ISSUE 149

# BOARD PERSPECTIVES:

取締役会のリスク監視：Risk Oversight

## 取締役会におけるデータ・プライバシーに関する議論のフレームワーク

**データのグローバルな流通とデータ・プライバシーに関する規制の動向により、取締役会においてデータ・プライバシーに関して集中的に議論を行う必要性が増しています。**

サイバーセキュリティが継続した取締役会における課題である一方、急速に拡大する個人情報保護規制へのコンプライアンスを確保するためには、データ・プライバシーについても、対象を定めた取り組みを行う必要性がますます高まっています。プライバシーリスクは、組織が取得し保有するデータの量や種類により生じる課題です。進化する規制環境、ビジネスやテクノロジーの変化は、このリスクをさらに複雑にしています。取締役は、データ・プライバシーの主要な構成要素についてよく理解し、適切に質問する準備をしておく必要があります。

プライバシーに関する規制は、個人データ（個人に関連するデータ）の適切な取り扱いに重点を置いており、健康情報、社会保障番号、銀行口座、病歴など、さまざまな保護情報が含まれ、さまざまな当局や機関によって規制されています。また、新しいテクノロジーによるデータの作成や収集に伴い、個人データの定義も広がっています。取締役は、それら個人データの構成がどのようなものであれ、収集や利用、保護について、適用される法律および規則に従った適切なガバナンスを経営陣と議論する必要があります。また、個人データが収集や購入、変換や保存、共有され、収益の対象となるにつれ、この議論はより困難になっていきます。

当局の規制監視、サイバー攻撃のリスク、プライバシー保護に対する顧客（消費者）の要求が高まり続ける中、取締役は、データガバナンスや情報セキュリティに関するトピックについて、経営陣や企業のサイバーおよびデータ・プライバシー担当者と、取締役会で議論できる体制を整備する必要があります。そのため、以下では、データ・プライバシーに関する取締役会での議論に関連する8つのトピックを紹介します。

**データの種類や保管場所を把握していますか。**

企業は、企業の最も重要な情報関連資産（crown jewels）を特定・把握しておくことに加え、保有する個人データが適切にプライバシー保護管理されており、データがデータ主体のアクセス要求や削除要求に該当するか、開示義務があるか等を理解する必要があります。このような理解を進めていくと、組織は、構造化されているか否かにかかわらず、データを棚卸しすることによりカタログ化し、保管する必要があることに自ずと気づきます。

protiviti®
Global Business Consulting

また、個人データの収集方法や利用目的について、組織のプライバシー通知における開示と規制における義務の両方に則り、明確に文書化することが必要です。また、アクセス制御や暗号化技術など、リスクに応じた適切なセキュリティ管理を実施する必要があります。

個人を特定できる情報を保管する全ての組織にとって、定期的なデータの棚卸と評価は一般的な方法です。取締役は、適切なプライバシー情報の管理が行われていることを検証するために、組織が外部の関係者や知見をどのように活用しているか、経営陣に質問する必要があります。外部監査人がこのようなプライバシー情報管理の話を挙げる可能性があるため、経営陣は組織内の高リスクのデータを棚卸し、保護されたデータが規制やリスクに応じて適切に保護、共有、廃棄されていることを確認する必要があります。

### データを取得・保有する目的について、明確な見解を持っていますか。

取締役は、情報を収集する組織の事業目的、収集プロセス、および、データの利用について、顧客に伝達される通知の内容を理解しておく必要があります。「なぜ」は、「何を」と同じくらい重要です。取締役が考慮すべき質問には、次のようなものがあります。

- 企業は、適用されるプライバシーに関する法律や規制を遵守しながら、戦略を推進するために必要な特定のデータのみにデータの収集と保持を限定しているか。
- 企業は、収集した情報をどのように取得し、利用しているか。
- データ収集や管理要件に、考慮すべき業界特有の要因があるか。（例：医療機関、金融機関）
- 顧客（消費者）との接点であるさまざまなメディアにおける方針とプロセスを見直したか。

このように、組織のミッションや価値観は、取得するデータにも関係します。このような議論により、データ収集に関する情報が明確になり、データ・プライバシーのリスク管理方針が導き出されることがあります。これらは、専門家のレビューが必要な可能性があります。

### 自社が対象とするコンプライアンス要件を把握していますか。

現在、少なくとも世界62か国が独自のプライバシールールや義務付けを実施、または策定中です。つまり、米国の多くの州を含め、地球上の至る所にプライバシーに関する法律が存在します。複数の国や地域で新たに発生した独自のプライバシー要件に対応するためには、ビジネスプロセスのコンプライアンスを確保するための専門人材の強化や、より多くの投資が必要になる可能性があります。

取締役会は、社内外の法律顧問が改定される個人情報保護法を常に把握し、組織が関わる国や地域におけるデータ・プライバシー要件に関する知識を拡大する責任を、組織全体でどのように共有・文書化しているかを確認する必要があります。取締役は、特定された適用法令に基づき、グローバルかつ複雑なプライバシー要件に対処するための経営戦略を理解する必要があります。この戦略によって、組織内のどこにプライバシーリスクが存在し、投資が必要なのかが決まります。さらに複雑な要因として、判例法（裁判所の判断）が急速に進化しており、組織や取締役に対するリスクや罰則が拡大する可能性があることです。そのため、組織のプライバシー戦略を継続的に評価する必要があります。

### 自社の法的契約は、データ保護の要件に合致していますか。

個人データの越境移転は、ますます困難になっています。個人データを特定の地域内に留めることを義務付けている国もあれば、一定の法的義務を満たせば、個人データを他の地域へ転送することを認めている国もあります。

例えば、EUと非EU諸国間のデータ共有に関して、欧州連合（EU）が事前に承認した標準契約条項（SCC）[1]を企業が使用しているかどうかを、取締役は確認する必要があります。これらの条項は、個人の権利と自由を考慮し支持する目的で、個人データの送り手と受け手の双方が同意する標準的な条件を提供するものです。これらのSCCを採用することは、EU諸国とのデータ交換における規制要件であり、欧州委員会によって強制されています。また、取締役会は、契約条項内の合意事項を単に合意するだけでなく、合意事項に沿って運用されていることを確認する必要があります。

### 顧客（消費者）、従業員、第三者の個人情報をどのように保護していますか。

プライバシーリスク管理の重要な要素は、組織が保有する個人情報の保護です。情報へのアクセスを試みる敵対者のレベルは、組織化された詐欺的なフィッシング戦術や、ダークウェブでの攻撃プログラムの配布、高度持続的脅威（APT）など、ここ数年で劇的に上昇しました。

1 欧州委員会が事前承認した「標準契約約款（SCC）」（2021年6月4日）は、https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en を参照してください。

市場では、ゼロトラストアーキテクチャを利用して、全ての人が全ての情報に、常に安全にアクセスできるようにすることが一般的な傾向となっています。この考え方は、今日の顧客（消費者）やサプライヤーとのデジタル化されたやり取り、ハイブリッドな職場環境（オンサイトとリモートの組み合わせ）、拡大し続けるデータ保護要件、ますます巧妙化するサイバー攻撃やランサムウェアなどの複雑な状況に対応するために、企業が保護すべきデータにサイバーセキュリティ管理を近づけるという目的に適っています。

時間の経過とともに浸透しつつある実施策（プラクティス）は以下の通りです。

- 認証技術における強力な「継続した検証（本人確認）」の導入
- ネットワークアクセスの細分化（セグメント化）による攻撃対象領域（侵入時の「影響範囲」）の制限
- エンドツーエンド暗号化（送受信者の端末のみのデータ復号）とネットワークの継続的な監視
- データおよびアプリケーションへのアクセスを許可する際の最小限のアクセス権限許可
- プライバシー規制とデータ管理の積極的な統合を促すためのプライバシー・バイ・デザインおよびサイバーセキュリティ・バイ・デザインの導入

取締役会の立場からは、可能な限り強力なプライバシー保護を実現することを促します。

**個人情報保護のコンプライアンスの観点から、自社の問題点や対策を把握していますか。**

データ・プライバシーが優先事項であるにもかかわらず、企業はコンプライアンスへの準備において、障壁に直面しています。時間やリソースの不足、そして法律や規制の複雑さがその例です。

取締役会は、個人情報保護のコンプライアンス上の問題点を特定し、その重大性を評価し、個人情報保護プログラムを強化するためのベストプラクティスを適用するよう、経営陣に対して奨励する必要があります。この協議において、予算やリソースの充足度、結果に対する説明責任などの評価が含まれることがあります。また、健全性の審査（ストレステストプロトコル）、机上訓練（テーブルトップエクササイズ）、そしてそれらから得られる洞察もまた、取締役会の関心を集めています。

**自社のデータ・プライバシー管理の水準を把握していますか。**

消費者の個人データへのアクセスや利用状況、および企業のプライバシーガバナンスを測定する指標を確認することが出来る、さまざまなプライバシーツールが活用できるようになっています。これらのツールは、経営陣や取締役会が、戦略目標に対する組織のパフォーマンスを理解し、効果的に伝達するのに役立ちます。CEOや取締役会のダッシュボードに主要業績評価指標（KPI）を表示することは必須ですが、複数のツールからのデータを組み合わせなければいけないことが課題となる場合があります。今後、企業はツールの統合により、現在の自動化されたシステムやモデルを合理化し、より持続可能なプロセスや報告を実現することになると思われます。

また、環境・社会・ガバナンス（ESG）レポートによる評価の影響もあります。企業はESG報告に基づいて評価されることが多くなっており、組織のデータ保護能力の測定が今後より重視されるようになると思われます。そのため、内部告発や違反の外部開示、顧客（消費者）および従業員の個人データの損失による財務上およびレピュテーションへの影響を明確化することに関する方針は、善管注意義務（duty of care）の責任を果たす上で取締役会が注視すべき領域です。

**取締役会は、データ・プライバシーに関して、経営陣と一体となって取り組んでいますか。**

データの普及は、取締役会に課題をもたらしています。例えば、取締役会は、情報テクノロジー、サイバーセキュリティ、人事、法務、コンプライアンス等、複数の部門が各々の活動で収集、利用、保管するデータのプライバシーとセキュリティリスクについて責任を負っています。一部の取締役会では、データ・プライバシーのリスク管理に関するトピックを検討する技術委員会を設置しています。また、これらのトピックを監査委員会に割り当てたり、規制の厳しい環境ではコンプライアンス委員会に割り当てたりする場合もあります。上場企業の場合、これらの問題は、データ・プライバシーのリスク管理に助言を与える委員会の全ての会合において、毎回、あるいは必要に応じて検討する価値があります。すなわち、効果的な分析とダッシュボードを整備することの重要性を強調しています。

B to Cのビジネスモデルを持つ企業では、これらの問題にさらに注意を払う必要があります。取締役会は、少なくとも年に一度、データ・プライバシーのリスク管理のパフォーマンスに関する報告または説明を受ける必要があります。取締役は、首尾一貫したデータ・プライバシーガバナンスのプロセスが確立され、ビジネス戦略と整合したデータ・プライバシーの保護を可能にする効果的なコントロールによって補完されているという信頼を得る

目的で、企業のリーダーシップを発揮する必要があります。

上記のテーマや質問は、企業の業務に内在するリスクを考慮し、取締役会で熟考されるべきものです。

## プロティビティの支援

世界中の組織は、データ・プライバシーを取り巻く環境にかつてないほどの変化にさらされています。州、連邦、およびグローバルな規制の進化により、ビジネス、テクノロジー、および法的な運用の調整がほぼ常時必要となっています。これらの変化は必ずしも互いに排他的ではなく、しばしば重なり合い、非常に複雑な法的規制のシナリオを生み出しています。

プロティビティのデータ・プライバシー・コンサルティング・チームは、効果的なプライバシーおよびデータ保護プログラムの開発および維持のため、お客様が直面するデータ・プライバシーの固有リスクと課題を理解しています。

プロティビティは、コンプライアンス、ビジネスプロセス、テクノロジー、情報セキュリティ、コミュニケーションのスキルと経験を生かし、お客様と協力して、法規制や義務の理解、ニーズの把握、適切なコンプライアンスや保護の対策の実施、新しい規制や変化への対応に取り組んでいます。



protiviti®