protiviti®
Face the Future with Confidence

2021年1月22日「グローバルプライバシーリスクを管理する～刻々と変化するプライバシー法やデータ保護法への対応～」ご質問とプロティビティの回答

No.	頂いたご質問	Protiviti回答
1	当社は日本の個人情報保護法に対応するためにPマークを取得していますが、Pマークはプライバシーマネジメントプログラムとして他の国の法規対応にも活用できますか。	Pマークは日本の個人情報保護法を対象としたプライバシーマネジメントプログラムとなっているため、Pマークに従った運用だけでは残念ながら諸外国のプライバシー関連法と互換性があるとは言えません。より網羅性のあるプライバシーマネジメントプログラムへと拡張する必要があります。幸い、PマークはISOのマネジメントシステムを参考に構築されていますので、Pマークを取得されている企業の場合はISO27001と統合させ、さらにご紹介したISO27701と統合することによって比較的効率的にグローバルなプライバシーマネジメントプログラムへと移行することができますので、既存の枠組みを活用されるのであればそのような対応をされることを推奨しています。ただ、プライバシーマネジメントプログラムの構築は各企業の状況に応じてアプローチが異なるものなので、場合によっては新規に構成しなおすほうが良いこともしばしばあります。ぜひ一度ご相談ください。
2	当社では外国の法規制対応は現地に任せているのですが、問題はありますか。	実際GDPR対応でも欧州支社が独自に行っており本社では関与していないという日本企業はわりと数多くあるかと思います。ただ、本日のプレゼンテーションでもお伝えした通り、プライバシー対応はコーポレートリスクの一つとなっている中、支社だけがハンドルするということを継続していくのはむずかしいのではないかと考えています。可能であれば日本の本社がグリップを握りつつ、必要に応じて権限移譲を行うというスタイルに移行していくことが好ましい状況だと思います。もちろん、これに関しても企業ごとの解はことなるため、一概にこうすべきだということは申し上げることはできません。
3	プライバシープログラムが大切なのはなんとなくわかりましたが、何から始めたらよいのかがまだピンときません。	お勧めは、適用される法規制を洗い出した上でGAP分析を始めることです。それによって企業が現在抱えるプライバシーリスクが可視化できますので、打つべき具体的な対策をアクションアイテム化することが可能です。
4	専属スタッフが必要な理由は何ですか。	どのような業界、産業、業種に属していても、個人がかかわる限りプライバシーは個人にとって重要なものだからです。プライバシーに対する関心の高まりは、企業の選好にも影響を与えるようになっているため、企業は社会の要求として従来よりも高いプライバシーの基準をもつよう要求されています。専属のスタッフを持つことでよりプライバシーに配慮したビジネス活動が可能となります。 プライバシーマネジメントの活動は多岐にわたり、また法規制の理解やリスクアセスメントの実施方法については高い専門性が求められます。中途半端な対応を行うことは組織にとって制裁リスクやブランド棄損リスクを高めることとなるため対応が必要です。専属スタッフの用意が困難な場合は外部サービスの利用による対応もご検討ください。
5	個人情報保護は各国別の対応よりも、ある程度グローバルに共通要件をまとめて実行する必要性について、どう納得させるとよいでしょうか。	プライバシー関連法は世界中で整備され、改訂が進んでいます。デジタル化が進む中で各国の個人のプライバシーへの関心も高まり、改訂される際はGDPR等高額な制裁金の設定と厳格な運用を要求する法規制を参照する国が増加しています。そのため、各国でより緻密な対応が必要となる傾向があります。対応すべき国が少ない場合は各国別対応でもよいかもしれませんが、対応する国の数が多い場合はコストが増加するというデメリットもあります。さらに同じ企業で矛盾した対応が生じる可能性も高く、ブランドイメージへの影響も懸念されます。プライバシーの重要性が増す中で、企業として統一した対応方針を持たないことは、コーポレートリスクとなっており、コスト上もデメリットが大きくなりつつある状況と考えます。
6	ISO27701は、日本ではいつ頃から開始されるのでしょうか。	第三者認証機関が独自に行うプライベート認証では、既にISO27701の認証が行われており、国内でも認証取得を終えている企業がございます。日本の認定機関であるISMS-ACによるISO27701(PIMS)認証機関の認定は、昨年12月15日から開始されています。現在、各認証機関が認定を受けるための準備を行っており、はっきりした時期は申し上げられませんが春ごろから認証を開始する認証機関が出てくることが見込まれます。 https://isms.jp/topics/news/20201215.html

protiviti®
Face the Future with Confidence

2021年1月22日「グローバルプライバシーリスクを管理する～刻々と変化するプライバシー法やデータ保護法への対応～」ご質問とプロティビティの回答

No.	頂いたご質問	Protiviti回答
7	各国の法令を満足するプライバシーポリシーを効果的に作成する方法があれば教えてください。	プライバシーポリシーとは、社内のプライバシーに関する方針を示すものと理解して回答します。 プライバシーにはOECDガイドラインやFIP (Fair Information Practices)と呼ばれる原理原則があり、日本の個人情報保護法を含め、ほとんどの法規制はこれを参照に作られています。そのため、組織全体でのプライバシー方針はOECDガイドライン等の原理原則をもとに構成し、各国の法規制が持つ独自の要件については追加要件として地域ごとに管理することが効果的な対応となります。 グローバルなポリシーを策定する際のポイントとしては、「個人の権利の尊重」、「個人の情報に対するコントロール権の付与」、「情報のライフサイクルを通じた透明性の確保とプライバシー設計」、「個人データ保護状況の監督、是正」「アカウンタビリティ」「監督当局等との連携」といった点を抑えた内容とすることが挙げられます。 含むべき項目を把握するためにも、まずは適用をうける各国の法規制に対してGAPアセスメントをおこなうことから始めてください。
8	当社は国内をメインにサービスを提供しているのですが、日本においてプライバシーリスクが顕在化した事例や優先的に対処すべき点はありますか。	2020年6月の改正個人情報保護法に影響を与えたリクルート会社による就活生の内定辞退率推定を行った事案は、プライバシーリスクが顕在化し、プロファイリングに対する規制強化の流れを生じました。 日本の個人情報保護法対応に関しては、保有個人データの対象が拡大したことへの対応やデータ漏えい等に対する報告義務が生じているため、その対策が喫緊では必要となりますが、プライバシーリスクという意味ではプライバシーバイデザインを組織が行う個人データ処理に導入するようにされることが望ましいと考えます。
9	CISA資格の価値についてどうみていますか。	プライバシー管理における資格の有効性に関する質問として回答させていただきます。 CISAの領域の中にはセキュリティに関する領域が含まれますので、その知識やスキルはプライバシー保護におけるセキュリティ対策等では有効かと考えます。同様にCISMやCISSPといった資格も同じことが言えると思います。 こられの資格がプライバシー管理における全ての領域をカバーするものではありませんので、保有していれば十分というものではありませんが、リスク感性を高めるという点では共通の視点が多く含まれていると考えます。