KPMG

KPMG Newsletter

KPMG Insight

Vol.
51
November
2021

Topic ②
複雑化するデータ保護規制への対応

Topic　ガバナンス・リスク

複雑化するデータ保護規制への対応

KPMGコンサルティング
Technology Risk Services
大洞 健治郎／パートナー

2022年4月、日本国内で再改正された個人情報保護法が施行されます。今回の改正では、「個人関連情報」や「仮名加工情報」といった新たなデータ区分が定義されるなど、事業者において管理を求められる対象が大きく広がりました。また、法令違反に対する罰則金も大幅に引き上げられ、諸外国の厳格なデータ保護規制にまた一歩近づく内容となっています。

テクノロジーの進化に伴い、あらゆる領域でのデータ利活用が進むなか、事業者が対処すべき個人データ関連リスクは多種多様に変容しています。どの事業者においても、データの利活用は今後の競争優位を確保するために不可欠な重要課題です。現場が安心してデータの利活用を進められるよう、基本的なデータリスク対応の仕組みを整備しておくことは、今後必須となるでしょう。

本稿では、法令の遵守と安全なデータ利活用のために、今回の法改正のポイントを平易に解説しながら、2022年4月までに事業者が実施すべき対応について提言いたします。なお、本文中の意見に関する部分については、筆者の私見であることをあらかじめお断りいたします。

☑ POINT 1
データ社会での成功要因は、必要なデータを生み出し、つなげる力である。

☑ POINT 2
データの多くはどこかで個人に紐づくパーソナルデータであるため、データの利活用を企画する場合にはプライバシーリスクへの対処も求められる。

☑ POINT 3
相次ぐ諸外国のデータ保護規制強化の流れを受け、日本の個人情報保護法も再改正され、2022年4月に施行される予定となっている。

☑ POINT 4
複雑化するデータ保護規制に対応し、データ社会における競争優位を確保していくためには、プライバシーリスク対応を含むデータガバナンスの仕組み作りが必要である。

大洞 健治郎
Kenjiro Obora

Ⅰ データ社会で求められる“つなげる”力と新たな課題

企業の時価総額ランキング最上位を独占するGAFAM（Google、Amazon、Facebook、Apple、Microsoft）は“ITジャイアント”とも呼ばれますが、そのビジネスの特徴を表現するならば、むしろ“データジャイアント”と言うほうが的確かもしれません。コンピュータメーカーやSI企業などの従来型ITジャイアントとは、明らかにデータ利活用の観点で一線を画しているからです。

今後のデータ社会では、ますます多くのサービスがデータドリブンで提供されるようになり、その傾向はさらに加速していくと思われます。その場合、必要なデータを自ら生み出し、それらを効果的につなげることのできる企業は生き残りますが、そうでない企業は淘汰のリスクを負うことになるでしょう。将来にわたる期待収益の現在価値の総和が、企業の株式時価総額に反映されることを鑑みれば、GAFAMの上位独占はデータ社会の到来を予見する鏡であり、その社会を支える基盤プレイヤーへの大きな期待の表れとも言えます。

DXの中核はデータの戦略的利活用であり、企業には「既存のデータをどう生かすか」だけではなく、「必要なデータをどのように生成し、それらをどのようにつなげて価値を生み出せるか」という構想力が求められます。あらゆるデータが共有され、高度な分業が成立する機能連携型のデータ社会では、もはやB2BやB2Cといった区分は重要性を持ちません。すでに先進国では、誰もが必要とする大量消費ニーズが姿を消し、多様化する個々のウォンツにバリューチェーン全体で適時適切に応えていくことが求められています。データ社会を進化させる推進力は、まさにこの点にあるとも言えるでしょう。好むと好まざるとにかかわらず、我々は見えざる手により、今後データ社会の網の目の中へ深く引きずり込まれていくのです（図表1参照）。

1. セキュリティかプライバシーか～ネット空間のほとんどの問題は匿名性に起因

一方、データを媒介する現在のネット空間は未成熟で荒れています。迷惑行為や巧妙な特殊詐欺などの犯罪行為が横行し、多くの組織的犯罪に対して十分な抑止力が働いていません。誹謗中傷問題やフェイクニュースの拡散なども含め、ネット空間におけるほとんどの問題は利用者の匿名性に起因しており、それが攻撃者の隠れ蓑となっています。本来、自由を謳歌するのであれば、発言や行動に対する責任がセットで求められるべきです。しかし、現在のネット空間にはそれが欠如しているのです。

インターネットが日常生活に浸透し、あらゆる経済活動がサイバー空間へシフトしていくなか、この問題への対応策として、今後は多くの場面で匿名性の低減がより進んでいくものと思われます。データ社会における本人認証や行動監視の機会が増え、多くのデータがプライバシー性を有するものとなります。身の周りにあるIoTセンサーで収集されるデータが何らかの形で個人に関する識別子と紐づきやすくなっていることを鑑みれば、データ社会で利活用されるデータは、そのほとんどがプライバシー性を有するものとなっていくでしょう。

セキュリティを強化するためには、追跡可能性というプライバシーリスクを一定程度取る必要があります。そのリスクバランスを最適化しようとする試みを「プライバシーバイデザイン」と言いますが、それをすでに実践できている企業はまだまだ少数です。

2. データプライバシーに係る新たな問題

プライバシー問題というと、他人に知られたくない事実の秘匿に係る問題と捉えられがちです。しかし、データ社会におけるプライバシー問題はもっと複雑です。

ひと昔前ならば、個人情報保護とは企業内で保有する顧客リストや従業員名簿の管理と言っても大きな間違いではありませんでした。従来、多くの企業ではセンシティブな個人情報の取扱いを極力控え、データの第三者提供にも厳しいハード

図表1　各国データ保護規制 ～直近での主な動き～

年月	地域・国	主なデータ保護規制の動向
2020年 7月	アメリカ	カリフォルニア消費者プライバシー法（CCPA）の執行開始
2020年 7月	ドバイ	データ保護法2020（DIFC DPL）の施行
2020年12月	ニュージーランド	プライバシー法（PA）2020の施行
2021年 2月	シンガポール	個人データ保護法（PDPA）2020改正の施行
2021年 6月	EU	データ国際移転標準契約条項（SCC）改訂版の発行
2021年 8月	ブラジル	一般データ保護規則（LGPD）の執行開始
2021年 9月	中国	中国データセキュリティ法（DSL）の施行
2021年11月	中国	中国個人情報保護法（PIPL）の施行
2022年 4月	日本	令和2年改正個人情報保護法（APPI）の施行
2022年 6月	タイ	個人情報保護法（PDP）の全面施行
2023年 1月	アメリカ	カリフォルニア、バージニアのプライバシー法（CRPA, VCDPA）施行
2023年 7月	アメリカ	コロラドのプライバシー法（CPA）施行
2023年12月	EU	データ国際移転標準契約の改訂対応期限

ルを設けてきました。しかし今、状況は一変しました。現在は、スタティックな名簿情報よりも、個人の購買履歴や行動ログのような動的なデータの取扱いが圧倒的に増えてきています。むしろ、それら動的データの分析を通じて積極的に個人のセンシティブな属性推定さえ行うようになってきています。そして、それを取り扱う多くの当事者にとって先進性と競争優位こそがビジネス上の重要命題であり、そのプライバシーリスクが意識されることはあまりありません。

属性推定や自動意思決定には、常に偏見や誤判断の問題がつきまといます。それは、システムが誤って解釈した個人の属性が、当人も知らないまま未来永劫、それ以降のサービス提供に利用され続けるという、いわゆる「偏見の固定化」が生じ得るからです。また、AIにより誤った判断が行われていたとしても、当人にはその裏側にあるロジックや基礎となるデータを知るすべはありません。その結果、誤りを正すことができないというブラックボックス問題も起こり得ます。正しいロジックで正しく推測が行われ、属性を把握できた場合であっても、人の弱みに付け込むような不適切な営業アプローチを行えば、法令に違反しなくとも倫理的な問題が生じるでしょうし、消費者の反感を買って炎上する可能性も高まります。

3.複雑化するデータ保護規制と企業に迫られる対応

そもそもデータは無体物であり、事前の適切なアレンジがなければ、所有権を主張することができません。また、実物資産と異なり、データ資産は複製コストがゼロで、瞬時に世界中へ拡散することも可能です。一旦海外へ流出してしまったデータは、法的措置を講じることが容易ではありません。また、国内の個人データで広告収益を上げる海外事業者に対しても、税を課すことすらままなりません。

こうした状況下にあるがゆえに、世界中で国内保存が義務付けられるデータローカライゼーション規制を制定したり、海外の事業者に対する法規制の“域外適用“を宣言したりする国・地域が相次ぎ、企業のコンプライアンス対応は複雑化の一途を辿っています。

先行する諸外国のデータ保護規制は、前述のような新たなリスクに対する企業の管理責任、説明責任を厳しく求める内容となっており、2022年4月に予定されている日本の改正個人情報保護法もその後を追っています（図表2参照）。よって、各企業はデータの利活用を推進しながらも、同時にデータ保護の規制遵守を徹底するという難しい舵取りを迫られているのです。このバランスを適切に取るためには、何より本質的なリスクの理解が重要となります。

また、データセキュリティの確保という観点でも、企業のセキュリティ管理者が対応しなければならない課題は山積しています。テレワークの浸透やクラウド利用の拡大といった大きな環境変化により、セキュリティリスク自体が大きく変容しているからです。究極のエンドポイントはデータであり、データそのものの保護対策としてPETs（プライバシー強化技術）などの技

図表2　2022年4月個人情報保護法の主な改正ポイント

改正後条項	改正ポイントの概要
第2条	保有個人データの定義から、短期間しか保有しないデータは対象としないとしていた除外規定を撤廃
第16条の2	違法又は不当な行為を助長し、又は誘発するおそれがある方法による個人情報の利用を禁止
第22条の2	個人データの漏えい、滅失、毀損等が生じた際に、個人情報保護委員への報告及び本人への通知を義務付け
第23条	要配慮個人情報やオプトアウトで提供を受けた情報を含む場合には、オプトアウトによる第三者提供を禁止
第24条	個人データを海外の事業者へ提供する場合にあらかじめ本人へ提示すべき情報を拡大
	個人データを提供した海外の事業者での管理状況を確認するための対策の実施と、本人請求を受けた場合の情報提供の義務付け
第25条	記録の作成義務に、個人関連情報の第三者提供も追加
第26条の2	個人関連情報を第三者へ提供する場合には、予め本人の同意を得て、提供に係る記録の作成・保管を行うことについて義務付け
第27条	保有個人データに関する公表事項等を拡大
第28条	電磁的記録の提供による開示の請求権を規定。また、第三者提供の記録についても、開示請求可能な対象として追加
第30条	利用停止及び消去の請求について、目的外利用が行われている場合に加え、16条の2に違反する場合も請求可能と規定
	利用の必要がなくなったデータや漏洩等の事故の対象となったデータについて、利用停止又は第三者提供の停止を要求可能と規定
第35条の2	仮名加工情報の作成基準を指定。削除情報等の安全管理措置を義務付け。目的外利用を禁止する一方、本人通知要件や公表義務、事故報告義務は緩和。識別行為や本人へのアクセス行為は禁止
第35条の3	仮名加工情報の第三者提供を禁止。委託や共同利用は可能
第87条	是正勧告に応じなかった法人に対する罰則金上限を1億円に引き上げ

術活用を検討する場面も、今後は増えてくるでしょう。

たとえば、秘密分散技術のように、分散された個々のデータはまったく意味を持たず、利用ごとに必要な分量だけ有意なデータへ再構成されるといった仕組みが普及すれば、データ社会の安全性はより高められます。

とはいえ、データの利活用や規制遵守、セキュリティ対策、いずれの観点からも今後はデータガバナンスは必須となってきます。社内でのデータの取扱いやリスクの全体像を把握し、データをどこにどのような形態で保持すべきかを判断し、リスクに応じた管理策を決定するためには、データガバナンスの機能が求められるのです。

Ⅱ 改正個人情報保護法、対応すべき5つのポイント

前述した文脈を踏まえ、2022年4月に施行される個人情報保護法の改正内容を俯瞰すると、企業として対処すべき重要なポイントがより明確になってきます。

1. 管理すべきデータ範囲の拡大

まず、最も影響の大きい改正点の1つが、規制対象となるデータの範囲の拡大です。これまで、開示対応などが義務付けられてきた「保有個人データベース」は「6ヵ月以上保持するもの」という日本独自の優しい前提条件でした。しかし、今回の法改正では、この期間条件が撤廃されます。つまり、短期保有のデータであっても、保有個人データベースとしての公表や開示請求対応、苦情受付などの義務が課されるのです。

また、「個人関連情報」という新たに設けられたデータ区分にも注意が必要です。これは、自社内では特定の個人を識別することのできないデータであったとしても、それを他の事業者へ渡した際に個人を特定できる可能性が想定される場合には、そのデータ提供に関する本人同意を取得しなければならず、記録の作成・保存義務も課されるというものです。つまり、今後すべての国内事業者は、従来の顧客名簿のような分かりやすい個人データだけでなく、データ社会で想定されるライフログのような動的データなども含むより幅広いデータ全般の管理が必要となります。経理や監査部門にとっても、他人事ではない課題と言えるでしょう。

2. 海外データ移転に係る要求事項の厳格化

次の改正点は、データの海外移転に関する説明責任の厳格化です。業務委託でデータを渡す場合も含め、個人データを海外の事業者へ渡す場合には、その利用目的はもちろんのこと、①当該外国の名称、②適切かつ合理的な方法により得られた当該外国における個人情報保護制度に関する情報、③当該第三者が講ずる個人情報の保護のための措置に関する情報、をあらかじめ本人に提供しなければならないと義務付けられます。

さらに、当該海外事業者による適切な管理が継続的に実施されていることを確認するための措置を講ずるよう求められ、本人が望む場合には、その措置内容に関する情報を本人に提供しなければなりません。つまり、海外へ個人データを越境移転する場合には、当該国での法令環境や事業者の管理状況を確認して説明を行うだけでなく、その管理状況を日本側で監督・確認する具体的な方法についても整備のうえ、本人からの要求に応じて情報開示できる態勢を整備しておく必要が出てきます。

3. 本人請求への対応義務の拡大

3つ目のポイントは、本人請求への対応義務の拡大です。今回の改正により、本人から「電磁的記録」、つまり「デジタルデータ」として情報開示を請求された場合、事業者側はそれに応じる必要があります。これまで情報開示は郵送対応のみとしてきた事業者も少なくないと思われますが、今後はデータ開示のための仕組みを整備することが求められます。

また、保有する個人データそのものだけでなく、それを第三者へ提供した記録についても開示請求が可能となりましたので、これにも対応しなければなりません。前述のとおり、これまでは6ヵ月以上保有するデータベースについてのみ対応義務が生じていましたが、今後はその期間制限が撤廃され、あらゆるデータについて開示が必要になるという点にも留意が必要です。

加えて、これまでデータの消去や利用停止などを請求できるケースは不適切な取得や目的外利用があった場合に制限されていましたが、本人の権利または正当な利益が損なわれる恐れがある場合にも請求可能と緩和されました。この改正によって、事業者側の対応負荷は大きく増えるものと想定されます。

4. インシデント報告の義務化

4つ目は、インシデント報告の義務化、つまり漏えい、滅失、毀損などの事故が発生した場合に、当局への報告および本人への通知が義務化される、という点です。これは、事故の可能性を認識してから原則として3~5日以内に、個人情報保護委員会へ報告するとともに本人に対する通知を行うことを義務付けたものです。報告対象となるのは、①要配慮個人データが含まれる場合、②財産的被害につながり得るデータが含まれる場合、③不正の目的をもって行われた可能性がある事案の場合、④1,000人を超えるデータが漏えいした場合、のいずれかに該当した場合です。たとえば、「システムの設定ミスにより、クラウドに保存していた自社のデータが第三者

から閲覧可能な状態となっていた」というケースでも、閲覧可能なデータが1,000人分を超えていたり、データにセンシティブなものが含まれていたりする場合には報告義務が発生します。

どの企業においても、セキュリティ事故が発生した場合に経営層への報告を行うルールはすでに定められていると思いますが、あるサーバへの不正アクセスの痕跡が認められた場合に、そこで扱われている個人データの種類や件数を即座に把握できないという企業は少なくないと思われます。セキュリティ事故が発生した場合に備え、当局への報告の要否を判断するための仕組みと報告ルート、当局への報告や本人への通知の発出責任者などは事前に整備していく必要があるものと考えます。

5. 透明性の確保と不適正利用の禁止

今回の改正では、上記以外にも保有個人データに関する公表義務として具体的な安全管理措置の説明が求められている点や、「仮名加工情報」というデータ区分が新設され、事業者におけるデータ利活用の制限を一部緩和している点など、細部での変更点があります。ここでは紙面の都合上、事業者への影響が大きいものとして上述した4つのポイントを概説しましたが、もう一点、重要にもかかわらず見過ごされやすい改正点があります。それは、今回新たに第16条の2として新設された「不適正な利用の禁止」です。「違法又は不当な行為を助長し、又は誘発するおそれがある方法により個人情報を利用してはならない」というシンプルな一文ですが、これにより多くの問題を網にかけられる万能条項となっています。

たとえば、採用活動のAIプロファイリングで不公正な自動判断が行われた場合、この条項に抵触する可能性が高くなります。国籍や性別等の特定の属性により採否が左右されているとなれば、個人情報の不適切な利用と見なされるからです。このことについては、ガイドライン上にも明記されました。また、ネット上にすでに公表されている情報であっても、特定の人物に対する偏見が助長されるようなデータをかき集めてまとめて公表する、といったスクレーピングを使ったオンライン上のヘイト行為は「個人データの不適正利用」に該当するとも例示されています。この条項に基づく改善命令に応じなかった場合、法人であれば1億円までの罰則金を課すことも可能であるため、今後、さまざまなオンライン犯罪等への対処に本条項が用いられる可能性が考えられます。

III プライバシーリスク対応を含むデータガバナンスの必要性

どのような企業も、今後、社会全体に広がる大きなデータ流通網のなかへ否応なく組み込まれていくでしょう。データ利活用の重要性がますます高まる一方で、プライバシー性を有するデータの取扱いにはさまざまなリスクが伴い、複雑なデータ保護規制への目配りも必要になります。

データの利活用を構想するうえでも、あるいは法規制へのコンプライアンスを確保するためにも、その前提となるのは、自社内のどこにどのようなデータがあるのかを把握できている、ということです。そのうえで、それぞれのデータの取扱いにどのようなリスクが考えられるのかを評価し、必要となる対策を検討するデータガバナンスの仕組みを構築する必要があります。データガバナンスの整備によって自社のビジネスを最大化する形態でデータを保持できれば、意思決定の支援も可能となるでしょう。

国内企業では、2022年4月より施行される令和2年改正個人情報保護法への対応が喫緊の課題となっていますが、この検討のなかでデータガバナンスのあるべき姿についても十分に協議し、データ社会のボーダーレスなビジネス競争を勝ち抜くことのできる管理態勢の整備につなげていくことを期待します。

関連情報

データ保護規制に関するコンテンツ

ウェブサイトでは、世界各国のデータ保護規制対応等の情報を紹介しています。

https://home.kpmg/jp/ja/home/services/advisory/risk-consulting/global-privacy-compliance.html

本稿に関するご質問等は、
以下の担当者までお願いいたします。

KPMGコンサルティング株式会社
Technology Risk Services
大洞健治郎／パートナー

Kenjiro.Obora@jp.kpmg.com

KPMGジャパン

marketing@jp.kpmg.com
home.kpmg/jp

home.kpmg/jp/socialmedia