GDPRコンプライアンスのためのデータプライバシー、データ保護、とその統合の重要性

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

EU一般データ保護規則(GDPR)ガイドラインでは、EU内で発生する取引だけでなく、EU市民に影響を与える取引について、所在地にかかわらず、EU市民の個人データとプライバシーを保護することが求められています。欧州連合(EU)内の対象となる個人データを管理または処理するすべての組織は、所在地に関係なく、GDPRを遵守しなければならないため、これは非常に大きな課題です。

そして、個人データには何が伴いますか？GDPRによれば、個人データとは、「識別されるまたは識別可能な自然人（「データ主体」）に関する」[1]すべての情報に及び、このような識別情報には、名前、何らかの種類の識別番号、電子メールアドレス、または「自然人の身体的、生理的、遺伝的、精神的、経済的、文化的、社会的アイデンティティーに特有の1つまたは複数要因」を含みます。[2]

組織がGDPRの遵守を達成するために、本質的に2つの主な責任が伴います。組織は、データ主体に対してデータをアクセス可能かつ削除可能な方法で、個人データを保管および管理しなければならず、輸送中および保管中にこれらの個人データを管理および保護しなければなりません。しかし、これらの責任は、組織がデータ処理者であるか、データ管理者であるかにより変化しますが、多くの組織は、一定程度両方の可能性を備えています。

データ処理者とは、データ管理者に代わって、個人データを処理する「自然人または法人、公的機関、代理店またはその他の団体」です。[3] データ管理者とは、「個人データの処理の目的と手段を単独で、または、他者と共同で決定する自然人または法人、公的機関、代理店またはその他の団体」を指します。[4] 簡単に言えば、データ管理者はデータを収集し、データ処理者はそのデータで何らかの処理を行います。しかし、データ管理者とデータ処理者の両方がGDPRを遵守し、不正なアクセス、破壊、損失、暴露からデータを保護しなければはりません。

> 「データプライバシーとデータ保護は、似たような用語であり、しばしば重複しますが、必ずしも同義ではありません。」

企業が個人データを管理し、GDPRの遵守要件を満たしているかどうかには、さまざまな意味合いがあるため、デジタルデータの移動やデータ処理に関連する「プライバシー」と「保護」という用語のニュアンスを深く理解することが重要です。

プライバシーと保護

データプライバシーとデータ保護は、似たような用語であり、しばしば重複しますが、必ずしも同義ではありません。データ保護とは、破損や損失から情報を保護するためのプラクティスまたはプロセスです。データプライバシー（または情報プライバシー）は、組織の処理ルールおよびプラクティスに関連しており、不正な方法で、データ管理者とデータ処理者がデータを使用することを規制しています。

Dave Brunswick
マネージドファイル転送ソフトウェア市場において、シニアコンサルティングやアーキテクチャーの役割を担うなど、テクニカルセールス、プリセールス、技術戦略、エンジニアリング、製品管理、製品開発において25年以上の経験を有しています。現在、Cleo社の北米プリセールス兼ソリューションサポート担当副社長を務めています。

もっと簡単に言えば、データ保護とは、不正アクセスからデータを保護することです。一方、データプライバシーは、アクセスを許可した人に何が起こるかに関連します。データ保護は、通常、情報を保護することを中心に行われ、暗号化、安全な通信プロトコル、明文化されたセキュリティポリシーを含む場合があります。データプライバシーは、個人を特定できる情報(PII)の収集、保管、使用方法に焦点を当てた法的な問題と考えるのが最適です。データ保護の焦点はセキュリティですが、データプライバシーは、情報の管理方法や使用方法に関連します。

このような違いは、SOX（米国企業改革法）、HIPAA（医療情報の相互運用性と説明責任に関する法律）、GDPRなどのコンプライアンス義務の対象となっている組織の今日のプライバシーとサイバーセキュリティに関する議論にとって重要です。したがって、データの移動と処理（およびそれらのワークフローを取り巻く業務手順）は、必要なコンプライアンス基準を遵守するために検討、測定、監視する必要があります。

デジタルビジネスのコンテキストでは、データ保護はデータプライバシーと必ずしも同等ではありません。デジタルデータが技術によって保護されていない場合、プライバシーを確保することは極めて困難です。誰かが悪意を持って個人情報を使用する可能性がある場合、そのプライバシーは完全に不確実です。データ処理者およびデータ管理者として機能する組織は、コピーデータ保護、暗号化、管理ファイル転送(MFT)、安全な統合など、データのガバナンスプロセスを強化するのに役立つデータ保護技術を採用することが重要です。

プロセスの重要性

GDPRの義務は、データの統合と取り込み（データ処理）を含むデータ処理にかなり重点を置いています。したがって、組織は保護の観点だけでなく（どこにあってもデータをどのように保護するか）、プロセス保護の観点から（どのようにしてデータの使用を管理するか）からプライバシーを考え始めています。

組織がデータで行うことのほとんどすべてが処理を構成するため、事実上すべてのプロセスは、あるレベルでデータ転送を行います。ヘルスケア、金融サービス、物流、輸送などの業界では、データ転送は基本操作の中核であり、内部転送、外部転送、保管、表示、分析、変更、同期化、複製な

どのデータに対するあらゆる操作は、技術的には処理イベントです。

GDPRで概説されたすべての相互作用とあらゆるプロセスに関連して、これらのイベントを取り巻く幅広い流通過程の管理を調べると、データ転送は必ずあります。実際のところ、組織は、技術スタック全体について、以下の質問することが有益であると感じる場合があります。

- サプライチェーンに沿った企業リソース計画(ERP)ソフトウェア、電子データ交換(EDI)システム、輸送および倉庫管理システムを通じて、B2B（企業間）データはどのように移動しますか？
- 組織は、パートナーのフラットファイルをIDOCに変換して、組織のSAPシステムに取り込むことができますか？
- 組織がクラウドストレージリポジトリを使用している場合、データを安全に取得するクラウド統合プロセスとは何ですか？
- 組織に有用なセールスフォースCRM (Customer Relationship Management)システムの場合、他のアプリケーションからの購入、課金および出荷情報を最新の状態に保つためにどのような統合プロセスが必要ですか？
- データ倉庫からデータ分析プラットフォームへの情報の移動はどのように行われますか？

ほとんどの組織にとって見えない部分ではあるけれども、データ移動は、すべてのビジネスプロセスの中核にあり、B2B業務からクラウド、システムからシステム、アプリケーションからアプリケーション、システムから人、人から人まで、あらゆる方法でデータを保護する組織的責任があります。

> エコシステム全体のデジタルデータに対する処理が技術的処理イベントである場合、これらのイベントを適切に保護および管理する技術が必要です。

エコシステム全体のデジタルデータに対する処理が技術的処理イベントである場合、これらのイベントを適切に保護および管理する技術が必要です。同時にデータ処理者とデータ管理者であるこれらの組織は、データユーザビリティ、セキュリティ、ガバナンスのバランスをとって、コンプライアンスの必要性に応じて、どのようにデータを移動、統合、処理することを確実にしますか？多くの組織にとってその解決策は、エコシステム駆動型統合プラットフォームです。

データおよびデータ処理の保護

GDPRの新しい世界秩序と、ファイアウォール中においてデータフローを保護し、管理する必要性から、コンプライアンスへの道は技術によって築かれています。GDPRおよびその他のコンプライアンス指令により、組織は、一定程度の個人データ保護を提供する必要があります。そのため、組織は、データフローを保護、管理、制御し、不正なアクセスや使用を防止する必要があります。

暗号化と安全なファイル転送技術は、データを保護する一般的な手段ですが、明示的にデータプライバシーを有効にするわけではありません。ガバナンスとポリシー執行の仕組みが、まさにそれを行います。したがって、多くの目的のために、データプライバシーは、データ保護のサブセットであり、このポリシーがより広い保護を提供するとき、多くの場合、スマートポリシーの副次的影響です。

B2Bの環境では、ビジネスデータは、組織が本質的に制御できないシステム、アプリケーション、および人々の間で移動します。そのため、コンプライアンスとガバナンス（現代のビジネスエコシステムの重要な側面）は、適切なコア統合プラットフォームがなければ実装するのが非常に困難です。現代の組織は、高度な統合技術を使用してデータ処理をアップグレードする際、デジタル個人データの保護とプライバシーの両方を提供する一歩を踏み出します。

エコシステム駆動型統合プラットフォームは、データが転送中であるときにデータ処理イベントを保護し、エンドツーエンド暗号化を使用して休止状態になるので、許可されたユーザーだけがデータにアクセスできます。また、アプリケーションプログラミングインターフェイス（API）やファイルベースの統合など、統合プロセスのあらゆる側面を管理および制御するメカニズムも提供します。このガバナンスは、堅固なオーケストレーションエンジンと自動化、一貫性および信頼性をサポートするRESTful APIにより実現され、暗号化されているかどうかに関わらず、個人情報および機密情報を適切に処理できるようにします。**図1**は、従来のモデルを示し、**図2**は、エコシステム駆動型統合プラットフォームを示しています。

これらの相互作用とそれを取り巻くプロセスを保護することも同様に重要です。これには、データ移動のすべての側面を保護および管理するための基準、プラットフォームを保護すること、統合依存プロセスのアクセス、開始および終了に関する強力な監査およびレポートの提供など、多数の方法論および基準のサポートが必要です。

結論

GDPR違反にかかる費用は、劇的な影響に及ぶ可能性があります。組織は、組織のブランド、評判、信頼性への損害はもちろんのこと、データ侵害またはデータ誤用のために、年間売上高の最大4%のペナルティを課される可能性があります。

GDPRは、データ保護目的のために、最終的にはプライバシーの目的のために、組織のデータ収集、移動、処理方法についての評価、テスト、および更新を強制します。組織は、収集されたデジタル情報とその収集理由を個人が理解するのを助ける明確なプライバシーポリシーを公表する必要があります。GoogleやFacebookなどの多くの組織では、ユーザーがその情報を管理および削除する方法ついても詳しく説明しています。

図1 - 従来のモデル

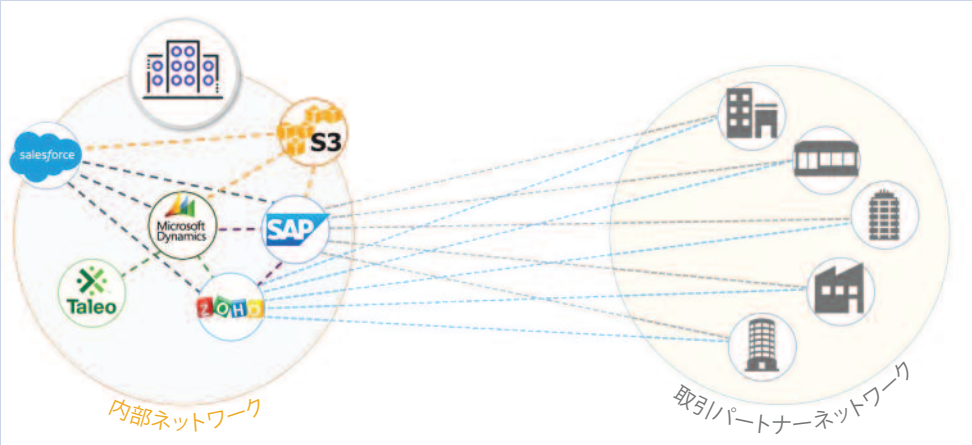

図2 - エコシステム駆動型統合プラットフォーム

これは、個人データの収集、保管、使用方法の改善を要求されている世界中の組織が、最新のエコシステム駆動型統合技術を評価、テスト、採用して、データを保護し、プライバシーとコンプライアンスを保証するガバナンスプロセスを利用することを意味します。

データ保護は本質的にデータプライバシーを保証するものではないかもしれませんが、これがなければプライバシーの約束を実現することはほとんど不可能です。しかし、データを保護するためのツールとデータの使用を確実に管理するための手順により、適切な統合プラットフォームを使用することで、組織は両方を実行できるようになります。

“データ保護は本質的にデータプライバシーを保証するものではないかもしれませんが、これがなければプライバシーの約束を実現することはほとんど不可能です。”

注釈

1 GDPREU.org、「Personal Data（個人データ）」、*https://www.gdpreu.org/the-regulation/key-concepts/personal-data/*
2 *同上*
3 GDPREU.org、「Data Controllers and Processors（データ管理者およびデータ処理者）」、*https://www.gdpreu.org/the-regulation/key-concepts/data-controllers-and-processors/*
4 *同上*

Enjoying this article?

- Learn more about, discuss and collaborate on information security management ISACA's Online Forums. *https://engage.isaca.org/onlineforums*