

# 一般データ保護規則

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と保護に関する新たな枠組みを確立するものです。

GDPRは、個人データを取り扱うすべての組織に新しい義務と責任をもたらし、個人には個人データの収集、処理、保存方法に関する新しい権利を提供します。

## GDPRの影響

GDPRを遵守する必要のある組織は、検討すべき点が多数あります。

具体的な状況に合わせて何が必要か判断するには、法的助言を求めることを強く推奨します。

## 1. データについて理解する

データを適切に保護することは、組織のデータ取り扱い方法、つまり、個人データがどのように処理、共有、利用、アーカイブ、削除されているか理解することを意味します。データとは何であり、どのように保存されているか理解することは、ビジネスにおいてGDPR戦略を構築する際に必要となる重要な点です。

## 2. 所有権と責任を判断する

データ保護を遵守するためには、責任ある所有者を特定することが重要です。組織によっては、データ保護責任者の任命が必要になることもあります。GDPRはまた、データ保護遵守プログラムの採用を求める新しい「説明責任」原則を導入しました。組織には、内部データ保護ポリシーを作成し、スタッフにトレーニングを提供する必要が発生します。

## 3. データ処理の法的根拠を確保する

GDPRが企業に文書化しなければならないと定めるもう1つの構成要素は、取り扱うさまざまな種類の個人情報を処理する法的な根拠です。たとえば、データ処理の根拠を「同意」とする場合には、同意を得る方法を検討し、いつどのような方法で同意を得たか明確に示せるようにする必要があります。

## 4. データ主体の権利を理解する

手順が確実に適用されるようにするには、個人データに関して所有者が持つ権利について理解する必要があります。たとえば、データ主体は電子的に自らの個人データにアクセスし、修正、削除、エクスポートする権利を持ちます。特定の状況では、自動的な意思決定やプロファイリングに対して反対する権利も持ちます。



## 5. プライバシーバイデザインを確保する

初めてプライバシーバイデザインが明確な法的要件となるため、ビジネス手順にどのように組み込むか検討し始めることが重要です。状況によっては、プライバシーエンパワーメントを実施することも必要となります。

## 6. 漏洩管理の準備を整える

データ漏洩管理ポリシーおよび手順を最新の状態に保ち、検証することは、堅牢なデータ保護プログラムにとって極めて重要です。GDPRでは、漏洩を検知し、適切な関係当局に適時報告することが求められ、漏洩だけでなく報告の不履行にも罰金が発生する場合があります。

## 7. 重要な情報を伝える

組織のオンラインプライバシーポリシーやその他の通知が、最新かつデータ保護の実践を網羅している状態にします。新しい要件には、「処理の法的根拠を詳述し、問題がある場合には抗議できる関係当局があることをユーザーに知らせる」という項目が含まれています。

## 8. プロバイダーと連携する

組織内のポリシーだけでは、GDPRの義務を果たすことができません。組織に代わって個人情報の処理を行う第三者もまた、データ保護に必要な基準を満たす必要があります。プロバイダーには、次の点について確認しておく必要があります。

- ネットワークおよび情報セキュリティ、プライバシー、データ保護に関する堅牢性の高い手法があるか
- 国際的に認められた規格に準拠し、そのコンプライアンスを検証しているか
- 信頼とセキュリティ意識の高い文化があることをいかに証明できるか、また、データ管理をサポートし、管理者としての義務を果たすために、どのような管理策を提供できるか

## Dropbox: データの保護

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。皆様の信頼に応えられるよう、セキュリティ、コンプライアンス、プライバシーを強化して Dropbox を開発し、今後も成長し続けます。

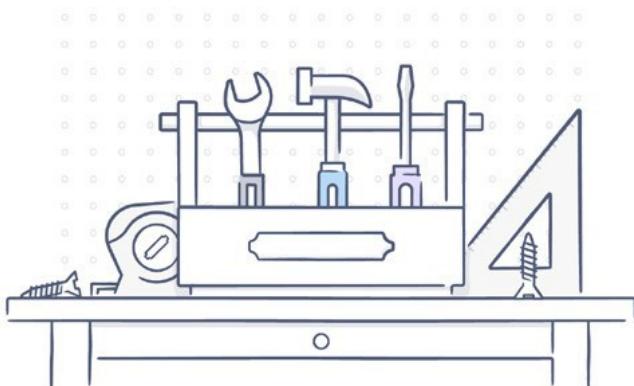
### セキュリティ: 保護と制御

#### 保護: アーキテクチャと情報セキュリティ

Dropbox は、安全な分散型インフラストラクチャと複数の保護レイヤで設計されています。この保護レイヤには、セキュリティ保護されたデータ転送、暗号化、ネットワーク構成、そして拡張可能で安全なインフラストラクチャ全体に分配されるアプリケーションレベルの管理機能が含まれます。Dropbox では、リスクを見極め Dropbox のセキュリティを促進するために、堅牢性の高い情報セキュリティ管理フレームワークを開発しています。また、セキュリティポリシーのレビューと更新、社員に対するセキュリティトレーニングの提供、アプリケーションやネットワークセキュリティのテスト(侵入テストも含みます)を定期的に実施しています。さらに、リスク評価とセキュリティポリシーのコンプライアンスも監視しています。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。

#### 制御: IT 管理者の強い味方

Dropbox は IT 管理者が必要とする管理機能を提供し、高い可視性を実現しています。管理者用ダッシュボードから、チームアクティビティを監視し、接続デバイスを確認し、共有に関する操作を監査できます。グループを作成して、フォルダに対するチームメンバーのアクセス権限を簡単に管理できます。チームフォルダマネージャーからは同期管理など、チームフォルダの状況を把握や制御ができます。リンクの権限設定を利用すれば、共有リンクのパスワード保護、有効期限を設定したコンテンツへの一時的なアクセス許可、組織内のユーザーに対するアクセス制限も行えます。アカウント移行ツールによって、担当者が変わっても、別のユーザーに簡単にファイルを移行することができます。遠隔削除機能を使えば、紛失または盗難にあったデバイスからファイルを削除できます。



### コンプライアンス: 信頼と検証

コンプライアンスはサービスの信頼性を立証するための効率的な方法です。Dropbox のセキュリティ対策が ISO 27001、27017、27018、SOC 1、SOC 2、SOC 3 など、世界的に認められている規格や規制に準拠していることをぜひご確認ください。独立した第三者監査機関が Dropbox の管理機能をテストして作成したレポートと意見をできる限りユーザーの皆様と共有いたします。Dropbox が準拠している規格と Dropbox のセキュリティ対策の検証について詳しくはコンプライアンスのウェブページをご覧ください。

### プライバシー: Dropbox の取り組み

個人情報か仕事の情報かに関係なく、Dropbox はお客様からの信頼を深く考慮し、Dropbox のシステム内にあるすべてのデータを保護するために尽力しています。プライバシーポリシーでは、お客様の情報の取り扱い方法と保護方法を説明しています。また、Dropbox はどのような頻度でデータ要請を受け、調査と対応を行っているかという情報を共有するために、透明性レポートと政府によるデータ要請原則を公開するとともに、ユーザーのプライバシーを保護するための法律改定にも取り組んでいます。

### 連携してデータの安全性を維持

Dropbox はデータを安全に保つため企業のお客様と協力しています。また、インフラストラクチャ、ネットワーク、アプリケーションを保護するため、包括的な対策を講じています。社員に対してセキュリティとプライバシー対策に関するトレーニングを実施し、信頼に値することが最優先であるという文化を醸成し、Dropbox のシステムや活動を第三者機関によって厳格に検証および監査しています。また、お客様もチームやデータを安全に保護するために重要な役割を果たしています。Dropbox では、お客様の組織のセキュリティ、プライバシー、コンプライアンスのニーズを満たす方法でアカウントの構成、使用、監視が行えます。Dropbox の共有責任ガイドは、アカウントの安全性を確保するために Dropbox が取り組んでいること、そしてチームのデータに対する可視性と制御を維持するためにお客様が実施できることについて詳しく説明しています。

このガイドの内容は情報へのアクセスを支援するものであり、法的助言ではありません。必要に応じて法的助言を受けてください。

