績があります。たとえば Dropbox は、クラウドのプライバシーとデータ保護に関する主要な行動規範として国際的に認められている ISO 27018 を初めて達成したクラウド サービス プロバイダーの 1 つです。
- Dropbox はプライバシー専門担当者を社内に配置し、GDPR の要件に則ってお客様のデータを保護できるよう、プライバシー プログラムやプライバシー ポリシーの策定と維持に努めています。
- Dropbox は、企業のお客様と交わす合意に重大な契約責任を盛り込んでいます。企業のお客様との合意には EU 標準契約条項を組み込み、また、EU-米国間のプライバシー シールド フレームワークで認定を受けています。これは、欧州連合から米国に移転された個人データの収集、使用、保存に関して、さらに法的保護と外部からの監視が適用されることを意味します。



GDPR 準拠を実現するまでのプロセス

こうした強力な基盤があることから、Dropbox は、GDPR への準拠によって個人データの扱い方が大きく変わることはなく、むしろ現在のセキュリティ対策とセキュリティ管理がさらに強化されると考えています。

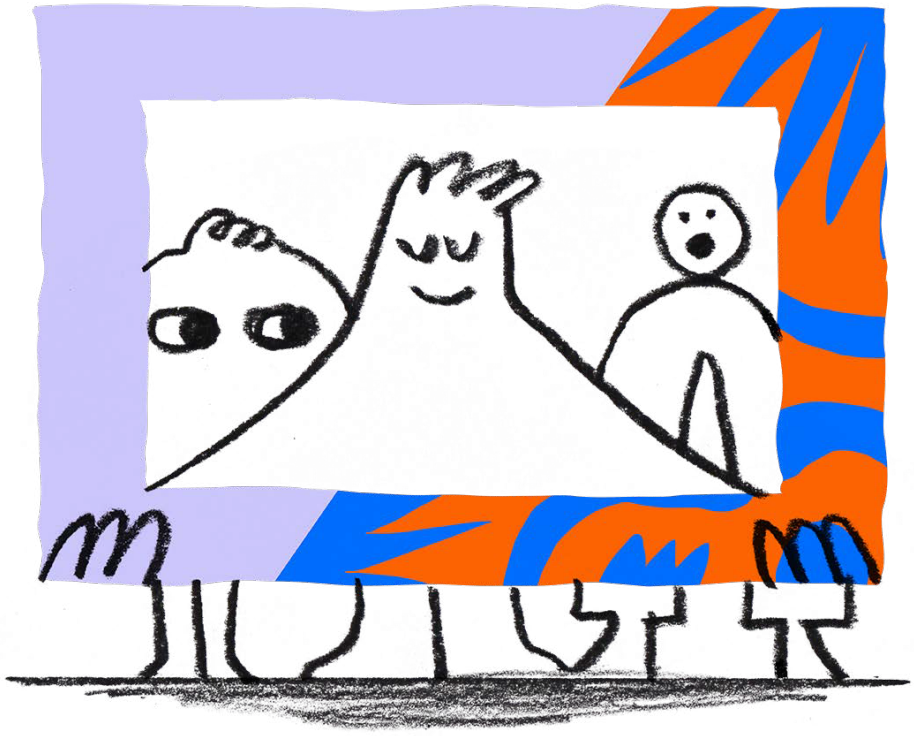
GDPR 準拠に向けての準備は、2016 年に規則が採択された直後から始まりました。最初のステップでは、**部署の枠を超えたデータ保護専門担当者チームを立ち上げ**ました。法律顧問、セキュリティとコンプライアンスの専門家、製品エンジニアとインフラストラクチャ エンジニアを米国とヨーロッパから集めてチームを構成し、GDPR の新しい要件の分析と対応を行いました。

次のステップでは、**弊社の現在のセキュリティ対策とデータ保護対策、GDPR 準拠への準備状況を評価**しました。方法として、GDPR と付随する最新のガイドラインを基に徹底的かつ詳細にギャップ分析を実施し、Dropbox に該当する部分を洗い出しました。さらに、現在の弊社の対策で GDPR の要件を満たせるのか、要件を完全に満たすには対策の改定が必要なのかどうかを検証しました。

続いてのステップでは、弊社の**個人データの取り扱い方法を徹底的かつ詳細に検証**しました。この作業は「データ マッピング」と呼ばれることもあり、弊社のシステムでユーザーの個人データを最初に収集したときから、削除して廃棄するまで、個人データのライフサイクル全過程を追跡します。

Dropbox は、GDPR の要件に則り説明責任の原則を確実に満たすよう、**既存の社内プロセスと社内手順を**充足しています。GDPR では、個人データに影響する決定事項や対策の文書化に大きな重点が置かれていることを考えれば、説明責任の原則を守ることは重要です。

専門チームの任命、GDPR 要件とのギャップ分析、データ マッピングの完了を経て、Dropbox は必要なステップとプロセスを構築し、2018 年 5 月までに GDPR への完全準拠を果たしました。



Dropbox