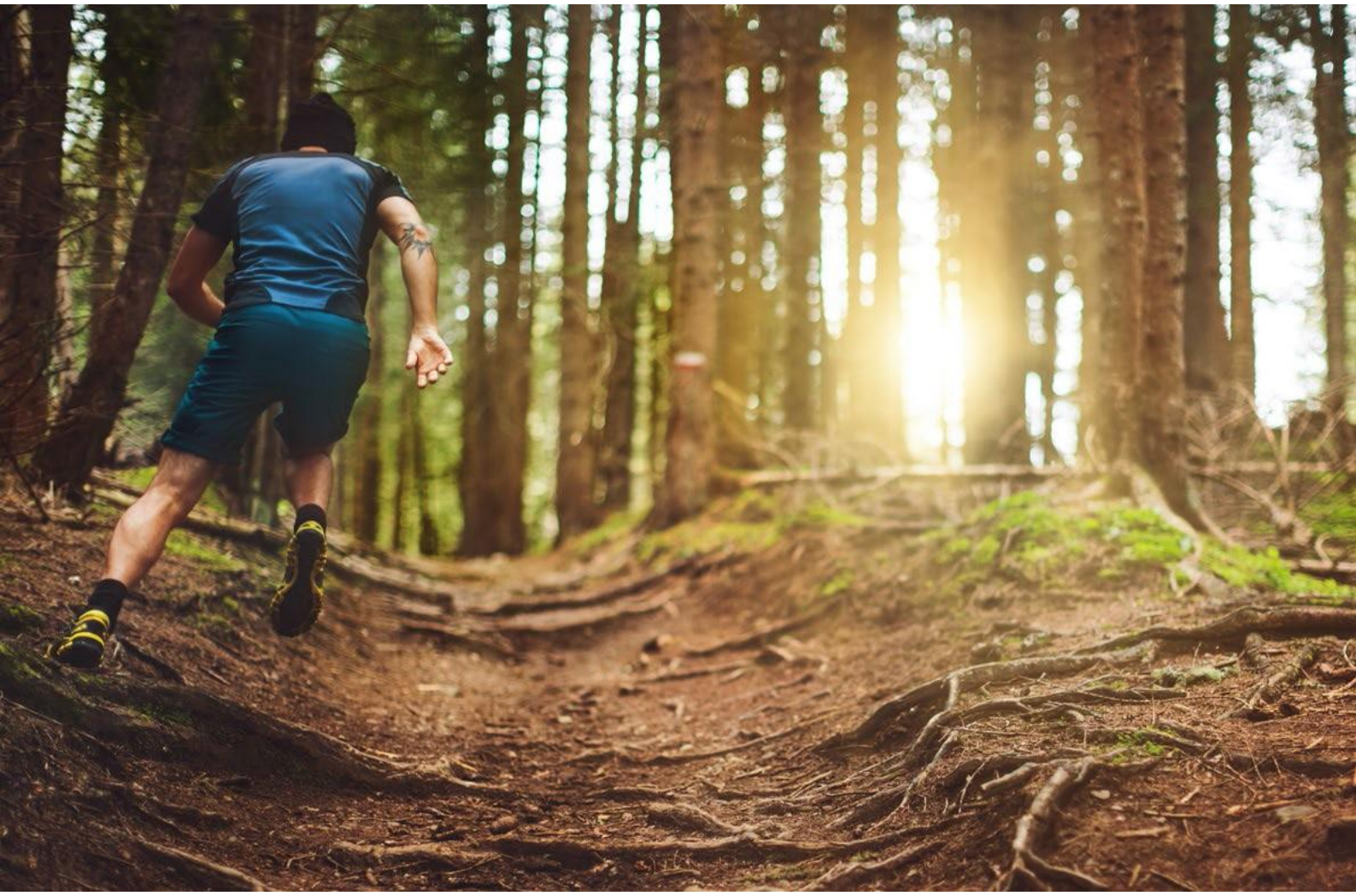
GDPR &Beyond
#GDPRbeyond

ビジネスホワイトペーパー

GDPRへの迅速な対応が必要とされる理由



MICRO FOCUS

CIO FROM IDG

GDPRの施行が間近に迫る中、EU全体で適用されるデータ保護法への全面的な改正に対して、各企業が着々と準備を進めているだろうと思われています。

ただし、それは楽観的な考えに過ぎません。EU各国で一般データ保護規則 (GDPR) が5月28日に施行されるというのに、どの調査結果を見ても、準備ができている企業は半数にも満たないのが現状です。そして何よりも、去年の3月末に発行されたある調査によると、英国内の約4分の1の企業が、英国のEUからの離脱によってGDPRが適用されなくなると勘違いした結果、GDPRへの準備を中止してしまったことが判明しました。

しかしながら、Canon EuropeのQuentyn Taylor氏が指摘するように、GDPRはEUからの離脱に関係なく適用されることが2016年の10月に明示されています。

オランダに拠点を置くAttorney Firstで弁護士を務めるJudith Vieberink氏は、次のように述べています。「多くの企業ではGDPRに向けた準備を進めているものの、全体としては準備が遅れています」

「・・・GDPRに向けた準備を進めているものの、全体としては準備が遅れています」

Attorney First、Judith Vieberink氏

最後までGDPRを後回しにする企業

多くの企業はすでに準備を進めています。Taylors氏は「大企業はすでに準備が進んでいるようです」と述べています。「つまり、大企業はプライバシーや信頼を重視することに対応できています。これらの大企業にとって最も大事な要素を適切に取り扱うことで、顧客は企業を信頼して取引を望むようになるのです」

GDPRがもたらす変化を考えれば、準備をギリギリまで後回しにするのは問題です。GDPRの施行による最大の変化は、制裁金が大幅に増えるということです。規則への準拠を怠った場合、最大で2000万ユーロまたはグループ全体の年間売上高の4%のうちいずれか高い方の金額が制裁金として課せられる可能性があります。

変更されるのは制裁金の額だけではありません。GDPRは、組織によるデータの管理方法を抜本的に変革します。

主な変更点の1つはGDPRが適用される地理的範囲であり、準備をやめてしまった英国企業の多くが誤解している点です。GDPRは、EU加盟国内の企業だけではなく、EU市民の個人データを扱うすべての企業に適用されます。簡単に言えば、顧客、契約相手、提供元、あるいは従業員がEU市民であれば、どの国の企業であってもGDPRが適用されるということです。

またGDPRにおいては、「同意」も厳密に定義され、要求されます。GDPRでは、データ主体、つまり個人を明示する必要があり、また同意の撤回も自由に行使できるようにしなければいけません。その一環として、GDPRではデータ管理者の透明性をより厳密に求めています。企業は、データ管理者またはデータ保護責任者 (任命されている場合) との連絡情報をいつでも提供できなければなりません。

この透明性を実現するため、個人データを収集する理由、その使用目的、海外に転送する場合の詳細、そしてデータの保有期間を明確に示す必要があります。

2000万ユーロ

制裁金の大幅な増額

重大な違反を犯した企業には、2000万ユーロまたはグループ全体の年間売上高の4%のうちいずれか高い方の金額が制裁金として課せられる可能性があります。

市民に再び力を

GDPRがもたらすもう1つの大きな変革は、個人データの修正や削除について、個人がより強力な権利を持つようになるということです。これは各方面で論じられている「忘れられる権利」の一環であり、現在のデータ保護法 (英国) やEUデータ保護指令において認められている権利を大幅に拡大したものです。

GDPRでは、データは特定の目的についてのみ収集と加工が許可され、データを将来の利用のために保管しておいたり、同意を得た目的以外のために加工したりすることはできません。

そして言うまでもなく、データは安全に保管される必要があり、セキュリティはGDPRの絶対的な主要原則の1つです。GDPRでは、データの保管庫に鍵を掛けたり、後で何らかの措置を講じるような対策ではなく、「プライバシーバイデザイン」が求められます。

つまり、セキュリティとプライバシーは、プロジェクトの最初から考慮されなければならない主要事項であり、潜在的な問題を可能な限り早期に特定して解決することが必要とされます。

データ保護責任者の任命

GDPRでは、新たにデータ保護責任者 (DPO) を任命する必要がありますが、これはGDPRの対象となる多くの企業では新たに設けられる役割となります。

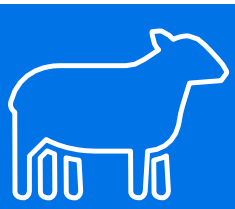
この要件の草案は、多くの専門家から曖昧な点があると指摘されています。 規則の第37条では、公共機関はDPOを任命しなければならないと規定していますが、その後の規定は曖昧です。

GDPRの目的から言えば「公共団体」の定義は各国の法律に準拠するものとなるため、国によって若干の差違が生じますが、専門家は「公共団体」には地方機関や政府の部署などだけではなく、エネルギー会社や運輸会社など、公共の社会機能を担う民間企業も含まれると考えています。

会社で個人データを定期的にあるいは体系的に処理している場合、あるいは性的嗜好、健康状態、犯罪歴などの「特殊なカテゴリのデータ」を取り扱っている場合は、ほぼ間違いなくDPOが必要となります。

誰をDPOに任命すべきかということも、また別の曖昧な問題です。契約社員でも正社員でもかまいませんが、何よりも適切な資格を持つアドバイザーであり、同時に独立した監督者であることが求められます。

DPOは、規則に準拠するためのアドバイスを提供でき、企業のITおよびセキュリティインフラに詳しく、さらに業務を完遂するのに十分なリソースを持っている必要があります。DPOの業務は、部下に任せられるような内容ではないからです。



データの役割 保護責任者

Vierberink氏はDPOの役割を「5本足の羊」と例えています。つまり、DPOは技術チーム、経営役員達、法務チーム、および監査チームとコミュニケーションを取りつつ、道徳的に行動しなければなりません。
Vierberink氏は次のように補足しています。「DPOは、不法行為と無思慮な行動を上手に見極めなければなりません」

「『木を植えるのに最適な時期は30年前』ということわざがあります。ですから、まだ始めていなければ、今すぐ始めましょう」

Canon、Quentyn Taylor氏

すべての企業にDPOが必要なわけではありませんが、Canon Europeの情報セキュリティ責任者であるTaylor氏は次のようにアドバイスしています。「公式にDPOが必要とされていない場合でも、DPOに適した人材を探すべきです。そのような人材はまれなのですから」

「社内で適任者を見つけることもできますし、外部の人間と契約することもできます」と前述のVieberink氏は補足します。大きな問題は「DPOの独立性をどうやって維持するか」ということです。

「まだ始めていないのなら、今すぐ始めましょう」

GDPRへの準備は大仕事であり、2018年5月25日へのカウントダウンはもう始まっているのです。計画を先延ばしにしがちな会社であるならば、今こそが始めるべきタイミングです。

「規則への準拠は簡単な仕事ではありません」とVierberink氏は警告します。ロードマップの計画の最初は、既存のプロセスを理解し、仕事の相手を理解することであるとVierberink氏はアドバイスしています。それを知ることで「仕事の規模が把握できる」のです。

まだほとんど準備が進んでいない中小企業に対しては、Taylor氏は次のようにアドバイスしています。「地元の規制機関、英国であれば情報コミッショナーオフィス (ICO) に行けば、計画に役立つ資料が多数あります」

さらに、すべての規模の企業にあてはまる最後のアドバイスとして次のように述べています。「データフローを特定することです。ツールに頼るのではなく、自ら手に入れた知識に頼ってください」

「『木を植えるのに最適な時期は30年前』ということわざがあります。ですから、まだ始めていなければ、今すぐ始めましょう」

GDPR & BeyondのWebサイトはこちらからご覧いただけます

「今、先行しているのは大企業です」

Canon、Quentyn Taylor氏

GDPR &Beyond

#GDPRbeyond