2020.11.12

デジタル変革を急ぐあまり、プライバシー保護を軽視していないか

Have Your Privacy Policies Kept Up with Your Digital Transformation?

4つの施策で重大なリスクを回避する

キリアン・キーラン　：エシカ 創業CEO

感染症の流行で人の接触が大幅に制限されたことを受け、多くの企業がデジタルトランスフォーメーションを加速させているが、データの取り扱いには十分な注意を払っているのか。変革を急ぐあまり、遵守すべきルールを無視してはいないだろうか。プライバシー保護に関する取り決めは、ここ数年でいっそう厳格化している。この点を軽視しては、取り返しのつかない重大な危機を招く可能性がある。

新型コロナウイルス感染症によって、あらゆる地域の企業はデジタルトランスフォーメーションを想定外の速さで進めるよう迫られている。事業を存続させ安全に再開しようと努める企業は、非接触型決済、クリック・アンド・コレクト（ネットで注文し店頭などで受け取る）のアプリ、高度な顧客関係管理などのサービスを急遽導入している。

こうした移行は事業継続のために不可欠だが、新たなリスクも生む。オペレーションをオンライン化する事業者にとっては例外なく、プライバシーをめぐるリスクが潜在し、対処を誤れば深刻な損害が生じることになるのだ。米国で新しい法規制の施行が始まるいま、方向転換を正しく行うことはこれまで以上に重要である。

さまざまな業界で、現実世界の専門家集団がデジタル空間になだれ込み、新参者の彼らは新たなシステムに大量のユーザーデータを注ぎ込んでいる。

レストラン業界では、老舗店は新たなオンライン注文・配達のインフラ構築や、その種のサービスをすでに提供している企業との提携に躍起だ。高等教育界では、1年分の授業料を失う危機に直面した教育機関は、慌てて全カリキュラムをオンラインに移行させ、授業から生徒の健康記録まで何でもデジタル化しようと急いでいる。ライブイベント業界では制作のベテランたちが、その確かな手法をオンラインおよび新たなクラウド技術へと移行させるよう求められている。

いずれの変更も、大量の個人データが適切に管理されず流出するリスクを伴う。このような状況下で、多くの事業者にとって大きな課題が2つある。

第1に、新たな技術の調達に関して――オンライン店舗の開設や、顧客の個人データを処理するコミュニケーション・プラットフォームの導入など何であれ――意思決定を迅速に下さなくてはならない。第2に、データ処理のインフラ、あるいはテクノロジー全般について、経験が乏しい。これらが相まって、よく知らない技術システムの導入をすぐに決めてしまうのである。

プライバシー保護の問題は二の次にしたい、目の前の危機を乗り越えたあとに対処すれ

ばよい、という気持ちはわからなくもない。しかし、それは間違いであり、制裁金や集団訴訟、広報活動の支障などを招くリスクを増やすことになる。

大西洋の両側で、規制当局からの圧力が高まっている。欧州では一般データ保護規則（GDPR）が 2018 年 5 月に施行。米国ではカリフォルニア州消費者プライバシー法（CCPA）が、7 月 1 日から法的効力を持つ（カリフォルニア州で操業する年間売上高 2500 万ドル以上の企業すべてが対象）。どちらの法も、ユーザーデータの管理をめぐる厳しい手順を定め、扱いを誤った事業者には多額の罰金が科せられることを警告している。

特に米国では、規制当局がパンデミックを理由に基準を実質的に緩めるとは考えにくい。カリフォルニア州検事総長のザビエル・ベセラは、CCPA の施行を推し進める揺るぎない意思を見せ、「我々は 7 月 1 日から本法の施行に本気で取り組みます。事業者の皆さんには、この危機的な状況において、データ保護に特別に配慮することを奨励します」と述べた。

事業の大部分をオンラインに移行させるのは、ただでさえ困難な大仕事だ。しかし幸い、プライバシーの問題への対処は、さらにもう一つの難事になるとは限らない。プライバシー侵害のリスクを最小化するために実行できる、シンプルで有効な手段がいくつもある。

今後の数カ月間で、迅速なデジタルトランスフォーメーションを合理的に、可能な限り安全に行うために、以下で挙げるプライバシー重視の施策を実践することを検討してみよう。それぞれは個別に実行可能だが、4 つすべてを達成すれば、プライバシーのリスクを大幅に軽減できるはずだ。

(1) 自社のベンダーと協業相手が顧客データをどう使っているのかに注意する

事業者は、デジタルトランスフォーメーションにおける多くの課題に対し、「プラグ・アンド・プレイ」（デバイスをコンピュータに接続すると、すぐに自動設定され使えるようになる）型のソリューションを約束する外部ベンダーとの契約に、すぐに飛びつきたくなるかもしれない。そして技術調達の過程で、データ処理契約（DPA）をすべて確認する必要性を認識しながらも、この段階を飛ばせばどんな事態を招くかを甘く考えがちだ。

CCPA と GDPR の規則では、顧客データを処理する第三者へのデューデリジェンスを怠った事業者は、金銭的責任を問われる可能性がある。実際に 2019 年、英国の ICO（個人情報保護監督機関）によってマリオット・ホテルグループが 1 億 2300 万ドルの制裁金を課されたのはこれが理由だ。

ベンダーの DPA を確認するうえで注視すべき重要な点は、相手がプライバシー保護の義務に準拠していること、および相手のデータ取り扱い方針が自社の方針と整合していることである。そうでなければ、自社のプライバシーポリシーにみずから違反するリスクを負うことになる。

加えて、ベンダーのいかなる DPA においても、協力会社（下請け）に関する文言を確認しよう。こちらから明示的に指示しない限り、ベンダーは別の業者に再委託をしない、という確約が必要だ。これによって、もしベンダー側が独断で規則を守らない第三者にデータ業務

を任せた場合、自社は法的に保護される。

(2) データを処理する際、リスクを監視するために影響評価を行う

データ処理における影響（インパクト）評価は、GDPR では多くのケースで義務づけられているが、CCPA では義務化されていない。とはいえ、急激な過渡期には、データ処理作業における基本的なリスク評価を実施すれば（それがどれほど退屈でも）、事業者はデータの保管や外注、その他諸々の事項について、潜在的に有害な決定を下す前に否応なく、じっくり考えることになる。

また、プライバシー保護違反の罪を問われた場合、リスク軽減に向けた積極的な取り組みを証明する行動記録があれば、規制当局に好ましく解釈される。

英国の ICO は「データ保護影響評価（Data protection impact assessments）」のテンプレートを無料で提供している。これを使えば、事業者は英国拠点の有無にかかわらず、プライバシーのリスクを正確に評価するための適切な手順をたどれるだろう。

(3) プライバシーポリシーの明確化に努める

CCPA の施行を前に、自社のプライバシーポリシーが主要ステークホルダーによって見直されるにあたり、文書がどのように解釈されるかを考慮しよう。目標はこのポリシーを、法律用語に明るい人だけでなく、自社の全顧客に理解してもらえるようにすることだ。

今後のいかなる規制要件にも対応できるよう、解釈の幅が広い文言を盛り込めば、自社を守ることになる――そう思う人もいるかもしれない。しかし優先すべきは、プライバシーに関する知識を増やしつつある顧客に対し、自社のポリシーへの理解を助け、会社を信頼してもらうことだ。

スラックのプライバシーポリシーからは、読み手にとってのわかりやすさと内容の綿密性は両立できるということが見て取れる。

(4) データ保護オフィサー（DPO）を指名する

事業規模の大小にかかわらず、データをめぐる意思決定は複数の部門に責任を分散させるよりも、中央で一元化するほうが望ましい。これは急激な過渡期には、まさに当てはまる。

DPO（Data Protection Officer：データ保護オフィサー）は、プライバシー保護の問題に関して組織内で中心的役割を担う。そしてプライバシー法執行の性質が不透明な時期に、規制機関との連絡・調整役として非常に重要となる。たとえプライバシーの問題に精通した人でなくても、プライバシー保護に目を光らせる権限を一人の担当者に移譲することは、手早く経済的にリスク軽減を図れる方法だ。

本稿冒頭で述べたように、迅速なデジタルトランスフォーメーションをうまくやり遂げるには、リスクを伴う行動が必要かもしれない。とはいえ事業者は、プライバシー保護の強化に向けたシンプルかつプロセス主導型の手法を実践できる。目下の状況では、規制当局の

寛大さに頼ることは無用のリスクとなるのだ。

データのプライバシー保護の実施には、経済学者が言う「時間的非整合性」というジレンマの特徴が多分に表れる。いま実行するには時期尚早に思えても、いざ実行するときには遅すぎるのだ。そして過去数週間で見られたように、「遅すぎる」ことは、事業の重要な岐路での深刻なつまずきとなるかもしれない。

HBR.org 原文：Have Your Privacy Policies Kept Up with Your Digital Transformation? June 29, 2020.