



世界のビジネスを激変させる個人データ・プライバシー保護規制(前編)

個人データ・プライバシー保護規制の変遷

B2Cビジネスにおいて、顧客データの分析・利活用の重要性が叫ばれてきた。一方で、欧州のGDPRを筆頭に世界各国で個人データ・プライバシー保護規制が強化されており、無条件で個人データを活用して得られる企業の競争優位性はもはや過去のものである。今、多くの経営者や事業担当者には、ビジネスにおけるデータとの関わり方が問われている。

個人データ・プライバシー保護の現在

政府動向

世界に広がるデータ保護当局の制裁強化

2018年5月に欧州でGDPRが施行されてから4年ほどが経った。(図1) 当時受けた驚きははまだ記憶に新しい。GDPR違反による制裁事例は既に1,300件を超えており、その数は年々増加している。(図2)

GDPR施行時、グローバルビジネスを展開する経営者達に懸念を抱かせたのは、規制違反により科せられる巨額な制裁金だったであろう。違反した企業には、

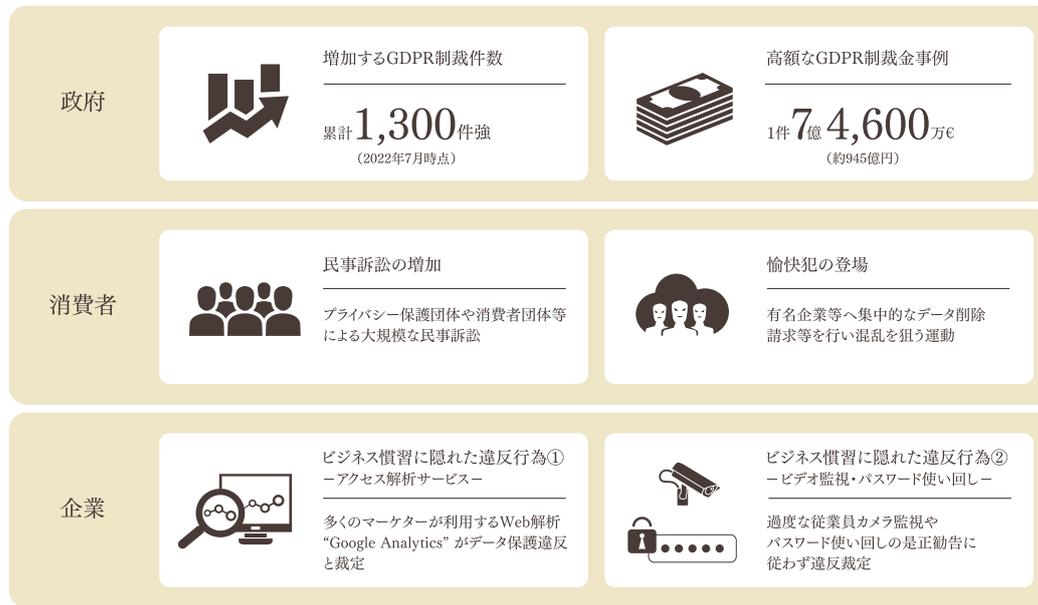
最大で全世界での売上の4%もの制裁金が科せられる。EU競争法をはじめ、EU域外の企業に対しても制裁金を科す事例を有していることから、懸念を抱く経営者も少なくなかったのではないだろうか。その懸念のとおり制裁事例は後を絶えず、特にビッグ・テック(Google、Apple、Meta Platforms、Amazon、Microsoft)に対する巨額制裁は目を引くものがある。

ここで、国によって異なる制裁の件数や金額に着目したい。(図3) GDPR違反について同じ欧州でも目立つのは、スペインの制裁件数とルクセンブルクの制裁金総額である。制裁件数が突出しているスペインの

個人データ・プライバシー保護の現在

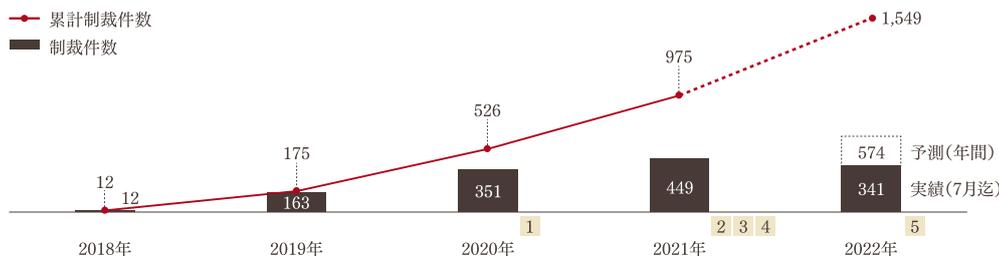
図1

GDPR施行(2018年5月)から約4年経った今…



GDPR違反による制裁件数の推移・主な事例

図2

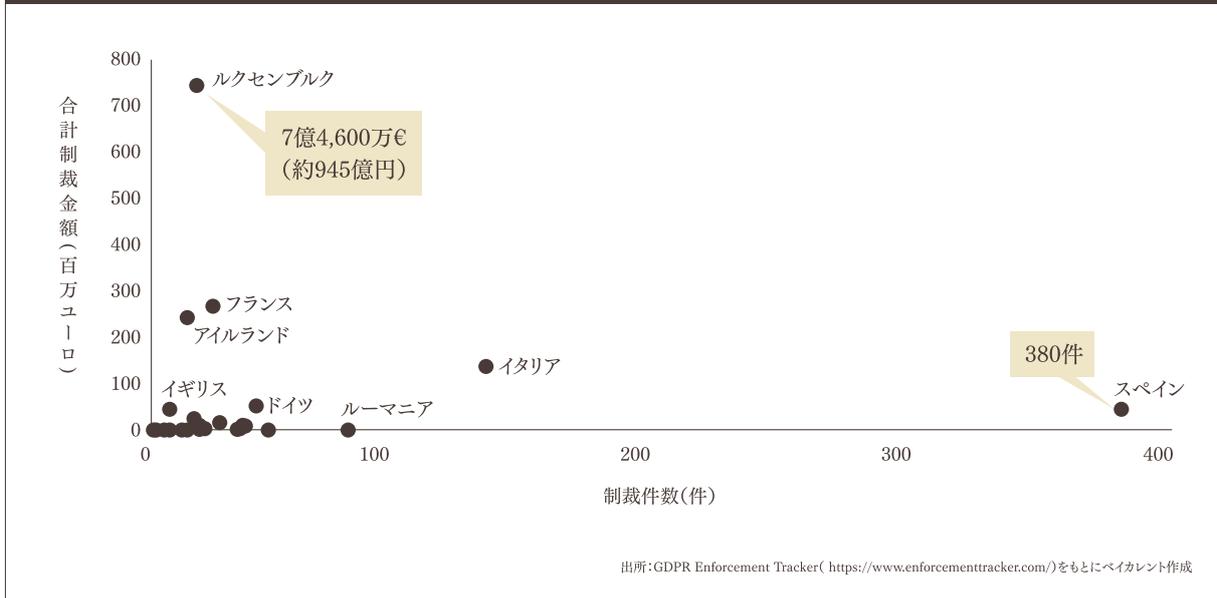


決定年月	対象企業	制裁当局	制裁金	違反内容
1 2020年12月	Google	CNIL (フランス)	約1億€ (約128億円) ※米 6,000万€ 愛 4,000万€	ユーザー同意のないクッキーの設置 ▶クッキー情報を開示せず、検索サイトにクッキーが埋め込まれていた
2 2021年7月	Amazon	CNPD (ルクセンブルク)	7億4,600万€ (約945億円)	顧客データ処理に関する違反
3 2021年9月	WhatsApp (Meta Platforms傘下)	DPC (アイルランド)	2億2,500万€ (約288億円)	個人情報の取り扱いに関する説明の不足 ▶スマホの電話帳データの使用方法に関する説明が不透明だった
4 2021年12月	Facebook Ireland (現・Meta Platforms)	CNIL (フランス)	6,000万€ (約83億円)	ユーザー同意のないクッキーの設置 ▶クッキー情報を開示せず、検索サイトにクッキーが埋め込まれていた
5 2022年2月	Google	AEPD (スペイン)	1億5,000万€ (約206億円)	難度の高いクッキー拒否操作 ▶承諾は1クリックで可能であるのに対し、拒否は複数回クリックを要した

出所:各当局公式情報などをもとにベイカレント作成

GDPR違反による制裁件数・金額(国別計)

図3



データ保護当局 AEPD (Agencia Española de Protección de Datos: スペインデータ保護庁) は、これまでに約 400 件の制裁を課している。この制裁対象にはカフェ経営者、Web サイト運営者といった、個人(私人)までも含まれており、1 件当たりの制裁金は比較的少額である点が特長である。他方、制裁金総額が突出しているルクセンブルクのデータ保護当局 CNPD (Commission nationale pour la protection des données: 国立データ保護委員会) がこれまでに課した制裁は、18 件。しかし、制裁金総額は約 7 億 5,000 万ユーロ、日本円にして約 900 億円(1 ユーロ 120 円換算)という巨額である。もっとも、この金額のほとんどは、2021 年 7 月に課した Amazon Europe Core への制裁金(7 億 4600 万ユーロ=約 895 億円)である。ビッグ・テックに対する制裁は厳しく、巨額の制裁金を課されることが多いため、結果的にビッグ・テックの拠点がある国は、制裁金総額が高い傾向にあることが伺える。

次に、欧州以外の国・地域を見てみると、GDPR ほどの高額な制裁金ではないものの、個人データ・プライバシー保護規制は強化され、制裁事例も増えている。

一例として韓国を挙げると、2021 年 8 月にデータ保護当局である PIPC (개인정보보호위원회: 韓国個人情報保護委員会) が Facebook Ireland 及び Facebook Inc. (現 Meta Platforms Ireland Limited 及び Meta Platforms, Inc.) に対し、64 億 4000 万ウォン(約 6 億 4,400 万円(1 ウォン 0.1 円換算))の課徴金と 2600 万ウォン(約 260 万円)の過料という高額な制裁金を課した。また、シンガポールのデータ保護当局 PDPC (Personal Data Protection Commission: シンガポール個人情報保護委員会) は毎月のように制裁事例を報告している。

こうした個人データ・プライバシー保護規制強化の傾向は世界各国にみられる。近い将来、欧州以外の国・地域でも GDPR に似た巨額の制裁事例が出てきてもおかしくはない。

消費者動向

民事訴訟の増加と愉快犯の登場

データ保護当局による制裁とは別に、個人データ・プライバシー保護を訴える一般消費者による民事訴訟も増加している。(図 4)

特にビッグ・テックに対しては、プライバシー保護

消費者による個人データ・プライバシー保護に関する集団民事訴訟の例

図4

発表年月	被告企業	訴訟経緯	状況/結果	賠償/和解金
2019年12月	TikTok	<ul style="list-style-type: none"> ・アプリの個人情報取り扱いを巡りユーザーが集団訴訟を提訴 <ul style="list-style-type: none"> ▶ アプリが利用者の個人情報を収集している主張 ・適用法令: カリフォルニア州消費者プライバシー法 	和解合意 (2022年2月)	和解金 9,200万\$ (約97億円)
2020年6月	Google	<ul style="list-style-type: none"> ・Chromeサービスについてユーザーが米連邦地裁に提訴 <ul style="list-style-type: none"> ▶ 同サービスシークレットモードは、閲覧履歴を残さずWebサイトを閲覧できると説明していたが、本モード中も個人情報を収集していたため ・適用法令: カリフォルニア州消費者プライバシー法 	棄却・請求却下 (2021年3月)	賠償金 50億\$ (約6,750億円)
2020年12月	TikTok	<ul style="list-style-type: none"> ・子どもに関するデータの収集、使用に関してユーザーが提訴 <ul style="list-style-type: none"> ▶ 子どもに関する広範なデータを広告収入の最大化に使用していると主張 ・適用法令: EU一般データ保護規則(GDPR) 	英国高裁にて 集団訴訟とし承認 (2022年3月)	数十億\$程度
2021年1月	Facebook (現: Meta Platforms)	<ul style="list-style-type: none"> ・データ搾取について英国のユーザーが集団訴訟を提訴 <ul style="list-style-type: none"> ▶ 400万人のユーザーが2015年から2019年の間にデータを搾取された ▶ EU競争法専門家がユーザーに賠償金を支払うべきと主張 ・適用法令: EU一般データ保護規則(GDPR) 	提訴検討 (2022年1月)	賠償金 31億\$ (約4,200億円)
2021年5月	Zoom	<ul style="list-style-type: none"> ・ビデオ会議サービスについてユーザーが集団訴訟を提訴 <ul style="list-style-type: none"> ▶ ユーザー情報を同意なくFacebook等と共有 ▶ また、ハッカーの侵入を防ぐための十分な対策をとらなかったため ・適用法令: カリフォルニア州消費者プライバシー法 	和解合意 (2021年8月)	和解金 8,500万\$ (約115億円)

出所: 各当局公式情報などをもとにベイクレント作成

団体を通じた市民からの申し立てや、消費者団体等からの大規模な集団訴訟が起きている。個人データ・プライバシー保護規制は、政府当局だけでなく一般消費者たちも自ら動き出すほど大きなムーブメントになっているのだ。

一方で、これらの消費者動向に乗じ、有名企業や不祥事を起こした企業等をターゲットとする愉快犯も登場している。例えば、個人情報の削除要求や開示要求を特定企業に集中的に行うことにより、要求先企業を混乱させ、その業務を滞らせる戦法だ。1件、2件の要求ならばまだよいが、ネット上の呼びかけで数千件の賛同者を集めるケースも確認されている。一種のネガティブキャンペーンであり、企業はこのようなことに対応しようとする、本業にも影響が及ぶであろう。

企業

ビジネス慣習に隠れた違反行為

高額な制裁金もさることながら制裁の理由となった違反事項にも着目したい。制裁を受けているのは、誰もが違反行為と分かるような活動だけでない。従来から当たり前のように行ってきたビジネス活動が違反となってしまうような事例も出てきている。印象的であった制裁事例を2つほど紹介しよう。

2022年1月、オーストリアのデータ保護当局が、あるドイツ企業による Google Analytics の利用を違反とした。同社の Google Analytics の運用では、GDPR で定めている適切なレベルのデータ保護が保証されていないと判断されたためである。

アクセス解析サービスとして、多くの企業で採用されている Google Analytics の利用が違反と判断されたことで、世界中の Web マーケターは驚愕したことであろう。

本件については、欧州データ保護観察機関（EDPS）に設置されたタスクフォースの中で、異議申し立ての調整を行うとされているが、これまで Google Analytics を利用してきた企業は運用方法を見直した上で、場合によっては代替サービスへの移行も検討せざるを得ないであろう。

また、2019年9月、フランスの UNIONTRAD COMPANY という翻訳サービスを専門とする零細企業に2万ユーロ（約240万円）の制裁金が課された。従業員に対して長時間にわたりビデオ監視を行っていたことや、業務用サーバーや電子メールのパスワードを使いまわしていることに對し、データ保護当局が指摘したにも関わらずは正しなかったためである。

2万ユーロという零細企業にとって大きな金額である制裁金にも注目したいが、それ以上に、ビデオ監視やパスワードの使いまわしとその注意勧告の無視が明確に違反であると判断された点に着眼いただきたい。小売をはじめ業務上カメラを設置している中小企業は多いであろう。また、パスワード使い回しも全くないと言い切れる事業者は必ずしも多くないのではないだろうか。

保護規制に對峙しなければならないのは大企業だけ

ではなく、中小・零細企業もである。

保護規制強化の背景・経緯

ここまで話を続けてきたが、次のような純粋で根本的な問いが浮かんでいるのではないであろうか。

なぜ、世界的に個人データ・プライバシー保護規制が強化・厳格化されるのか？

一見、迷いようのない問いに聞こえるが、いざ一言で答えようとする中々難しい。この世界的潮流を真に理解するためには、その理由となる背景や経緯を正しく理解する必要がある。以下、詳しく解説したい。（図5）

■ そもそもは、基本的な個人の権利保護

個人データ・プライバシー保護がなぜ必要か、一言でいえば、人権保護のためである。特に、欧州では「忘れられる権利（right to be forgotten）」という人権とその尊重が広く理解・浸透しており、世界初の判例を上げた歴史もある。現在の GDPR において、この権利は「消去権（right to erase）」と修正されているが意味するところは同じで、基本的人権（平等権、



自由権等) に対して新たな人権と言われるプライバシー権の一つに位置付けられている。(日本では欧州と異なり、権利が明文化されていない。)

「忘れられる権利」の意味は文字通りである。

幼少期に起こした悪行を例に取ってみる。アナログ時代であれば、月日とともに人々の頭の中から悪行の記憶は消え、忘れ去られてしまうものであった。しかし、デジタル社会に移り、インターネットによってデータ流通が飛躍的に促進されてくると、この悪行はWeb上で過去の不名誉として永久に残されてしまう可能性がある。これがプライバシー侵害に当たると考えられるのである。表現の自由や知る権利とのバランスが問われる。

欧州に「忘れられる権利」の思想を根付かせる契機になった歴史的な事案がある。

2014年5月、EUの最高裁判所にあたるEU司法裁判所は、スペインで起きたある訴訟に関して先決裁定を行った。その訴訟は、自身の好ましくない過去に関する記事(16年前の社会保障費滞納に伴う不動産競売に関する新聞記事)の検索結果表示からの削除を求め、私人がグーグルを提訴したものだ。これに対し、EU司法裁判所は「EU基本権憲章第8条が保障する個人データへの権利に照らし、EUデータ保護指令が保障する削除の権利及び異議申立権に違反する」という裁定を言い渡したのである。先行裁定に基づきスペイン最高裁判所は検索結果に表示できないような技術的措置を講じることをグーグルに命じた。以降、グーグルのサイトにコンテンツ削除を求める申請フォームが設置された。

GDPRにおいて、特に個人データの削除権が厳格であることが腑に落ちたのではないだろうか。

■ デジタル・データ活用への不安

また、データ基盤の整備やデータ分析技術等の開発が促進され、個人データ活用の巧拙がビジネスを左右する時代に突入している。PCやスマホ、タブレット、ウェアラブルデバイス等、デジタルが身近になり、子どもからお年寄りまでデジタルを活用しその恩恵を受

けることができる。特に、AI(人工知能)の技術進展と市場普及が、消費者の利便性を高めることは申し上げるまでもない。

しかし、このデジタル・データ活用の波は個人データ・プライバシー保護の観点で新たな脅威やリスクを生んでおり、様々な課題が国際的に議論されている。

例えば、保護者が知らないうちに、子どもの興味を引くようなデジタル広告を利用して、子どもの個人データを取得して活用、さらには子どもに高額な決済を誘導するような事案がグローバルで多発している。

さらに、AI活用に対する不安感などのネガティブについても論点となっている。

英国では超党派議員連盟が、労働管理におけるAIの広がりに関する報告書をまとめ、「AI上司」による労働者へのプレッシャーと、メンタル、フィジカルへの悪影響を指摘している。また米国では、バイデン政権下でAIによる人権侵害に対処するための権利章典作成に動き出している。

日本でもなじみのある話題としては「AI審査」が挙げられる。金融業界の多くの企業が融資や貸出の際に行う与信審査にAI活用を進めている。最近であれば、改正割賦販売法に後押しを受け、与信枠(利用限度枠)をAIによる審査で決めるBNPL(後払い決済)サービスが代表的である。この審査ロジックはもちろん公表されていないため、決済サービスの利用で、突然与信枠が引き下げられると利用者が当惑してしまうケースも少なくない。支払い遅滞など減額になりそうなことに身に覚えがない場合、利用者がAI審査に対しネガティブな印象を持ってしまうこともあるだろう。

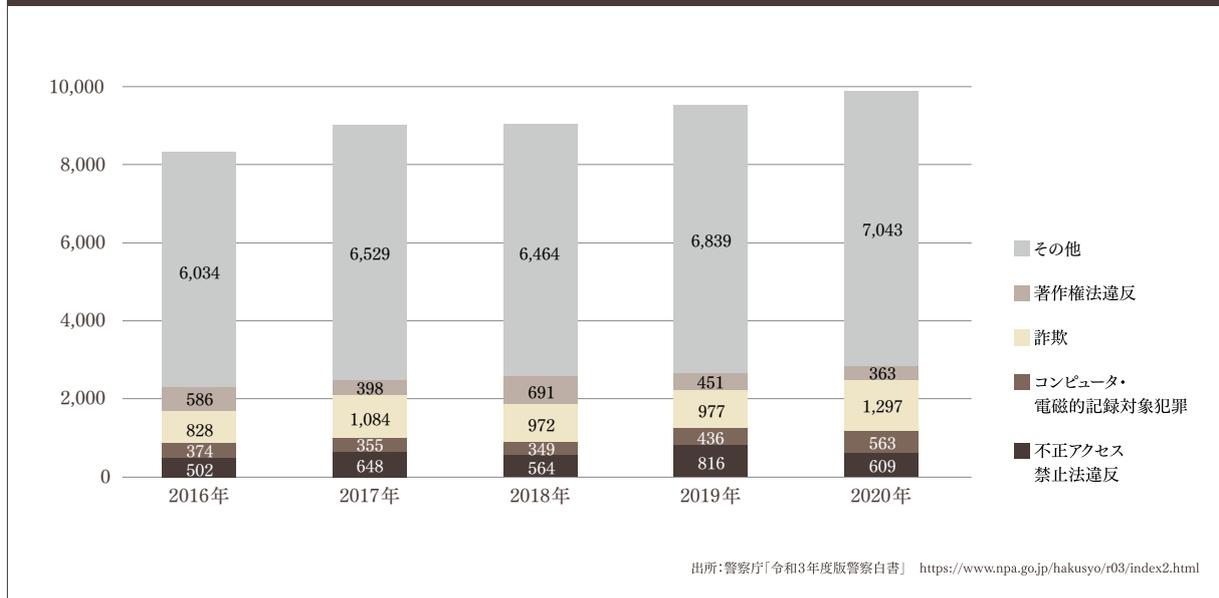
企業としては、AIを活用することにより、ビジネスの能率化を進めたいと考えがちだが、結果としてプライバシー侵害に発展することからも、AI規制に関する強化も進んでいるのだ。

■ サイバー空間における脅威

不正アクセスなどのサイバー攻撃も問題だ。個人情報報を盗み取り、経済的利益を得ることができるのは、従来、悪意のあるハッカー集団が得意とするところで

サイバー犯罪検挙件数の推移

図6



あった。しかしながら近年、ダークウェブを介した個人データの売買、専門知識がなくとも扱えるハッキングツールの増加などにより、誰でもサイバー攻撃ができる時代になった。サイバー攻撃による被害が今より拡大するであろう。(図6)

また、企業においては不適切な情報管理やメール誤送信などにより情報漏洩してしまうケースもある。情報漏洩の結果、信用失墜や事業停止に追い込まれることもある。

こうしたサイバー攻撃や情報漏洩等への関心は、世界共通のものであり、個人データ保護やセキュリティへの関心が高まっているのだ。

■ 国家レベルの監視

グローバルビジネスを展開する場合、国家レベルの監視に対する脅威も高まっている。

中国では国家レベルで企業保有データの監視を行っており、EC大手のアリババや、ネットサービス大手のテンセントのユーザーデータを、政府当局も閲覧できる。

インドもソーシャルメディアの監視を強化している。2021年2月、インド電子情報通信省が新IT規則を

公布し、同年5月に施行された。同法は大規模ソーシャルメディアプラットフォームに対し、事実上、インド政府による投稿の削除やアカウントの凍結を可能とするものである。

また、2013年には、元米国家安全保障局(NSA)職員のエドワード・スノーデン氏が、欧米諸国の大量監視の実態を暴露した。この他民間レベルでも、監視カメラの普及によるプライバシー侵害(交通監視カメラ、車内監視システムなど)、位置情報の活用による監視(GPS、ドライバー追跡システムなど)の脅威が増している。

国家レベルの監視に抵触した場合、当局が現地法人等に土足で入り込むこともあり得るだろう。その際、制裁金だけでなく、事業停止、企業ノウハウの流出、更には刑事罰も覚悟しなければならない可能性もある。

■ デジタルプラットフォーマーへの嫌悪感

こうした個人の不安や不満の裏で、欧州を中心としたビッグ・テックへの嫌悪感がある。

ビッグ・テックはこれまで、デジタル市場で国境を越えた経済圏を築き上げてきた。この大きな要因の1つは、デジタルプラットフォーマーとしての個人デー

タの活用、特にターゲティング広告による巨額の利益である。2011年1月に世界経済フォーラムが公表した報告「Personal Data: The Emergence of a New Asset Class」（邦題：個人データ：新たな資産カテゴリーの出現）では「個人データは、21世紀の貴重な資源である新たな「石油」になり、社会のあらゆる側面に触れる新たな資産クラスとして登場する」と述べられている。ビッグ・テックはまさに、個人データを新たな「石油」として広告収入を獲得するビジネスを実現したわけである。

ここで問題なのは、消費者とプラットフォームの関係性である。個人データを取り扱う事業者は、取得した個人データを利用目的の範囲を超えて利用してはならない。利用目的は、通常、プライバシーポリシーとして消費者に公開されている。しかしながら、デジタルプラットフォームとしての「優越的地位の濫用」により、消費者の意思を超える個人データの活用がビッグ・テックの経済圏成長に大きく貢献してきたのだ。

これに対するGDPRの基本的スタンスは、「個人データを利用して利益を得るならば、本人の同意を得た上でしかるべきプライバシー保護を行うべきだ」というものだ。プラットフォームビジネスが台頭している現在において、この「個人データ・プライバシー保護」は実体として「ビッグ・テック規制」の様相を呈している。

過度な中央集権を生み出してしまうおそれのあるメガプラットフォームに対し、その透明化・公正化についての再考を迫る門番としての側面がGDPRにはあるのかもしれない。

個人データ・プライバシー保護規制に対する企業の向き合い方

個人データ・プライバシー保護規制が強化されることにより、企業は経営から事業まで様々な面で負担が増すことは言うまでもない。特に制裁件数も制裁金額も多い欧州のGDPR動向は、グローバルビジネスを展開する企業にとって看過できないものであろう。中には、欧州ビジネスの撤退を検討する企業も出現している。

アメリカの新聞社であるTribune Publishing Company(TPCO)はGDPRの施行に合わせて、欧州顧客へのサービス提供を終了した。GDPR遵守によるビジネス継続ではなく、GDPR施行国からのビジネス撤退を選んだ。

日本ではヤフーが2022年4月、欧州におけるポータルサイト「Yahoo! JAPAN」のサービス提供を停止した。この理由について公表では「サービス利用いただける環境を継続的に提供することが困難になったため」とされている。私見ではあるが、この行間を読むとすると、サービス継続に必須となるGDPR及びeプライバシー規則の遵守に対する初期対策や継続的な対応、制裁リスク等に鑑みた結果、事業性が低いと判断されたと推察する。こうした動きに追従する企業は、今後、増えていくのではないであろうか。

一方で、グローバル化推進や撤退困難など理由は様々あるであろうが、多くの企業はこの保護規制の下でビジネスを行わなければならない。次稿となる後編では、日本企業はこの世界的な潮流に対しどのように向き合うべきかに迫りたい。

エグゼクティブパートナー 永尾 裕樹