急がれるEU一般データ保護規則（GDPR）対応

EUで、新しい個人データ保護規則（GDPR）が施行された。日本企業も、EU住民の個人データを取り扱う場合は、GDPRを遵守しなくてはならない。グローバルに見るとGDPRは他の国の基準にも影響を与えており、日本企業はGDPRへの対応を一過性のものとせず、腰を落ち着けた取り組みを行うべきである。

GDPRの発効と日本への影響

個人データ保護の法律であるEU一般データ保護規則（GDPR）が、2018年5月25日に施行された。欧州連合（EU）を構成する28か国にノルウェー、リヒテンシュタイン、アイスランドを含めた31か国に適用される。EUはプライバシーを重要な個人の権利としており、保護対象となるデータの範囲は日本の個人情報保護法よりも広く、事業者の義務も厳しい。何よりも課徴金が高額で、違反すると最大で2000万ユーロか、世界年間総売上の4%のいずれか高い方を支払わなければならない。

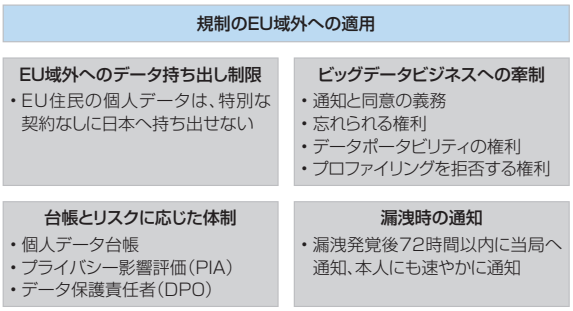
これまでEUでは、1995年に発令された「EUデータ保護指令」（以下、指令）に基づき、EU各国がそれぞれ個人情報保護に取り組んできた。しかし、EU単一市場政策を進めるにあたって、加盟国ごとに個人情報保護の法律が異なることの弊害が大きくなってきた。また、ソーシャルメディアやスマートフォンなどの普及により個人にまつわるデータが大規模に活用されたり、近年では自動車の走行情報などモノのデータまで分析されたりするなど、指令発令時には想定していなかったデータ活用がなされるようになった。このため、個人が自分の情報を自分の意思でコントロールできるようにすることが必要になってきている。GDPRは、こうした時代の変化に合わせて個人の権利と事業者の義務を強化し、さらにそれをグローバルに通用する規制として制定された。

GDPRで規制されているのは、図表に示す通り、①EU域外への規則の適用、②EU域外へのデータ持ち出し制限、③ビッグデータビジネスへのけん制として、個人データの取り扱いについての本人通知・同意、忘れられる権利[1]など、④個人データ取り扱いについて記載した台帳の整理及びプライバシーの影響評価、⑤漏洩時の通知などである。

①に示したようにGDPRの対象国は、先に挙げた適用国だけではない。物品やサービス提供などのためにEU住民の個人データを取り扱う場合は、EUにオフィスがあるかどうかに関係なく、企業はGDPRを遵守しなくてはならない。つまり、日本企業もGDPRの対象になるということだ[2]。

ではどれだけの日本企業が対象となるのだろうか。個人情報保護委員会の委託を受けて野村総合研究所が実施した調査[3]によると、全体の84.3%が、外国から日本へ個人情報の「越境移転はしていない」と回答していることから、残りの約16%が越境移転しているものとみられる。さらに、越境移転元としてEU等を挙げている企業が50%であるため、GDPRの適用対象となり得る日本企業は約8%と推計される。また日本経済新聞社の調査[4]によると、GDPRに対する「必要な対策はすべて終えた」と回答した企業は21%にとどまり、全体の8割の企業が対応を完了していない状況となっている。

図表　GDPRの主な規制



（出所）野村総合研究所

NOTE

1) 本人が個人データの消去を要求できる権利。
2) EUは、独自の基準に照らして個人データの保護が十分でないと判断される国へのデータの移転を規制（越境移転規制）している。日本は、EUから個人データの保護が十分であると認められていないため、EU住民の個人データを日本へ持ち出すためには、EU当局の指定する特別な契約を締結しなければならない。ただし、先の個人情報保護法の改正により、GDPRの保護水準に大きく近づいたことを踏まえ、EUから日本の個人情報保護制度の十分性が認定され、2019年1月1日より越境移転規制は解除される見込みである。
3) 国内1620社を対象とする「個人情報の保護に関する事業者の取組実態調査」。
4) 日本経済新聞社が、GDPR施行直前（2018年5月23日）に、国内主要100社に対して実施したアンケート。
5) 日本の個人情報保護法に登場する主体は、大きく分けると、本人、個人情報取扱事業者、第三者という3者で、このうち個人情報取扱事業者がGDPRのデータ管理者に相当する。

GDPRへの対応の要諦

GDPRへの対応はここまでやればよいという一律の基準があるわけではないが、まず行うべきは現状を調べて講ずべき対策を明確化することだろう。その第一歩となるのが「データマッピング」である。欧州の個人データを取り扱う業務やデータベースを棚卸しして、取り扱いの実態を把握する作業である。例えば、情報システムで個人データを管理している場合、サーバがどこの国に所在しているのか、クラウドを利用している場合、その事業者はGDPRに準拠しているのかなど、実態把握に向けた確認項目は多岐にわたる。

データマッピングの際、日本の個人情報保護法との違いで注意しなければならないのは、「個人データの対象」が広いということである。GDPRでは個人を識別する可能性のある情報を幅広く包含するように記載されており、個人情報保護法では非個人情報とされる、例えばIPアドレス、クッキーID、携帯電話の広告ID、携帯電話の位置データなども含まれる。

また、個人データを取り扱う根拠（なぜ個人データが必要か）を明確にしておく必要もある。GDPRでは、適切な根拠がない限り、個人データの取り扱いは認められない。さらに、GDPRに登場する主体の違いにも注意が必要である。GDPRには、本人、データ管理者（Data Controller）、データ処理者（Data Processor）、第三者の4者が主体として登場する。日本の個人情報保護法では、データ処理者は出てこない[5)]。GDPRに登場する「データ処理者」は、「データ管理者の代わりに個人データを取り扱う主体」と定義されているだけであるが、マーケティング会社、決済事業者、ITベンダーやクラウド事業者のようなITサービス事業者、さらには弁護士・会計士といった専門家が該当するとされる。

データマッピングはあくまで、対応に向けたアクションを明確にする上で、実態を把握するための計画フェーズの一部であり、この後、GDPRに向けた体制を構築するフェーズ、実際の運用フェーズが控えている。

多くの日本企業には、「GDPRは厳しすぎる」と感じられるかもしれない。しかし、グローバルの視点で見ると、個人データ保護のルール形成に対するEUの影響力は大きく、南米や近年ではアジアに至るまで、各国の個人情報保護制度がGDPRを基準に見直されるようになってきている。つまりGDPRに対応することは、グローバルで個人データを保護する仕組みを作ることであり、デジタル時代に求められる基盤だといえる。実際、グーグルやフェイスブックなどの米国のビッグデータビジネスIT企業は、GDPRの厳しい基準をクリアするため、プライバシー保護担当者を多数採用して取り組んでいる。

そう考えれば、GDPR対応は一過性のものではなく、長期的に腰を落ち着けて取り組むべき活動であることが理解できよう。そしてその活動は、顧客や従業員からの「信頼」という最も重要な資産となって、各企業の繁栄につながっていくものと思われる。

Writer's Profile

小林 慎太郎 Shintaro Kobayashi
ICTメディア・サービス産業コンサルティング部
上級コンサルタント
専門は ICT公共政策・経営
focus@nri.co.jp