bsi.

...making excellence a habit.™

プライバシー規制

ISO/IEC 27701の役割を理解する

著者: Kieran McDonagh, Riskscape Law Ltd

ホワイトペーパー

目次

はじめに

個人データのプライバシーについては、非常に話題になっています。組織は、お客様、従業員、ビジター、近隣住民の個人情報の取り扱い方法を慎重に検討しなければなりませんが、多くの組織にとってこれは困難なことです。2018年5月にGDPR（一般データ保護規則）が適用されたことで、どこに拠点があろうとも、EU市民の個人データを扱う場合は、すべての組織がGDPRを順守しなければならなくなりました。EU以外では、少なくとも132カ国がプライバシー法を制定しています。 これらの国々の間で個人データを転送する組織は、プライバシー保護のための管理策を検討する際に、各関連法を考慮しなければなりません。

このような法律への準拠を支援するための管理策の導入および監視は、複雑な課題となる可能性があります。このような状況をより管理しやすくするために、規格を導入することで、組織は規制順守のためのステップの実施に自信を持つことができます。役立つ規格として、国際的に合意された規格であるISO/IEC 27701があります。これは、組織が既存のISO/IEC 27001 情報マネジメントシステム（ISMS）を拡張して、プライバシー要求事項に対応できるようにするための規格です。

本ホワイトペーパーでは、プライバシーに関連する規制の概要、ISO/IEC 27701が果たすことのできる役割、そして企業や消費者にとって意味することについて説明しています。

欧州のプライバシー事情

欧州の消費者数百万人の個人データは、2018年5月25日以降、GDPRにより法律で保護されています。 個人データを扱うすべての組織は、その規模を問わずGDPR、またはGDPRを組み込んだローカル法に準拠しなければなりません。 例えば、英国で、これはデータ保護法2018(DPA 2018)に準拠することを意味します。

2009年にリスボン条約を通じて法的効力を持つようになったEU基本権憲章には、個人のプライバシー権が含まれています。GDPRは、このプライバシーの権利に基づいて構築されているため、個人データを収集、分析、共有、保存、削除（以下、総称して「処理」といいます）する際には、プライバシーを考慮しなければならないとしています。GDPRには、個人データの処理に際し次の通り要求する一連の原則が含まれています:

- 個人のために合法的、公正かつ透明性をもって処理されること
- 特定の目的のために収集され、他の目的のために再利用されないこと
- その収集および処理は最小限にすること
- 常に最新の状態を維持すること
- 可能な限り最短の保存期間とすること
- 不正な処理、損失、破壊または損傷から保護されていること

GDPRは、個人データのプライバシーを保護するために実施しなければならない管理策の種類を定めています。GDPRでは、個人データの処理方法を検討する際に、そのような処理が個人データを処理される個人の権利及び自由に対して高いリスクを与えるかどうかを評価することを要求しています。 このような評価は、個人データが処理される様々な状況で適用する必要があります。 組織によっては、これらのリスクを評価することが難しく、この評価の実施方法について、規制当局に助言や指針を求めた組織もあります。

ISO/IEC 27701の役割

ISO/IEC 27701規格は、ISO/IEC 27001 (ISMS)を拡張し、プライバシーに関する要求事項を組み込んだものです。多くの組織がすでにISO/IEC 27001 (ISMS)を導入しており、基盤が整っているため、プライバシー情報マネジメントシステム（PIMS）を構築する際の複雑さは軽減されます。ISO/IEC 27001に精通している組織に対しては、プライバシーに対応するためにISMSを拡張し、プライバシー情報マネジメントへの取組みを実証する手段を提供することで、GDPRや他のプライバシー法への準拠を支援することができます。

この規格では、個人データまたは個人識別可能情報（PII）の管理を体系的かつ透明性のあるものにするために、実施しなければならない管理策を特定しています。これは、組織がPIIのコントローラまたはプロセッサとして活動する場合に必要な管理策を定めたものです。

本規格の管理策は、PIIの収集、分析、共有、保存、削除のライフサイクル全体を対象としています。GDPRが要求しているように、PIIに関連する個人は、これらの管理策の中心に置かれます。

規格のベネフィット

グローバルでの一貫性

組織は多くの場合、複数の国で活動しているため、異なる法域のもと順守しなければならない多くのプライバシーおよび情報セキュリティ要求事項があります。国際的に認められた規格を使用することで、組織はすべての要求事項をまとめ、コンプライアンスを達成および維持するために、一連の処置として集約することができます。これは、PIIを国境を越えて転送する際、国境をまたぐ両国に異なる法律や管理要求事項が存在する場合に、組織にとって特に重要になります。

利害関係者の関与

また、規格は、取締役会または顧客代表など組織の利害関係者が設定する追加要求事項を組み込むための構造を提供することができます。

ベストプラクティス規格に基づくプライバシーおよび情報セキュリティ準拠のための標準化されたアプローチはコンプライアンスプログラムの開始、中間、および終了を明確に示します。 規格の要求事項を満たすことで、コンプライアンスを達成または維持するためのビジネス事例を支援するために使用することができ、シニアマネジメントにとって問題を具体化するのに役立ちます。このようなプログラムを成功させるには、利害関係者による強力な支持が不可欠です。

プログラムマネジメント

あらゆる資本支出を正式なプロジェクトで管理することを義務づけている組織は、プログラムマネジメントのフレームワークとして規格を使用し、変更および「通常通り」の活動の両方のリスク評価、緩和、監視活動を組み込むことができます。

プログラムでは多くの場合、要求事項およびプロジェクト目的を特定するための正式なプロセスを使用し、それらを組み合わせることで真の価値を生み出すことができます。規格は、まさにこれを行うための構造を提供し、内部または外部審査と組み合わせることで、コンプライアンス活動を調整するための緊密なフレームワークを提供します。これにより、周辺の課題に気を取られたり、脱線したりすることなく、コンプライアンスの達成および維持に集中することができます。

プログラムマネジメントの一環として規格を使用することで、異なる部門、地域、技術的な職務が、透明性のある単一の要求事項に基づいて協力することができます。これは、国境を越えたデータ転送が複数の国で管理される場合に不可欠です。

また、プロジェクト・デリバリー・アプローチを採用することで、シンプルな指標を用いて進捗状況をシニアマネジメントに説明することができ、コンプライアンスを達成および維持するための作業に信頼性を与えることができます。プライバシーおよび情報セキュリティの準拠に向けた進捗状況をシニアマネジメントにわかりやすく提供することは、GDPRなどの新しい法律に関連する法的リスクの管理に不可欠です。特に、コンプライアンス違反に対する罰金は数百万ドルに達することもあるため特に言えることです。

社内教育

また、規格文書は、その規格の技術分野における専門家以外の人を教育するためにも利用できます。また、組織全体で意識改革を行う研修プログラムを確立したり、技術スタッフをその分野の専門家として認定したりすることも有効です。組織がコンプライアンスを順守するためには、すべてのスタッフ、コンサルタント、請負業者、ビジター、および第三者が、プライバシーおよび情報セキュリティ管理策を適切に実施し、順守しなければなりません。各グループは、それぞれの責任を十分に認識し、管理策を効果的に運用する方法を確実にするために、それぞれのニーズに沿った特定の研修プログラムを必要としています。 規格は、異なるグループ間における共通のメッセージを共有しながら、研修プログラムを包括的に行うためのフレームワークを提供します。

保証

規格は、管理策をテストするためのフレームワークを提供し、成功したテスト結果を用いてプライバシーおよび情報セキュリティに関する保証を提供するためにも使用できます。これは、管理目標として変換される要求事項を確立するのに役立ち、プライバシーおよび情報セキュリティ要求事項に準拠するために、組織が実施しなければならない管理策の特定を支援することができます。そして、内部および外部の利害関係者に保証を提供するために、管理策のテストを計画し、実施し、報告することができます。規格により、このワークフローが体系的に整備され、シニアマネジメントの目標を達成するためのプロジェクトとして管理することができます。

公認規格への準拠の達成および維持を実証することは、規制当局およびサプライチェーン全体のサプライヤーなど、内部および外部の利害関係者に保証を与えることにつながります。どちらも、組織がプライバシーおよび情報セキュリティ要求事項を順守していることを保証する必要があり、サプライヤーはコンポーネントまたはサービスを受け入れる前にこれを必要とします。この要求事項は、サプライチェーン保証においてますます重要なものとなっています。 規格は、サプライチェーンの上流および下流双方のパートナーが情報共有のリスクを理解し、データ転送に追加の管理策を実施することで、残留リスクを低減することができるような管理策のベースラインを提供します。

積極的な取組み

プライバシーおよび情報セキュリティ管理策をどれだけ整備しても、組織はデータ侵害のリスクは依然抱えています。組織が規格に準拠しているにもかかわらず、プライバシーまたは情報セキュリティ侵害を被った場合、組織は、ベストプラクティス規格に準拠しているにもかかわらず侵害を被ったと主張することができます。このように組織が順守するための最善の努力を実証することができず、自らを危険にさらすことにもなりかねません。

このような侵害を関連する規制当局に報告する際、公認規格に準拠していることで、規制当局に対して、管理策が体系的に整備されており、侵害の後も容易に強化できることを保証することができます。規格への準拠を実証しなくても、成熟した管理環境があり、プライバシーおよび情報セキュリティ要求事項に真剣に取り組んでいることを規制当局に納得してもらうために、組織はより努力する必要があるかもしれません。

このような状況で規制当局と話し合いをすると、しばしば制裁を受けることがあります。組織は、公認規格への準拠を、制裁または罰金に対する議論の緩和要因として利用することができます。GDPRの罰金は、グローバルの年間売上高の4%という多額のものになる可能性があるため、公認規格に準拠することで得られる投資効果は非常に大きいものになるでしょう。

重要な概念

プライバシーおよび情報セキュリティ要求事項の用語は、この分野に慣れていない人にとっては難しいものです。しかしながら、重要な概念を定義することが、国際規格を策定する作業の中心であるため、支援は可能です。 規格は、実務者が管理策を実施する日々の作業で使用可能な、国際的に認められた重要な概念の定義を示すものです。ISO/IEC 27701および関連規格は、プライバシーおよび情報セキュリティにおけるコンプライアンスプログラムにとって必要な多くの重要な概念を定義しています。これらの重要な概念のいくつかを以下に説明します。

定義: 個人識別可能情報 (PII)

ISO/IEC 27701:2019では、情報セキュリティおよび関連する管理策を対象とするISO 2700x規格群に共通する用語を使用しています。これは、PII主体または個人に対してセキュリティおよびプライバシーを提供する際に、保護および管理しなければならない情報資産を表すために、個人識別可能情報（PII）という用語を使用しています。

PIIは、ISO/IEC 29100:2011の箇条2.9で、単独、または他に紐づけられた情報と組み合わせて、PII主体または個人を特定するために使用できる情報と定義されています。この用語は、医療記録およびその他の個人的な健康情報の保護を目的としたHIPPA（医療保険の相互運用性と説明責任に関する法律）などの米国連邦法で最もよく使用されます。 そのため、例えば、個人のIPアドレスはそれ自体がPIIではありません。ただし、IPアドレス表の名前など、他に紐づけられた情報と組み合わせることが合理的に可能な場合は、PIIとなります。

機微PIIは、ISO/IEC 29100:2011の箇条2.26で、PII主体または個人の最も私的な領域に関連する情報を含むPII、または開示された場合に個人に重大な影響を及ぼす可能性があるPIIと定義されています。

個人データ – EUの用語

EUでは、GDPRの中で「個人データ」という言葉が使用されています。「個人情報」とは、第4条において、合理的な手段を用いて個人を特定することができる、個人に関するあらゆる情報と定義されています。そのため、例えば、名前が公開されていなくても、IPアドレスによって個人をプロファイリングすると、その情報は「個人データ」となります。

EUでは、GDPR第5条において、特別なカテゴリの個人データとは、個人に関する最も私的な領域を明らかにするものであり、EU基本権憲章に基づく権利および自由の行使を妨げる可能性があるものと定義されています。例えば、個人の人種または民族的起源、宗教的信条、性的指向などの情報は、特別なカテゴリの個人情報とみなされます。GDPRでは、こうした情報を追加のプライバシー管理策で保護することが求められています。

定義: プライバシー

「プライバシー」とは、PIIの「処理」に対する適切な管理策の最終結果を表す用語とみなすことができます。ISO/IEC 29100:2011の箇条2.22には、プライバシー利害関係者の定義として、PIIの処理に関連した意思決定もしくは活動に影響を与える可能性のあるPII主体または個人が含まれています。 よって、プライバシーとは、PIIの処理の結果としてPII主体または個人に悪影響が及ぶのを防ぐことと定義することができます。

GDPRでは、プライバシーについて定義していませんが、その目的として第1条で、個人データの処理に関する個人の基本的権利および自由の保護、特に個人データの保護に関する権利を謳っています。

PIIのプライバシーに対するリスクは、ISO/IEC 29100:2011の箇条2.19において、事象、その結果又はその起こりやすさに関する情報のギャップがPIIのプライバシーに及ぼす影響として定義されています。

プライバシー管理策は、ISO/IEC 29100:2011の箇条2.14で、プライバシーリスクの起こりやすさ又はそれが起きた結果の影響を低減することによって、プライバシーリスクを処理する組織的、物理的、および技術的な対策として定義されています。

定義: 情報セキュリティ

適切な情報セキュリティがなければ、プライバシーを守ることはできません。適切な情報セキュリティは、PIIのプライバシーを守るために必要ですが、それだけでは十分ではありません。PIIの開示、紛失、破損を防ぐには、情報セキュリティ管理策によってPII処理のライフサイクル全体が保護されていなければ効果的ではありません。ISO/IEC 27000: 2018の箇条3.28では、情報セキュリティを情報の機密性、完全性、および可用性を維持するための適切な管理策の最終結果と定義しています。

機密性は、ISO/IEC 27000:2018の箇条3.10で、情報を受け取る権限のない者に情報が開示されない情報セキュリティの特性として定義されています。開示は、組織の外への意図的な情報漏えい、間違った人物への偶発的な開示、または不正確なアドバイスに基づく意図的な転送の結果である可能性があり、これらは不正な開示となります。

完全性は、ISO/IEC 27000:2018の箇条3.36で、情報がその正確さおよび完全さを保持する情報セキュリティの特性として定義されています。また、これらの特性をユーザに保証するために、情報の正確さおよび完全さを更新するための管理策を整備することが望ましいです。

可用性は、ISO/IEC 27000:2018の箇条3.7で、情報が必要に応じて認可されたユーザからアクセス可能になるという情報セキュリティの特性として定義されています。情報にアクセスするためのユーザの要求事項は、ビジネスプロセスの重要性によって異なります。したがって、あらゆる状況下で情報を提供するために必要な取決めの精巧さも異なります。

GDPRでは、第5条で個人データの情報セキュリティの原則を定めています。これは、不正または違法な処理、および偶発的な損失、破壊、損害から個人データを保護するために、適切な技術的または組織的な手段を使用することを要求するものです。

ISO/IEC 29000:2018の箇条3.28では、真正性、責任追跡性、否認防止、信頼性など、情報セキュリティの他の特性も情報セキュリティの一部とみなすことができるとしています。ほとんどの実務者は、これらを機密性、完全性、可用性のサブプロパティとみなしています。

定義: 管理策

管理策とは、リスクを処理するための手段を提供する活動のことです。 ISO/IEC 29000:2018の箇条3.14では、管理目的を管理策により達成することを求められる事項を記載したものと定義しています。 箇条3.61では管理策をリスクを修正する対策と定義していますが、プライバシー管理策の場合は、プライバシーリスクを修正するとしています。GDPRでは、管理策または管理目的を定義していません。

グッドプラクティスでは、特定のプライバシーリスクに対処するための管理目的の特定をサポートします。一つのプライバシーリスクは、複数のプライバシー管理目的に当てはまる可能性があります。各管理目的は、効果的な運用によりPIIのプライバシーリスクに対処する一連の管理策（組織的なもの、技術的なもの）を設計することを要求しています。ISO/IEC 29000:2018の箇条2.14でプライバシー管理策は、プライバシーリスクが顕在化することの起こりやすさまたは結果を低減するものと定義されています。ISO/IEC 27701に準拠するためには、それぞれの管理目的を定義し、各目的を満たすように管理策を設計する必要があるため、PIIのプライバシーをともにサポートする管理策のフレームワークを提供します。

定義: テスト

テストとは、管理策の設計またはその運用の有効性を評価する活動です。適切なテストが行われなければ、管理目的を達成するためにその管理策が適切であるかどうかを正確に評価することはできません。 同様に、管理策の運用について適切なテストを行わなければ、その管理策がリスクの処理に有効であるかどうかを正確に評価することはできません。

テストのグッドプラクティスでは、事前にテスト計画を作成する必要があります。 計画では、以下のことを定めることが望ましいです:

- 管理目的
- テストされる管理策の設計の特性
- 設計を評価するための基準
- 運用中の管理策のアウトプットに対するサンプル規模
- 効果的な運用を実証する閾値受容レベル
- テスト結果の許容範囲および許容範囲外の報告基準

プライバシー管理策のテストでは、PIIを扱うビジネスプロセスの分析で示された中心的なユースケースを考慮するすることが望ましいです。ただし、すべての状況で完璧に動作するビジネスプロセスは存在しないため、テストでは、ビジネスプロセスが誤って動作したり、悪意のある内部または外部のエージェントによって中断されたりするユースケースも考慮しなければなりません。一連のユースケースのテストが成功して初めて、プライバシーリスクが管理されていると考えることができます。

外部の情報源は、PIIのプライバシーに対するリスクを助長する可能性があります。例えば、最小化の原則は、組織がPIIをほとんど収集しないことを意味します。 しかし、収集されるPIIがどんなに少なくても、他のデータソースと組み合わせれば、個人が特定され、プライバシーがリスクにさらされる可能性があります。プライバシーリスクのテストでは、外部のデータソースを組み合わせて個人を特定するシナリオも考慮することが望ましいです。有名な例では、あるジャーナリストが異なるデータソースを組み合わせて、情報コミッショナーの名前でパスポートの申請を成功させたことがあります。

ISO/IEC 27701に準拠するためには、組織が扱うPIIのプライバシーに対するリスクが評価され、管理策が導入され、管理策テストの包括的なフレームワークを通じて管理策が効果的に機能していることを実証する必要があります。そのため、テストはこのプロセスの中心的な役割を果たします。

グローバルプライバシー規制状況の概要

GDPRの適用に関する重要な情報源は、欧州データ保護委員会（EDPB）です。データ保護影響評価の実施など、さまざまなトピックのガイダンスを発行しており、オンラインで入手可能です (https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en)。

EDPBは、1998年データ保護法として英国法に組み込まれたデータ保護指令95/46/ECによって創設された前身組織である第29条ワーキンググループの役割を引き継いでいます。EDPBが設立された際、従業員の監視および侵害の通知などのトピックについて、1997年以降に発行されたガイダンスをすべて採用しました。 このガイダンスはすべてオンラインで入手可能です All of this guidance is available online (https://ec.europa.eu/justice/article-29/documentation/index_en.htm)。

EDPBは、ガイダンスが必要と思われる領域を検討する際に、英国個人情報保護監督機関（ICO）（www.ico.org.uk）やフランス共和国データ保護機関（CNIL）など、EU内の各データ保護当局（DPA）の間でコンセンサスを得るように努めています。

DPAは、個人データの処理を管理する組織の登録、組織および個人への助言、個人からの苦情への対応、データ侵害が発生した組織の調査および罰金を担当しています。また、DPAは、個人データの処理がGDPRに準拠していないと判断した場合、組織を提訴します。

GDPRのいくつかの側面をどのように順守するかについてはまだ曖昧な点がありますが、DPAが組織の非準拠を理由に提訴した事例は、DPAおよび裁判所が組織に対し法律を順守させることをどのように期待しているかについての有益な指標となります。 EUの最高裁判所である欧州司法裁判所に上告された場合、その判決は決定的なものとなります。これらの事例は、最も複雑な状況下でGDPRをどのように実施するかを示す傾向があります。これらの事例はオンラインで報告されています (https://eur-lex.europa.eu/homepage.html?locale=en)。

GDPRのグローバルな影響

GDPRは、データがどこで処理されるかに関わらず、欧州市民の個人データを対象としているため、世界中の組織にとって高い基準となっています。その他の国では、自国のデータ保護法の改正を検討する際に、グローバルソーシャルメディアの時代におけるデータ保護の最新モデルとしてGDPRに注目しています。ブラジルは、GDPRの原則の多くを採用する、2020年施行の新しいデータ保護法（LGPD）を導入しました。また、同じく2020年施行の新しいカリフォルニア州消費者プライバシー法（CCPA）は、GDPRの概念の一部を採用しています。ワシントンD.C.の立法者たちは、CCPAを先取りする可能性のある連邦データプライバシー法の導入を目指して交渉しており、GDPRと同様の保護を実現することに注力しています。そのため、GDPRに準拠していれば、国際的な法律に準拠するために必要な労力は少なくて済みます。

その他の欧州のプライバシー法

GDPRは、EUの機関における良好なデータ保護の実践を求める「規則（EU）2018/1725」と、EUの法執行機関における良好なデータ保護の実践を求める「特定データ保護指令（680/2016）」の2つの法律と並行して策定されました。規則（EU）2018/1725は、2018年12月11日にEU機関に対して発効されましたが、指令は、地域の有効化法を通じて各法域で発効されました。それは英国のDPA2018に組み込まれ、2018年5月23日に施行されました。コピーはオンラインで入手可能です (http://www.legislation.gov.uk/ukpga/2018/12/contents)。

AdTechのビジネスモデルが問われるeプライバシー規則

GDPRおよび指令に加えて、EUでは、2002年の電子通信プライバシー指令 (2002/58/EC)またはeプライバシー指令を更新するための新しい法律を策定しています。この指令は、2003年のプライバシーと電子通信に関する規則（PECR）を通じて英国で法的効力を持ち、「クッキー法（cookie law）」として知られるようになりました。

導入当時、「クッキー」法は、インターネットサイトがユーザのコンピュータにクッキーを置くために、ユーザに許可を求めることを義務付けていました。 ただし、これがどのように機能するのか、法律では明確にされていませんでした。企業は、ユーザが過去にコンピューターへのクッキー配置を拒否したかどうかを確認するためにユーザの設定について会社に通知可能なクッキーを既に配置している必要があることを懸念していました。
また、ウェブサイトにアクセスする度にクッキーが置かれることにユーザは同意しなければならないのか、それとも最初のアクセス時だけかについても、法律では不明確でした。こうした混乱により、法律が広く解釈され、多くのサイトが法律の精神に準拠していませんでした。

今回のeプライバシー指令の改訂は、2002年の旧法以降のインターネット上での個人データ処理における変化に対応し、GDPRと要求事項を合わせることを目的としています。この新法は、GDPRと同様に規則となるため、EU全域で一律に適用されることになります。規則の最新ドラフト（2019年3月13日）では、電子的な「対人通信」の一環としてのあらゆる個人データの処理を、GDPRと同様のプライバシー管理策の対象としています。

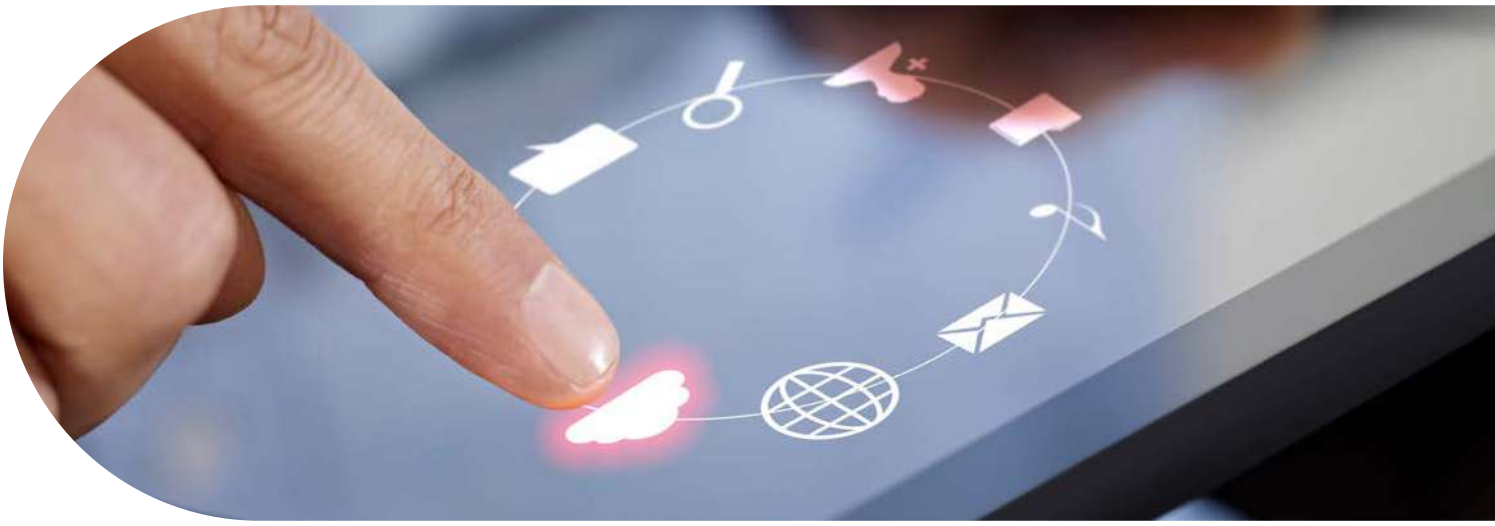
メタデータの処理についても、本規則の作成時に考慮されています。 オンライン上の個人データの処理に関連するメタデータも個人データに分類されるかどうかは、まだ決着がついていない課題ですが、判例はこの結果を後押ししているようです。これにより、メタデータも個人データと同様のプライバシー管理策が必要となります。

サイトでのアクティビティを記録するためにクッキーを使用することについて、ウェブサイト訪問者に警告する必要性は、元の指令における最も一般的な側面でした。このように、訪問の度に警告を発するという要求事項は新規則で削除されるのではないかと期待されていました。

最新のドラフトでは、ブラウザ設定でクッキーに対する一般的なオプトインまたはオプトアウトを可能にすることで、訪問者の負担を軽減しようとしています。しかしほとんどの場合、同意が必要となります。同意のレベルはGDPRのレベルを満たし、「自由に与えられ、具体的で、十分な情報を与えられ、明確である」ことが期待されます。 また、ウェブサイトは、個人データがどのように処理され、どの第三者に転送されるかを訪問者に知らせる必要があります。一部のウェブサイトでは、このGDPRの要求事項を反映したクッキー同意バナーの設定をすでに始めていますが、ICOは大多数のウェブサイトがまだGDPRに準拠していないことをすでに強調しています。

組織によっては、処理の制限、顧客への通知、同意の確保が課題となります。この課題に対応できない場合、ビジネスモデルを変更しなければならない組織も出てくるでしょう。ICOは、2019年6月に発行したAdtechに関する出版物 (https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf)の中で、組織にこのリスクを警告しています。

eプライバシー規則は、2019年後半または2020年に最終決定され、24ヶ月以内にすべてのEU加盟国で自動的に法律となる予定です。 その他の欧州経済地域の国々（ノルウェー、リヒテンシュタイン、スイス）は、本規則を自国に適用するための予定について交渉することになります。第三国では、二国間で交渉し、特定の国の組織がEU市民の個人データをオンラインで処理することを希望する場合など、eプライバシー規則の要求事項を現地の法律に反映させる必要があります。



大規模なデータシートを処理する企業にとっての 競争法上の課題

大量の個人データを処理する組織は、その処理が競争法にも抵触する可能性があることに気づいています。

競争法は、市場での支配的な地位を利用して、同じ市場において他の組織による競争を低下させることを防止することを目的としています。 ソーシャルメディア・プラットフォームなどの組織が、多くの人の個人データを処理する場合、市場調査データの収集やディスプレイ広告の提供などの市場において支配的な地位を占めていると考えられます。 新規参入企業は、何百万人もの既存顧客とそのインターネットデータによる恩恵を受けられないため、既存のソーシャルメディア・プラットフォームに対抗するのは難しいかもしれません。このような支配的な立場が、他の組織がこうした市場調査データを収集することを妨げ、市場での競争を低下させると考えられる場合、ソーシャルメディア・プラットフォームは競争法の監視対象となる可能性があります。

EUでは、欧州委員会の競争総局が、特定の市場における特定の組織の市場シェアを見て、市場での競争にリスクがあるかどうかを判断する傾向があります。競争法によって市場調査データの市場における支配的な地位が認められた場合、制裁措置としては、反競争的な行動に対する罰金、子会社の売却、支配的なグループの解体などがあります。 欧州委員会は、ソーシャルメディア・プラットフォームが他社との競争を阻害しないようにするための新たな規制のあり方を積極的に検討しています。

オンラインに掲載された個人情報による被害

いわゆるWeb 2.0では、ユーザが自分で作成した素材をオンラインで投稿すると、その素材は個人情報とみなされます。ホスティングサイトは、こうしたデータのプライバシーを保護するだけでなく、ユーザによる作成素材をホスティングすることが第三者への損害につながるかどうかも考慮しなければなりません。ソーシャルメディア・プラットフォームを、単にプラットフォームの基盤技術を提供するテクノロジー企業としてではなく、個人の投稿の発行者として規制すべきだという声が、多くの国で高まっています。

ニュージーランドで出版社は、2015年に制定された「Harmful Digital Communications Act（有害なデジタル通信法）」により、ユーザによる作成素材のホストは、特定のコンテンツに関する苦情が出された場合、その著者が苦情を無視した場合でも、オンライン素材を削除することが義務付けられています。 2019年4月、英国政府はユーザによる作成素材のホストに「注意義務」を課すことを提案するホワイトペーパーを発行しました。(https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/793360/Online_Harms_White_Paper.pdf)。 法制化されれば、子どもまたは弱い立場の人々にとって有害な内容が含まれていると判断された投稿は、厳格な時間内に削除することが求められることになります。 アイルランドも同様の法律を検討しています。米国では、ソーシャルメディア・プラットフォームに、ユーザが作成したコンテンツに対する責任を求める声が上がっています。米国議会はこの課題を十分に考慮し、ソーシャルメディア・プラットフォームに対し、オンライン上の被害にどのように対処しているかについて証言するよう求めています。

ユーザによる作成素材のホストを、技術者ではなく発行者と見なす方向で法律が動いているようです。このような状況の変化は、主要なソーシャルメディア・プラットフォームだけでなく、すべてのオンラインホスティングプラットフォームに大きな影響を与えます。ユーザによる作成素材をホストする組織は、投稿を精査し、有害と思われるものを速やかに削除するための新しいビジネスプロセスを構築しなければならないかもしれません。

プライバシーおよび情報セキュリティ規格の導入

規格は、プライバシーおよび情報セキュリティに関する法律や規制を順守しようとする組織にとって、管理目的のベースラインを提供するものとして役立ちます。複数の法律を順守しなければならない場合、単一の規格を使用することで、各法的要求事項を単一の構造にまとめ、組織にとってコンプライアンスの取組みの焦点として使用することができます。規格を導入することで、組織は規制当局やサプライヤー、顧客に対して、プライバシーおよび情報セキュリティ管理策を備えているだけでなく、シニアマネジメントがこれらの課題に真剣に取り組んでいることを示すことができます。

GDPR 認証への挑戦

EDPBは2019年6月に、組織がGDPRに準拠していることを実証するための新しい認証スキームの要求事項に関するガイダンスを発表しました (https://edpb. europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201901_v2.0_codesofconduct_en.pdf) 。将来的には、データ主体のアクセス要求、苦情処理プロセス、プライバシー・バイ・デザイン、データ主体とのコミュニケーションなど、GDPR準拠の全側面を対象とする認証スキームが開発される可能性があります。

現在、GDPRのすべての側面を対象とする認証スキームはありません。EDPBは、一部のGDPR管理策のみを対象とする認証スキームが、組織がGDPRに対し全体的に準拠していることを示すのに役立つと指摘しています。そのため、当面の間、ほとんどの組織では、寄せ集め状態の認証スキームがGDPR認証の基盤となることが予想されます。

プライバシーガバナンス

組織が変化する環境に対応するためには、優れたビジネスガバナンスが重要であり、それを支援するために様々な規格が用意されています。例えば、マネジメントシステム規格は、品質マネジメントや安全衛生、プライバシーおよび情報セキュリティなど、様々な分野において組織がリスクを管理し、パフォーマンスを向上させるのに役立ちます。

マネジメントシステムによる取組みのベネフィット

ビジネスプロセスまたは製品に対する規格に準拠することは、組織が特定の分野において発展することにつながります。しかし、マネジメントシステム規格を導入するには、組織内のすべての機能に影響を与える、より強固な取組みが必要です。マネジメントシステム規格が効果を発揮するためには、組織の既存のマネジメントに組み込まれていなければなりません。

マネジメントシステム規格は、規格への準拠を常に堅牢なものとし、長期的に持続可能なものとすることに重点を置いています。この種の規格は、組織全体の管理をより体系的かつ透明性のあるものにします。規格に準拠することは、組織がそのマネジメント責任を真剣に受け止めていることを実証するものとなります。

リーダーシップの関与

マネジメントシステム規格の主な特徴は、組織のシニアマネジメントが関与することを要求していることです。これにより、プライバシーおよび情報セキュリティなどの課題に管理層が大きな関心を寄せ、シニアマネジメントチーム内での課題の注目度を高めることができます。

また、さらなる投資や関心の必要性についての将来的な話の支えにもなります。ほとんどの組織にとって、コンプライアンスへの取組みは永遠に続くものであり、国際規格に準拠することで、最初のエネルギーを燃やした後に集中力を失いがちなプログラムに継続的な焦点を与えることができます。

統合の効率化

また、どのマネジメントシステム規格も、モジュール式で共有できるように設計されており、組織に新しいマネジメントシステム規格を導入する労力を最小限に抑えることができます。組織が品質などの一つのマネジメント規格を組み込んだ後に、プライバシーおよび情報セキュリティなどのマネジメント規格を追加するために必要な労力は、最初の規格の時よりもはるかに少なくて済みます。

マネジメントシステム規格を通じて、プライバシーおよび情報セキュリティ要求事項に準拠しようとする組織は、安全性や品質など他の技術分野に将来的に取り組むことができるように、組織の堅牢性および持続可能性に投資していることになります。

まとめ

本ホワイトペーパーでは、プライバシー規制の現状を探りました。世界的に見て多くの相違点および類似点があることを実証しただけでなく、eプライバシー指令のような特定の規制要求事項の重要性を強調しています。

すべての規制は、個人のプライバシーの権利を支援するためのポジティブな意図を持っており、GDPRによって築かれた基盤は、世界中の他の国や州への足がかりとなっています。もちろん、これらの間にはニュアンスの違いがあり、組織にとっての課題となることもありますが、そこは国際規格がサポートしてくれます。

ISO/IEC 27701は、組織に対し、個人識別可能情報の活動にガバナンスを置くことを奨励するマネジメントシステム規格として素晴らしいものです。

また、司法権の違いを考慮することを求め、シニアマネジメントがプライバシーに真剣に取り組むことを奨励しています。これは、新しい規制が施行されるときに非常に重要であり、その影響が収益に影響を与える可能性があります。

また、規制状況は複雑かつ常に変化しており、定期的に見直す必要があることを認識することも重要です。 マネジメントシステムによる取組みを採用することにより、組織は、運営するビジネス環境に照らしてパフォーマンスを継続的に監視および評価することが奨励されています。 ISO/IEC 27701は、組織、政府機関、学術機関が知識を結集して、これをサポートできるガバナンスフレームワークを提供する素晴らしい規格です。

著者

Kieran McDonagh, Riskscape Law Ltd

Kieran McDonaghは、**経験豊富なデータ保護およびサイバーセキュリティの専門家です。また、彼は国際規格を使用して、データ保護、サイバーセキュリティ、ビジネスレジリエンス、およびサプライチェーンリスクマネジメントにおける管理策の審査、リスク評価、および修復を行ってきました。**

また、BNP Paribas、BP、Centricaの規制順守プロジェクトを指揮し、現在は国際規格ISO 31700 - Privacy by Designを策定するBSI委員会のメンバーでもあります。 サイバーセキュリティ、経営科学、法律において修士号を取得しています。

査読者

本ホワイトペーパーは、以下の方々によるピアレビューを受けています:

Geoffrey Goodell, Senior Research Associate, UCL CBT, UCL Computer Science.

匿名希望の査読者1名

ISO/IEC 27701はBSI Shopでご購入いただけます：

shop.bsigroup.com/bsisoiec27701

Why BSI?

BSIは、1995年に世界初の規格であるBS 7799（現在は世界で最も普及している情報セキュリティ規格であるISO/IEC 27001）を策定して以来、情報セキュリティ規格の最前線で活躍しています。また、それだけにとどまらず、プライバシー、サイバーセキュリティ、クラウドセキュリティなど新たな課題にも取り組んでいます。だからこそ、私たちはお客様のお役に立てるのです。

BSIは、193カ国、86,000を超えるお客様と共に働き、自動車、航空宇宙、ビルトエンバイロメント、食品、ヘルスケアなど、さまざまな分野にわたるスキルと経験を備えた、真に国際的な企業です。規格開発およびナレッジソリューション、認証、プロフェッショナルサービスにおける専門知識を通して、BSIは、業績を向上させ、お客様が持続的に成長し、リスクを管理し、最終的にはレジリエンスを高められるよう支援します。

BSIの製品及びサービス

知識

当社のビジネスの核心は当社が創造し、お客様に影響を与える知識にあります。
規格の分野では、業界の専門家を集めて、国内、地域及び国際レベルで 規格を策定することで、専門家団体としての評価を高め続けています。
実際、世界で最も認められた10規格のうち、BSIが起源で作成された規格は8規格になります。

認証

プロセスの適合性の独立評価または特定の規格に準拠した製品を提供することで、高レベルのエクセレンスを発揮します。
当社は、お客様が規格の恩恵を最大限に享受するために、世界クラスの実施および監査テクニックでお客様をトレーニングいたします。

コンプライアンス

真の、長期的な利益のために、当社のお客様は規則、市場のニーズまた規格への現状のコンプライアンスを確認する必要があります。そうすれば、それが習慣となります。
当社はこのプロセスを促進するため様々なサービスと分化されたマネジメントツールを提供しています。

bsi.

BSIグループジャパン株式会社
営業本部
TEL: 045-414-3021
Eメール: Sales.Japan@bsigroup.com