KPMG

GDPR
EU一般データ保護規則

期限が迫っています。準備はできていますか？

なぜ「プライバシー」が問題となるのでしょうか？

近年のデジタル革命やソーシャルメディアの普及、モバイル端末の急激な増加等によって、よりターゲットを絞り込んだアプローチで消費者に訴えかけることが可能となっています。

現在、企業が保有する顧客、消費者、従業員、サプライヤーに関する個人情報の量は増加し続けている一方で、情報システム、業務プロセス、サプライチェーンのグローバル化によって、個人情報に対する情報セキュリティの確保にも複雑さが増しています。

このような状況が企業において新しいビジネスの手法や大きな機会を生み出すかたわら、これまでにない課題が生じています。個人情報の適切な取扱いやプライバシーに関して新たに生じるリスクへの対処といった問題に晒されているのです。

さらに、プライバシーに関する規制環境の目まぐるしい変化が、企業において法令を遵守して個人情報を管理することをより難しいものにしています。

GDPRとは何でしょうか？なぜそれに留意する必要があるのでしょうか？

EU一般データ保護規則（General Data Protection Regulation: GDPR）は、デジタル革命が続く現在において、EU市民の個人情報を取り扱う際に要求される基準を、ヨーロッパの視点から設定し、制定されたものです。

4年間の長きにわたる欧州議会の議員による困難な交渉の結果、GDPRを批准したことによって、ヨーロッパでは個人のプライバシー権を引き続き重視していくという姿勢が全世界に強く印象づけられました。GDPRは非常に強力な規則であり、これまでのEUのプライバシー規制環境からの大きな変化を意味しています。

GDPRでは、負荷が高く複雑で新しい要件が多数導入されます。その一部は次のページで解説しますが、重要なのは、EU加盟国全域に単一のプライバシー関連規則が初めて適用されるということです。また、GDPRはEU圏のみに留まらずに影響を及ぼすため、その調整活動は国境を越えて対応する必要があります。

GDPRの施行は2018年5月に迫っています。準備のために残された期間は短く、のんびりとはしていられません。多くの企業は、その時までに対応すべきことが山積みとなっているはずです。

「GDPRによって要求事項が改正され、EUの規制当局による管轄権や潜在的な強制力が拡大することによって、プライバシーの問題はグローバル企業が抱えるリスクのトップに躍り出ました。グローバル企業には、プライバシーリスクの再評価と対応が求められています。プライバシーをビジネス戦略の中心に据えなければならないのです。後手に回ってはいけません。」

Mark Thompson

KPMG英国
グローバルプライバシーアドバイザリー責任者

GDPRが適用されることによる変更点

GDPRでは多くの既存の法令要件が変更されるとともに、多数の新たな要件も導入されます。これらの変更点は複雑であり、企業は個人情報の取扱いを大幅に強化しなければならないでしょう。

	EUデータ保護指令	GDPR
罰金	管轄地域により異なる（例: 英国は50万ポンド）。	違反に応じた階層別の罰金体系。 レベル1は**全世界の売上高の2%**または1,000万ユーロ（いずれか高い方）。 レベル2は**全世界の売上高の4%**または2,000万ユーロ（いずれか高い方）。
データ保護責任者（DPO）	一般的にDPOの選任は求められていない。	政府機関、または**大規模調査や特殊なカテゴリーのデータを大量に処理する企業**においてはデータ保護責任者の選任が求められる。
監督当局の強制力	監督当局の権限は国内法に基づく限定的なものである。	監督当局には**広範囲にわたる権限**が付与される。
管理台帳	個人情報管理台帳の維持は**求められていない**。	一般的に個人情報管理台帳の維持が企業に求められる。
違反の通知	一般的に違反の報告義務はない。	規制当局への**72時間以内**のプライバシー違反の報告が求められ、将来的には本人への報告も求められる。
セキュリティ	セキュリティ要件は**不明確**である。	監視、暗号化、匿名化が**明確に求められる**。

「GDPRによって、EU地域内で事業やサービスを提供しているEU非加盟国の事業者のなかには、EU地域内での活動を再考せざるを得なくなるところも出てくるでしょう。これは、「グローバルな」サービスを運営することをさらに困難なものとするとともに、EU市場でのビジネス活動においては、EU諸国と同等レベルの個人情報保護の遵守が必要となってくるでしょう。」

Doron Rotman

KPMG米国
ナショナルプライバシーアドバイザリー責任者

GDPRが適用されることによる変更点

	EUデータ保護指令	GDPR
プライバシー影響評価（PIAs）	PIAsの実施は義務として求められていない。	活動が**「高リスク」とみなされる**場合には、企業はPIAsを実施しなければならない。
本人の権利	アクセス権などのさまざまな権利がある。	**データポータビリティ**や**データ削除**についての権利も含まれる。
慎重に取り扱うべき個人データ	特に**宗教的信条、身体や精神の健康状態、民族的背景**。	EUデータ保護指令と同様であるが、**生体データや遺伝子データ**も含まれる。
同意	管轄地域によっては「**黙示**」の同意に依拠する可能性あり。	**明示的**な同意を得ることが求められる。
データ処理者	処理活動の際に処理者が規制当局の監視下におかれるケースは限定的である。	処理者も**監視対象**となる。管理者は処理者の**適性評価**を実施しなければならない。

「GDPRは、APAC（アジア太平洋地域）のビジネスコミュニティに強いメッセージを送りました。その結果、APACを拠点とする企業は個人情報に対する意識が高まり、ビジネスを成功させるためには個人情報保護が重要であることを認識したのです。」

Dani Michaux
KPMGマレーシア
アジアパシフィック　サイバーセキュリティ責任者

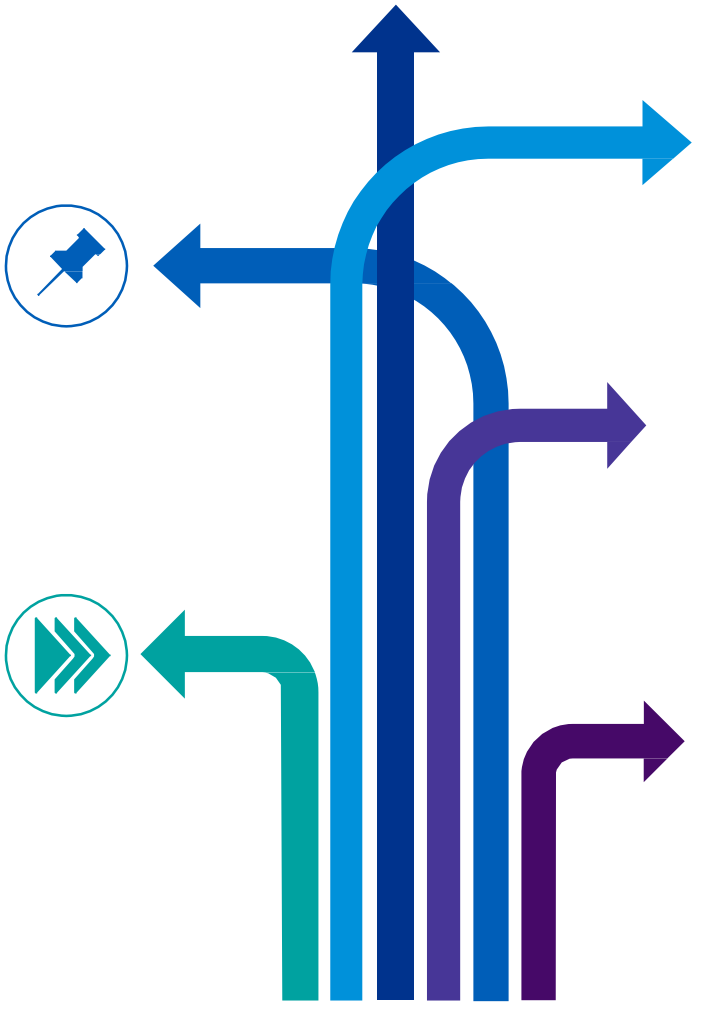
企業は何をすべきでしょうか？

- GDPRへの対応状況を評価して、現時点での成熟度を把握してください。単なる点検ではなく、GDPRが定義するプライバシーが業務を遂行するうえでリスクに晒されていないか確実に把握できるよう、実効性のある評価を集中的に実施してください。
- 実用的かつ現実的なGDPRの対応計画の策定に注力してください。そうすることにより、企業の事業戦略全体に適合した適切なレベルでリスクに対応することができます。自社にとっての成功とはどういうものなのか、明確な見解を持つようにしてください。
- 最もリスクの高い分野に重点を置いて、日々の業務プロセスのなかにリスク対応策が組み込まれるよう計画を立案してください。プライバシーを適正に取り扱うということは、リスクに適切に対処するということです。そして、顧客が自分の個人情報の監視を強めていくに従い、プライバシーを正しく取り扱えることが同業他社との一層の差別化の要因となることを覚えておいてください。

KPMGによる支援

KPMGにはプライバシーの課題に取り組む企業をサポートしてきた豊富な経験があります。KPMGの専門家チームならば、体系的で柔軟なアプローチを取り入れて、顧客企業のビジネスのニーズを満たすことが可能です。
以下は、KPMGが提供するGDPR関連サービスの例です。

評価 – 第三者的な立場で企業の現時点におけるGDPRに伴うリスクを評価し、現状と望ましい状態とのギャップを明らかにします。



設計 – EUにおけるGDPRなどの法的要件を満たすプライバシー法令遵守計画を顧客企業とともに設計します。

導入 – GDPR施行後にプライバシーリスクを軽減するための確実かつ持続可能な業務プロセス、プライバシー管理方針、管理策の導入等をサポートします。

戦略 – 実用的なGDPR環境下のプライバシー戦略を顧客企業とともに策定し、経営幹部の承認を得るための支援をします。

運用 – GDPR環境下における管理態勢の運用を支援するために、継続的なサポートやアドバイスを提供します。

監視 – GDPR環境下のプライバシー管理環境の維持をサポートします。

KPMGの強み

人材

KPMGのプライバシーチームには、業界で認知されたリーダーや200名を超えるInternational Association of Privacy Professionals（IAPP）の会員が所属しています。また、多くのKPMGメンバーファームには、KPMG Law Legal Servicesの法律の専門家からプライバシーやGDPR対応計画などに関するサポートを受けられる体制が整備されています。

経験

KPMGは、複雑で規制の厳しい業界の顧客企業に対し、各業界固有のプライバシーに関するニッチな課題を解決し、包括的なプライバシー法令遵守計画を策定するなどのサポートを提供してきました。

グローバルにも、ローカルにも対応

グローバルに展開しているKPMGでは、グローバル企業の本社、各国拠点や子会社に対して一貫したサービスを提供することが可能です。

KPMGのアプローチ

KPMG独自のアプローチやそれを支える実現手段は実証されたものであり、複雑な状況を切り開いてGDPR対応の迅速化に寄与します。

KPMGコンサルティング株式会社
サイバーセキュリティーアドバイザリー
パートナー　田口　篤

企業活動におけるプライバシーデータの利用にはリスクがありますが、その一方、プライバシーデータは重要なビジネスインフラとしての側面も持っています。国際的にプライバシーデータを活用して企業ブランドやサービス品質を高めるためには、GDPRへの対応は優先的な経営課題として捉えられるべきと考えます。まずは一刻も早く、自社グループにおけるプライバシーデータの所在と取り扱い状況の「見える化」を進めて下さい。

KPMGコンサルティング株式会社
サイバーセキュリティーアドバイザリー
ディレクター　大洞 健治郎

グローバル企業ではプライバシーデータの国際移転におけるGDPRへの対応だけでなく、移転先各国における法令要件へのコンプライアンスも確認しながら全体最適を探ることになります。法令要件に準拠するための業務プロセスの見直しに伴い、規程や手順書等の改訂、従業員に対する教育・周知、場合によってはシステムの変更なども同時並行で実施する必要があり、プロジェクト管理をしっかり行いながら進めていくことが重要です。

Contact us

KPMGコンサルティング株式会社
サイバーセキュリティアドバイザリー

TEL：03-3548-5111
cybersecurity@jp.kpmg.com

www.kpmg.com/jp/cyber-security

本冊子は、KPMG Internationalが2016年に発行した「The General Data Protection Regulation, The clock is ticking, are you prepared?」を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供するよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。