IBM Analytics
ホワイトペーパー

一般データ保護規則に向けての計画

IBMの支援でデータを保護、管理して、把握しましょう

概要

顧客情報を使えばトレンド、行動、支出に関するきわめて貴重なインサイトを得ることができます。これはターゲットを絞ったマーケティング、よりよい消費者への提案、さらには実用性の高い新製品にもつながります。しかし、個人情報の利用と保管は適切な取り扱いをしないと組織にとって大きなリスクにもなります。

これを念頭に、ヨーロッパ諸国は大量のデータ保護のルールを作り出してきました。データ・プライバシーとデータ・セキュリティの両方にまたがり、個人の直接的な同意、ないしは合法的な理由のない個人データ利用と戦うものです。これまで、これらのルールは時代遅れの1995年のデータ保護指令(DPD)に基づいているだけでなく、矛盾した形で強制されてきました。そのペナルティーも、ルールを遵守するために必要な時間や支出と比べれば小さなものでした。

一般データ保護規則(GDPR)はこれらすべてを変えそうです。2016年5月に交付されたGDPRは2年間の移行期間中です。2018年5月、これはEUマーケットで営業するないしはEUデータ主体(個人)の個人データを処理するすべての組織に即時に適用されます。

GDPRによると:

- **処理**とは個人データ、または個人データ群に対して実行されるあらゆる操作、ないしは一連の操作を指し、自動化された手段の使用有無は問いません。DPRではその具体例をあげて定義しています。
- **個人データとは**直接、間接に身元を示す、ないしはデータ主体の身元を明らかにできるあらゆるデータ、例えば名前、ID番号、位置データ、オンライン認証情報などと定義され、自然人である限りは顧客、従業員、その他の誰に属しているものであっても該当します。

こうも広いガイドラインなので、何の影響も受けない組織を探し出すことは不可能ではないとしても困難でしょう。GDPRはその越境的な性格から、対象範囲が広く、全世界レベルになります。例えばEUには拠点がなくても、EUデータ主体に物品、サービスを提供する、ないしは彼らの振る舞いをモニターする組織もGDPRに縛られます。物品やサービスの提供が有償なのか無償なのかは関係ありません。

現存の国内法に代わってGDPRはすべてのEU諸国に協調のとれた統合データ保護フレームワークを作ることを目指しています。そのゴールは:

- EUデータ主体のデータ保護権を強化、向上すること
- EU全体でデータ保護法令を一体化させてデータの自由な流れを促進すること
- 最新のテクノロジーに合わせて法律を近代化すること

第29条データ保護専門調査委員会(GDPRをヨーロッパデータ保護委員会[EDPB]として強制する予定の規制当局そのもの)は行動計画を作成して、GDPRが2018年5月に施行された時点から効果的に行動する準備を整えています。

組織も同様に今から対応すべきです。つまり、2018年5月までにGDPRに準拠するのに必要な人材、ポリシー、プロセス、テクノロジーを集めるということです。ギャップを突き止めて、データを保護し、管理し、把握するための手順を実装するために既存基盤を改築すべきときがやってきました。遵守できないと、2千万ユーロ、ないしは前年の年間総売上の4パーセントのどちらか高額なほうという巨額の制裁金につながりかねません。[1]

GDPRの主要な責任と義務

EUデータ主体のデータに触れる組織にとって、前述のGDPRのゴールは5つの主要な責任と義務としてまとめることができるでしょう。

1. **EUデータ主体の権利:**GDPRはEU内のデータ主体の権利を強化します。例えば、データ主体が自分の情報へのアクセス、ならびに消去を要求できることを成文化し、明確化しています。さらに、組織は個人データを容易にアクセスできるようにし、処理の内容をはっきりと分かりやすく示す必要があります。この情報を利用可能にすることで、データ主体は自分の情報がどう利用されているか把握できます。
2. **個人データのセキュリティ:**多くの組織にとって大きな変化は、72時間以内にデータ流出を規制当局に報告しなければならなくなることです。高リスクシナリオでは、この報告の後に、データが漏洩した可能性のある個人に通知しなければなりません。すべてのデータは適切な技術的な手段、手続きでそれに伴うリスクに適したセキュリティ・レベルを確保しなければなりません。組織にはセキュリティ対策をとる義務があります。データ流出が起きていなくても、プロアクティブな手順をとっていなければ法令違反になる可能性があります。
3. **適法性と同意:**個人データの処理が適法となるのは、GDPRのリストにある六つの要素の一つに該当するときだけです(例えば、契約の履行に欠かせない、他の法令遵守のために必要、法律上の命令など)。同意の取得もこの要素の一つですが、GDPRでは、きわめて証明が難しくなります。同意にはいつでも取り消しできることなど厳密な要件があります。同意が取り消されれば、適法にデータを保持したい、ないしはその必要がある組織は結局他の要素に頼らざるを得なくなります。
4. **コンプライアンスの説明責任:**組織は規制当局が権力を行使して、データや施設にアクセスする可能性があることを予期すべきです。いつでも個人データに関するGDPR原則の遵守を立証できるようにしておくべきです。この証明を行う手助けとなる手法、つまりデータ保護影響評価を行う、行動規範を厳守している、承認済の手法によって証明をプロアクティブに求めているなどの手法が利用できる予定ですが、今のところ完全に定義されているわけではありません。
5. **計画的なデフォルトでのデータ保護:**最終的に、データ管理者はGDPRの核となる原則を遵守していて、データ主体の権利が守られていて、特定の目的に必要なデータだけが処理されていることを実証する技術的、組織的な手段を実装しなければなりません。言い換えると、個人のデータ・プライバシーはデフォルトの動作でなければなりませんし、組織の、そして技術的な手順に最初から組み込まれていなければなりません。

2018年5月までにGDPRに準拠するのに必要な人材、ポリシー、プロセス、テクノロジーを集めましょう。ギャップを突き止めて、データを保護し、管理し、把握するための手順を実装するために既存基盤を改築すべきときがやってきました。

推奨事項

このホワイトペーパーでは、かなりの量のある法律を煎じ詰めて5つの主要領域にまとめています。それが要求する機能はかなり広い範囲になります。従って、重要なのは異なるGDPR要件すべてにどうやって組織として対応するのか、はっきりとした明確な思想を持つことです。この点に関して、IBMはGDPR遵守に向かう重要な手順の支援として使える機能、テクノロジーを同時にもたらすソリューション・フレームワークを作り上げました(図1)。

図1に示したのは:

- これらの要件に対応するために最終的に配置しなければならないポリシー、プロセス、規則、分析、監査機能のコンテキストの一番上に位置する5つの主要なGDPRの責任と義務。
- 構造化、非構造化、クラウド上、オンプレミスなど組織のあらゆるデータ・ソースと直接対話を通じてポリシーを実行する機能をもつデータ管理層。長期的には、できるだけ多くのポリシーにデータ管理層を自動的に対応させ、ポリシー実行も可能な限り自動化することがゴールになります。

図 1:IBM GDPRソリューション・フレームワーク。

- 継続的なコンプライアンス・モニタリングとセキュリティ事象や侵害のモニタリング。

このフレームワークの基本原則はオープン性と拡張性です。重要なデータ・プライバシー、セキュリティ活動の一部としてGDPRに必要な機能のいくつかに常に既存の投資を行うことになります。重要な点は、こうした投資がGDPRの要件拡大に対応して成長するにつれて、アーキテクチャーに組み込まれて保護されることです。

実用的な手順

こうした背景を念頭において、実用面を検討してみましょう。いくつか重要なプロセスを選んで、リスク評価を行うこともあるでしょう。この評価においては以下の質問に答えなければなりません:

- GDPRの範囲(EUデータ主体による自分の権利行使、データ侵害、規制当局の監査など)に含まれるかもしれない事象が起きる可能性はどの程度か、そうした事象が起きたときの結果はどうなるか?
- 現状と望ましい状態はどんなものか?
- その望ましい状態に到達するために必要な人材、ポリシー、プロセス、テクノロジーは何か?
- もっとも重要なテクノロジー・ギャップはどこに存在しているか?このギャップを埋める最善の方法は、既存投資の強化なのか、それとも新しい組織上、テクノロジー上の対策の導入か?

ゴールに向かって努力を始めたら、進展状況を確実に追跡、測定、監査します。

プロセスについて作業を行っている間が、データ評価実施に最適なときでもあります。この評価によって、企業内のどこに顧客データが存在しているのか、どこに個人データがあるのか、どれが廃止できる可能性があるのか、企業データの「お宝」はどこにあるのか、がよくわかります。EUデータ主体の要求ないしはデータ流出に対応するプロセスの設計にこの情報がきわめて重要です。

IBMの豊富な経験を活用しましょう

IBMは世界中のさまざまな業界の顧客に協力して、データ・プライバシー関連の事象への備えと対応を支援してきました。以下はその事例です:

- **通信**:データ・プライバシーとセキュリティの強化
- **銀行**:規制や法令のリスクへの対応支援に組織が利用できるソリューションの特定
- **製薬業界**:規制の要求と防御的な廃棄目標の支援
- **健康保険**:会員の機微データの評価と保護

通信

大手ヨーロッパ通信会社は新しいGDPRの準備で問題に直面しました。企業内のどこに個人データが保管されているのか、どのデータにコンプライアンスが必要で、セキュリティを強化しなければならないのか、まるでわかっていませんでした。

当初、この通信会社は人々にインタビューして、文書を調べることでデータを手作業で評価しましたが、この作業を大量の関連データに対応できる規模には拡大できませんでした。もっと自動化されたやり方が、しかも構造化、非構造化両方のデータが扱えるものが必要でした。

IBMと協力することで、個人の機微データをプロアクティブに探し出して、GDPRに備える最適の行動手順を決定できました。

銀行

ヨーロッパの金融サービス会社がバーゼル銀行監督委員会(BCBS) 239、Basel II、金融商品指令(MiFID)などの規則に準拠するのに大きな問題が発覚しました。既存アプリケーションが部分的にしか統合されていなくて、データの統合も不完全なためにデータ・サイロが生じていて、規制上の報告が遅れ、リスクの全体像も不正確でした。

IBM® Master Data Management (MDM)ソリューションを利用して、この金融サービス会社はデータ・ストアを使って顧客の統合された、正確な単一ビューを生み出して、顧客の完全なリアルタイム・ビューを実現しました。このソリューションによって、顧客エクスペリエンスを向上し、チャネルや連絡手段によらず同じ統合された顧客ビューが提供できるのでGDPRにも備えられるようになりました。

製薬業界

ある製薬会社のデータ・ガバナンス・プロジェクトには、さまざまな要件がありました。業務上価値のある情報や規制要件の対象になっている情報を維持するための効率的で適切な手法を確立する、訴訟に必要な情報を保存する、すでに必要のなくなったデータを注意深く廃棄する、といった要件です。

この会社はIBMと協力してIBM Global Retention Policy and Schedule Managementを実装して、規制の責任、義務、業務価値に基づいて業務でデータを維持、保管、廃棄するのを支援するポリシーを作成し、追跡しています。これによってコンプライアンス・リスクが減少し、不要な情報の日常的な防御的廃棄が可能になりました。

健康保険

健康保険会員1500万人以上、歯科保険会員1300万人、医療会員1000万人を抱えるある健康保険会社は、ほとんどの組織にはない規模の機微データを管理、処理し、それに責任を負っています。医療記録その他の健康関連情報のプライバシー、セキュリティ、長期的な保存を厳密に管理しながら、急速に増える医療記録、電子メール、報告書、処方箋、保険文書、その他の情報を適切に管理保管しなければなりません。

この会社は非構造化ファイル・システム内にある個人を特定できる情報を発見、管理するだけでなく、構造化データの階層保管管理戦略の実装を望みました。そのためには、どこに機微データがあるのかを理解して、さまざまなデータ・ソースにまたがったそのデータに対処しなければなりません。

IBMと協力してこの会社はIBM StoredIQ® for Data Assessmentを利用して、機微データの元の場所を突き止めて、それをより保護されたサーバーに移動しました。この会社はどこに情報が存在しているのか、データ・トポロジーを図示できました。部門、グループ、さらにはユーザー別のストレージ使用の概要もわかりました。機微データを突き止めて、粒度の細かいセキュリティを適用することで適切にマスクしました。記録を適切に分類しました。そして不要な情報を適切に廃棄しました。この健康保険会社は全社の最新データ・ソースに接続して、関連データの統合ビューを、数週間後ではなく数分で提供することができます。

GDPR対応計画をIBMと今すぐ始めましょう

GDPRはグローバルに営業している多くの業界の組織が直面している大きな問題です。しかし、GDPRの個々の主張の大部分は目新しいものではありません。IBMには世界中の顧客と協力して、エンタープライズ・レベルのソリューションをこうした広範な問題に提供してきた長い歴史があります。今すぐ行動して、データのリスクと義務を評価し、プロアクティブに情報を管理しましょう。2018年5月は思っている以上に急速に迫ってきています。

5つの重要なGDPRの責任と義務

1.EUデータ主体の権利

2.個人データのセキュリティ

3.適法性と同意

4.コンプライアンスの説明責任

5.計画的なデフォルトでのデータ保護

詳細情報

GDPRとデータを保護し、管理し、把握するためのIBMソリューションの詳細については、IBM販売担当者またはIBMビジネス・パートナーにお問い合わせいただくか、以下のWebサイトをご覧ください。

- **ibm.com**/analytics/us/en/technology/general-data-protection-regulation
- **ibm.com**/information-lifecycle-governance

IBM Analytics
Route 100
Somers, NY 10589

Produced in the United States of America
November 2016

[1] EU GDPR第83条(行政上の制裁金の一般条件)、5項と6項で定義されています。http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=NL

Please Recycle

IMW14906-JPJA-00