proofpoint

PROOFPOINTによるEU GDPRの順守

主な利点

- データの場所と使用方法を把握できます。
- データの保存・削除期間を自動的に設定し、個人情報の漏出を防ぐことができます。
- コンプライアンス違反をリアルタイムで識別し、解決できます。
- 個人データとそのデータを処理するアプリケーションに対する不正アクセスを阻止します。
- なりすましメール、認証情報を狙うフィッシング詐欺、個人データを盗む悪意のあるペイロードをブロックします。

European Union General Data Protection Regulation（EU GDPR）は、EU居住者の個人情報の収集、処理、保存、削除、転送、使用の規制を目的としています。EUで個人情報を取り扱う企業は、この新しい規則を遵守しなければなりません。

この規制では、個人データの収集者に「個人情報を保護するために、技術的および組織的な対策を効果的に実装し、必要な保護対策をプロセスに統合」することを義務付けています。

GDPRを遵守するには、複数のセキュリティ技術を使用し、ポリシー違反、コンプライアンスリスク、高度な脅威に対して一元的に管理を行う必要があります。Proofpointの統合サイバーセキュリティプラットフォームを利用すると、場所、デバイス、チャネルに関係なく、個人情報と重要なデータを保護できます。重要なファイルとコンテンツを管理するだけでなく、アーカイブファイルにすばやくアクセスし、GDPRへの対応状況を迅速に把握して、EU居住者の個人データの盗難や消失を防ぐことができます。

GDPR対応に役立つProofpointのソリューションは次のとおりです。

- Information Protection
- Information Archive and Compliance[*1]
- Email Protection
- Targeted Attack Protection

合法性、公平性、透過性

GDPRでは、基本的に、データに対する権利は個人に戻されます。EU居住者には、個人データに対するアクセス権だけでなく、「忘れられる権利」も認められます。つまり、すべてのデータストアからのデータを削除する権利が認められています。

メール、ファイル共有、データストア、SharePointサイト、クラウドアプリケーションの個人データの識別、取得、削除に必要な可視化を維持できる組織はごく少数です。個人の検索要求や監査に対応するには、個人データが保存されている場所、データを収集、検索、取得できる場所を把握しておく必要があります。

Proofpoint Information Protectionを使用すると、このデータガバナンスプロセスを管理できます。次のことができます。

- 様々なチャネルを通過する個人データを自動的に識別する
- コンプライアンス違反をリアルタイムに修復する
- データを露出する危険性のあるアクセスを隔離、削除または取り消す

保存制限

GDPRは、必要な個人データのみを収集し、必要な期間のみ保存することを義務付けています。この要件は特にメールのアーカイブで問題になります。別の法規制では、特定の種類のデータに対して異なる保存期間が義務付けられています。たとえば、納税記録、HR、医療データの保存期間は大きく異なります。組織は、GDPR対応のポリシーだけでなく、規制対象の保存期間要件を遵守するポリシーも適用する必要があります。

Proofpoint Information Archive and Compliance[*1]は、組織のデータガバナンスに役立つ柔軟で、完全に自動化された暗号化ソリューションを提供します。このソリューションでは、次のことを行うことができます。

- EU居住者の特定の個人情報に対する保存・削除ポリシーを一元管理し、一貫した方法で適用することができます。
- メール、企業のコラボレーションデータ、ソーシャルメディアデータなど、電子的に保存された情報（ESI）のソースを利用できます。
- 変更不能な監査証跡でポリシーの変更を追跡できます。組織のポリシー変更を正確に記録することで、GDPRのアカウンタビリティ要件を満たすことができます。

整合性と機密性

EU居住者の個人データが侵害された場合、収益全体の最大4%の制裁金が科せられる可能性があります。企業は、EU居住者の権利を守るだけでなく、個人データを保護し、データの窃盗や消失を防ぐ対策を講じる必要があります。

データ窃盗を防ぐ

サイバー攻撃の約91%はメール経由で実行されます。したがって、このチャネルの保護は非常に重要です。ProofpointのEmail ProtectionとTargeted Attack Protectionは、次の機能で、なりすましメールや認証情報を狙うフィッシング詐欺メールからメールのエコシステムを保護します。

- 送信者/受信者の関係性、ヘッダー、コンテンツなどのメール属性を使用して、送信者のレピュテーションを取得します。
- 受信ボックスに届く前に、悪意のある添付ファイルやURLを含むメールを検知し、分析を行いブロックします。
- 受信ボックスに侵入を試みる脅威に対応し、被害を回避します。

偶発的なデータ損失を防ぐ

組織の攻撃経路で最も多いものがメールです。送信データの消失も重大なリスクの一つです。メール送信での機密情報の流出を防ぐには、データ侵害のリスクを最小限に抑えることが重要です。Proofpoint Email Data Loss Preventionを使用すると、次のことができます。

- 組織内から送信されるメールを可視化し、完全に制御します。
- 地理的な場所、データタイプ、目的、セキュリティ統制に応じて80以上のポリシーを設定できます。EU居住者の個人データを含むメッセージを動的に検出、分類、ブロックできます。
- 個人データがメールで共有された場合、個人データを暗号化し、監視できます。

クラウドを利用することで、Proofpointのソリューションを脅威の状況に応じて適切な場所に配置できます。弊社の高度なサイバーセキュリティソリューションにより、EU居住者のデータの信頼性とコンプライアンスを維持し、保護できます。

注釈

[*1] 日本では現在取り扱いしておりません。詳細は営業担当にお問い合わせください。