GDPR 確立後のデータ保護とサイバーセキュリティ

#KingstonIsWithYou

GDPR 確立後のデータ保護とサイバーセキュリティ

序文

GDPR に備えて進取的に取り組みと雇用を行った企業や組織は少なくありません。貴社もその一社に数えられるかも知れません。しかし、サイバー脅威の進化は止むことがなく、したがって企業は息をつく暇がないのが現状です。GDPR は一度だけのコンプライアンスで済むものではなく、データ保護とサイバーセキュリティを継続する上での判断に必要なフレームワークです。つまり安心する余地はないのです。

本 eブックは、英国で最も経験豊富なサイバーセキュリティ解説者が、GDPR の確立に伴ってデータ保護がどのように変化したかについて簡単にまとめたものです。さらにコンプライアンスの必要性について企業が従業員を教育し、IT 部門とテクノロジープロバイダが IT インフラストラクチャを効率的に確立し、セキュリティの新生課題についてエンドユーザーに情報を提供する手段についても触れて行きます。

GDPR 確立後のデータ保護とサイバーセキュリティ

著者

本 eブックはデータ保護とサイバーセキュリティの専門家 5 名からの出稿を簡単にまとめたものです。

Rob Allen
@Rob_A_kingston

Rob 氏は Kingston Technology のマーケティング & テクニカルサービス・ディレクターであり、1996 年に同社に入社しました。Kingston のすべてのブランドと製品の PR、ソーシャルメディア、チャネルマーケティングを、Digital Marketing Media and Creative を通して統括する責任者です。

Tara Taubman-Bassirian
@clarinette02

Tara 氏は、弁護士、運動家、調停者、研究者、コンサルタント、後援者、作家といった数多くの肩書を持ち合わせています。プライバシー、知的財産、データ保護における専門知識を生かし、同氏は英国をはじめ、フランス、米国など世界を舞台に活躍する著名人として知られています。

Rafael Bloom
@rafibloom73

Rafael 氏は Salvatore ltd. のディレクターであり、テクノロジーと規制の変化によって生まれる戦略的、商業的、手続き上の問題と機会の管理を支援しています。

Miriam Brown
@Kingston_MBrown

同氏は Kingston Technology の B2B マーケティング・マネージャーであり、1997 年に同社に入社しました。Miriam 氏はすべての Kingston B2B 製品のマーケティング戦略、コンテンツ、キャンペーンを展開する責任者です。

Sally Eaves
@sallyeaves

Sally Eaves 教授は倫理的テクノロジーの支持者として知られており、最高経営責任者、最高技術責任者、教授 (Emergent Technologies)、グローバル戦略アドバイザーといった豊富な経歴の持ち主です。Sally 氏は受賞歴を持つ国際基調講演者、著者、研究者であるほか、独創的かつ権威あるソートリーダーシップを説くインフルエンサーでもあります。

GDPR 確立後のデータ保護とサイバーセキュリティ

目次

セクション 1 – GDPR が確立してから データ保護はどのように変わりましたか？

道のりは長い。過去 2 年間、諸企業の法務部は多角化しなければならなかったため、データ保護責任者の採用件数が急増[1] したほか、データプライバシーのコンサルティングを外部に依頼する件数が増大しました。データ保護にもたらされる影響評価 (DPIA) を通して情報を提供した企業は数千にものぼっているはずです。

しかし長い道のりは踏み出したばかりなのです。

GDPR の最大の課題は、入念な監視が必要であるということです。組織を問わず、スタッフが規則違反を犯しうる可能性は常に存在するのです。こうした問題は人材不足気味のセクターのほか、医療、教育、法律などといった自治的なセクターで深刻化します。例えば法律セクターでは、弁護士の間で機密性の高い訴訟情報を電子メールに添付して交換し合うことが疑問視されないといった例は枚挙にいとまがありません。医療関係者は患者データや MRI スキャンデータをセキュリティが施されていない電子メールアドレスで送受信したりします。重大なストレスにさらされている企業の場合、対処しなければならない事項が多すぎてストレスのレベルが一線を越えたときにコンプライアンスが無視されがちになります。生産性は時にしてプロトコルを犠牲にする結果を招きます。

変革が必要なのです。

チャリティーセクターにても意識の見落としが見られます。チャリティー関係者の間では、自組織が GDPR の対象にならないと考えがちです。GDPR は民間セクター、公共セクター、第三セクターを問わずすべてのセクターが対象になることを理解していたとしても、データ保護に予算を割くことを嫌います。

つまり目的は高尚であっても対応が非現実的なのです。GDPR 違反による罰金はかかりうる IT コストをはるかに超えるのです。

Tara Taubman-Bassirian
@clarinette02

GDPR、データ保護、IP コンサルタント

「第三セクター企業の間でよく聞かれるのは、‘「当社は慈善団体だ。GDPR の対象にはならない。」ということです。ウェブサイトのコンプライアンスを取ってみても、収集しているデータではなく、訪問者のデータを第三者にアクセス可能にさせていることが問題なのだと説得し続けています。」

2016 年以来

データ保護責任者 (DPO) の需要は700% 増え、急増の動向を見せています。

1. その他：GDPR の年間状況：知っておくべき統計情報と要点 www.varonis.com/blog/gdpr-effect-review/ [アクセス日 26.11.19]

GDPR が確立してからデータ保護はどのように変わりましたか？

データミニマイゼーション (data minimisation) が活用され始めている

現代社会ではデータの収集が容赦なく行われています。「ビッグ 4」(Google、Apple、Facebook、Amazon) は膨大な顧客データを保有しています。他の企業もビッグ 4 を模倣して可能な限り多くのデータを収集すると考えられます。しかし保有するデータが多くなるほどリスクも増大していくのです。GDPR が確立してから最も好ましいトレンドは、過剰なデータ収集に対する反発があるということです。懸命な企業はデータミニマイゼーションのコンセプトを取り入れています。つまり、必要なければ収集するなという考え方です。

Tara Taubman-Bassirian
@clarinette02

GDPR、データ保護、IP コンサルタント

「データミニマイゼーションは GDPR のコンセプトを最もよく反映したものの一つと言えます。いかなるデータベースでも、構築した時点でリスクとなるからです。」

Rob Allen
@Rob_A_kingston

Kingston Technology マーケティング & テクニカルサービス・ディレクター

「当社では、データの削除については厳格なルールを設けています。当然のことながら業務機密データは適正に保管されなければなりません。ただしその他のデータは1 年経過した後、削除します。保有する意味がないわけですから。」

このメリットはリスクを制限する以外にもあります。例えばマーケティングを例に挙げてみましょう。マーケティングのデータベースが整理されていない場合、陳腐化したデータを保有していることになります。データベースが何万人もの規模になると電子メールでマーケティングキャンペーンを頻繁に展開した場合、コストがかさんでいきます。それどころかキャンペーンのパフォーマンスデータが歪むことにもなります。

データミニマイゼーションは物理的なデータにも適用されます。顧客パスポートのスキャンデータを印刷するときは気をつけてください。また、アカウントのパスポートの書き取りも注意が必要です。データの物理的なコピーが必要なときは安全に保管しなければなりません。膨大な量の書類が置かれているデスクは威圧的に見えますが、安全であるとは言えません。

Rafael Bloom
@rafibloom73

ディレクター、Salvatore Ltd

「テクノロジーと現行ビジネスの関係については、見方がこれまでと全く変わっています。経営者の間でこうしたハイレベルのデジタル思考が必要不可欠になっています。」

GDPR の影響：企業経営陣から消費者にいたるまで

規制面でのコンセプトに基づくデータ保護は数十年前から存在しています。しかし Google[1]、ブリティッシュ・エアウェイズ、マリオットホテルチェーン[2]などといった大企業に課せられた罰金、そしてこれがニュースで報じられたことで、諸企業の経営陣は GDPR を重視せざるを得なくなりました。つまり大企業から中小企業へまで事態が波及したのです。

1. その他：GDPR の年間状況：知っておくべき統計情報と要点 www.varonis.com/blog/gdpr-effect-review/ [アクセス日 26.11.19]
2. The Guardian：GDPR がブリティッシュ・エアウェイズとマリオットホテルに課した罰金 £300m は何に使われるのか？ www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [アクセス日 26.11.19]

GDPR が確立してからデータ保護はどのように変わりましたか？

続く…

データ保護の強化を促しているもう一つの要因には取引先との関係があります。大企業は契約業者がデータ漏洩を起こしたことによって損害賠償の責任を負わされることを避けるため、契約を結ぶ前にサプライヤーのデューデリジェンスを綿密に行います。

商業的観点から GDPR が重視されるようになった一方、消費者はデータに関する権利をこれまで以上に認識しています。企業が消費者のデータ管理能力を失った場合、ここで注目すべきなのは、それがたとえデータ漏洩ではなくても消費者は賠償責任を問う権利があるということです。企業は細心の注意を払わなければなりません。

Sally Eaves
@sallyeaves

Sally Eaves Consultancy - CEO/ディレクター

「データ保護は企業にとって信頼の維持を左右する不可欠なものとなっています。」

セクション 2 – 企業は従業員をどのように教育していますか？

職場で「またか」とよく言われるがスタッフトレーニング。

したがってトレーニングは充実したものでなければならない。学識のあるスタッフはデータ保護に異論を唱える可能性が低い。データセキュリティのトレーニングをスタッフに提供している場合、たとえデータ漏洩があっても、情報保護監督機関 (ICO) は寛大な判決を下し得る。

Rafael Bloom
@rafibloom73

ディレクター、
Salvatore Ltd

「データをサプライチェーン品目と考えるようにしています。つまり品目の出所からライフサイクル全体にいたるまで適切な管理が必要であるということです。チームを会議室に集めて書類をシュレッダーにかけるなとか、ちゃんとしたパスワードを使えとか強要すれば確かに組織のリスクは下がるかも知れません。しかし、ただ物事を強要するだけで、長期的にみて大きな違いはあるのでしょうか？答えは「ノー」です。

ところが 2019 年 4 月に、デジタル大臣である Margot James が英国企業・組織 10 社のうち、3 社がサイバー脅威に対処するためスタッフをトレーニングしたという声明を出しています。トレーニングを重視する時期に直面しているのです。

トレーニングとは、選択肢方式の問題にチェックを入れていくのではなく、新しい文化を生み出すことなのです

つまり机上のレベルを超え、行動と文化を根本的に変革するトレーニングを展開します。データ保護に関連する質問に答えるだけのオンライントレーニングを購入するのは簡単です。しかしそれで会社を本当に守れるのでしょうか？

優れたデータ保護行動には、基盤となる 2 つの要素があります[1]。つはトレーニング臨機応変で充実しており、自社特有の課題を反映していることです[2]。つ目は、全従業員が携わる日々の業務活動と職場の文化を根本的に見直す必要性をもたらすのが GDPR であるということです。データについては組織を通して正しい方法で正しく行動する必要があります。例えば人事を例に挙げてみましょう。採用候補全員の詳細情報がそのままメールサーバーに置かれているとしたらどうでしょうか？
データ保護は各自の責任です。

1. インテリジェント CISO：1 年たった今、GDPR はデータセキュリティにどのような影響を与えたのでしょうか？
www.intelligentciso.com/2019/04/16/one-year-on-what-has-been-the-impact-of-gdpr-on-data-security/ [アクセス日 26.11.19]

企業は従業員をどのように教育していますか？

データの背後には必ず個人が存在します

消費者がデータに関する権利をこれまで以上に認識するようになったことは上のセクションで前述しました。データ保護トレーニングを効果的に行うには、データの背後に必ず人がいるということをスタッフに理解してもらう必要があります。従業員に、データを渡したすべての組織について考えてもらってください。データを保護するとは個人のプライバシーを守ることであると気づくはずです。

緊急対策を設ける

Sally Eaves
@sallyeaves

「データセキュリティとプライバシーに関する教育を継続的に進めることは企業にとって不可欠です。これは、一回限りまたは年に一度のトレーニングセッションであってはなりません。先行的で臨機応変かつ充実したトレーニングでなければなりません。移行、管理、防御すべきデータについて従業員との対話が必要です。」

Miriam Brown
@Kingston_MBrown

「トレーニングで従業員に、'これが自分のデータだったらどうするかと問いかけてみたらどうかと思います。取引先の銀行のマネージャーがもし自宅勤務していて、彼のラップトップに機密情報がある場合、自分だったらその情報が暗号化されたドライブに保管されなければならないと思います。

Rob Allen
@Rob_A_kingston

「データは自分のものであるかのように扱いましょう。」

セクション 3 -
IT 部門はデバイスのセキュリティを強化できますか？

テレワークは今日、一般的になっています

スタッフは複数のデバイスで業務データにアクセスします。自分のデバイスを列車やタクシーの中に置き忘れてしまうことも考えられます。そこで自社をセキュリティやデータ漏洩のリスクに晒さないでスタッフに効果的に働いてもらうにはどうするかが課題となります。データ保護のために積み上げてきたことがたった一人の従業員によって水泡に帰すことがあり得るのです。

Sally Eaves
@sallyeaves

Sally Eaves Consultancy - CEO/ディレクター

「データは送信中、保留中、そして使用中に保護されなければなりません。したがってこれらすべての状況でセキュリティ、復旧、データ喪失など含む全面的な対策が必要です。例えば暗号化処理されていない USB、暗号化されていない添付ファイルを送信、重要なユーザーデータを表示するウェブブラウザなど、見逃されがちなリスクに注意することは特に重要です。多数のデバイスがつながっている状態で勤務形態が進化し続けるなか、モバイルフォンに保存されているデータは会社のサーバーに保存されているデータと同様にセキュリティが施されなければなりません。

二要素認証 (Two-Factor Authentication)

一般企業にとって最も簡単な対処法はネットワークペリメーターを保護することです。つまりパスワードマネージャーと二要素認証を使用します。それだけです。単純なのです。二要素認証の良い例は、ユーザーがラップトップでパスワードを入力した後、モバイルフォンに送信されたパスコードをさらに入力するという方法です。

VP および暗号化された SSD/USB

SME では VPN の使用が普及されつつあります。これは公共の Wi-Fi ネットワークでビジネスデータにアクセスするスタッフの間で顕著に見られる傾向です。ただし企業は VPN 機能を過信しないよう注意する必要があります。VPN はソリューションの一部であって、完璧なものではありません。テレワーカーのハードウェア暗号化処理がかかっていないノートパソコンやラップトップに企業が VPN を実装するケースは少なくありません。自分のラップトップにファイルを保存しない人はいません。そのラップトップがハッカー攻撃にあったり、紛失したり盗難にあった場合、どうなるのでしょうか？暗号化処理された USB、SSD の価格は標準バージョンよりも幾分高いだけなのです。暗号化処理された USB を展開し、ノートパソコンにハードウェア暗号化処理がかかった SSD を装備することは、テレワーキングの課題解決に重要な役割を果たします。そうすればたとえデバイスを紛失したり盗まれても暗号化されたファイルにアクセスされることはありません。紛失した USB をリモート削除することもできるのです。

「サイバーセキュリティの専門家が二要素認証を導入するよう CEO を説得しようとしたにも関わらず、同意を得られなかった経験があります。'「面倒だ。手間がかかる。やりたくない。」というのです。その会社はそれから間もなく、詐欺に合い、£40,000 の被害を被りました。」

Rafael Bloom
@rafibloom73

ディレクター、Salvatore Ltd

「結局のところ、セキュリティの意識を高めるには、従業員と話し合って安全で生産的な戦略を見いだすことです。

Rob Allen
@Rob_A_kingston

Kingston Technology マーケティング & テクニカルサービス・ディレクター

IT 部門はデバイスのセキュリティを強化できますか？

プライベートサーバー、MSP

大企業の多くがオンサイトサーバーの設置に向けた準備を進める傾向が再び見られるようになりました。オンサイトサーバーを設置することで、公共アクセスが可能なクラウドには一切データを保存せずに済むため、独自サーバーの完全管理が可能です。一方、機密性の低いデータをクラウドに置き、個人データはオンサイトで管理するといったハイブリッドサーバーソリューションもあります。第三セクターの中小企業や組織では独自サーバーの設置はコストがかかりすぎるかも知れません。そこで検討に値するのがマネージドサービス・プロバイダやプライベートサーバーです。膨大な運営コストがかからずにセキュリティの対処が可能になるからです。

期限切れデータのオートフラグ

GDPR のコンセプトの一つは古くなったデータの削除です。例えば特定の個人データを 7 年以上保有すべきではありません。データが「期限切れ」になりかけたら知らせてくれる機能があったらどうでしょうか？適切なデータベースがあれば、データ保有期限が近づいたときに DPO に通知を自動送信するプログラムを社内の IT チームに作らせることは簡単です。

適格なベンダーを確保する

IT セキュリティ関連のメーカーやベンダーの数には限りがありません。リサーチをお忘れなく。自社の業界やセクターで特化した専門知識を持ち合わせている信頼あるプロバイダが提供するシステムを導入することが重要です。選んだベンダーがテクノロジーを持っているかだけでなく、導入にあたってデータセキュリティ上の課題を理解しているか判断する必要があります。

セクション 4 – テクノロジープロバイダはプロセスと不測事態対応度の把握をどのように改善できますか？

DPO の確保と保持

2016 年以来、データ保護責任者 (DPO) の需要は 700% 増となっており、急増していることがわかります。[1] ヨーロッパの雇用 DPO 人口は 500,000 人にも上ります。これは 2017 年当時の予測数の 7 倍です。[2] しかしながら DPO の役割は重視されず価値が認識されていないのが現状です。

DPO は企業全域にわたるセキュリティとデータプライバシー事情を見極めなければなりません。重大な責任が課される職務なのです。しかしながら企業によってはテクノロジーを最もよく理解しているスタッフに DPO という肩書を与えるだけの場合もあります。こうしたフタッフに、通常の職務をこなしながら企業全体のデータプライバシーを保護する責任が課せられるのです。

現実的には、このように新しく就任した DPO にサポートの一環として専門のサービスやツールが提供されなければなりません。専属の DPO がいる場合でも、データセキュリティは変化が速く、セカンドオピニオンが必要となる課題に必ず遭遇することになります。データセキュリティに関して外部のコンサルタントや弁護士を雇うことは賢明と言えますが、まず社内の状態をきちんとすることが大切です。

事態の明確化、コンティンジェンシープラン、デジタルコヒージョン

企業 IT インフラストラクチャの健全性は最も脆弱な部分が左右します。したがって自社の IT エコシステムに新しい要素を導入する時点で、セキュリティ面でどのような脅威があるかを明確に把握し、新しい製品を安全に使用する上でテクノロジープロバイダが明瞭なアドバイスを提供しなければなりません。

Tara Taubman-Bassirian
@clarinette02

GDPR、データ保護、IP コンサルタント

「髄所に CCTV カメラを設置するスタッフには、パスワードで保護されていなければセキュリティの価値がないと言っているんです。ウェブサイトにログオンして監視するだけですよね。それは強盗に、「留守にしているときにいつでもどうぞご覧ください」と言っているようなものです。

1. その他：GDPR の年間状況：知っておくべき統計情報と要点 www.varonis.com/blog/gdpr-effect-review/ [アクセス日 26.11.19]
2. The Guardian：GDPR がブリティッシュ・エアウェイズとマリオットホテルに課した罰金 £300m は何に使われるのか？ www.theguardian.com/business/2019/jul/10/gdpr-fines-ba-british-airways-marriott-data-watchdog [アクセス日 26.11.19]

テクノロジープロバイダはプロセスと不測事態対応度の把握をどのように改善できますか？

課題は不測事態への対応です。製品が寿命に達し、アップデートが必要な場合、どうしますか？保存されているデータに不測の事態が生じたり、IT の広範なエコシステムにセキュリティの欠点が発覚した場合、テクノロジープロバイダは緊急対策を助言できなければなりません。例えば MRI スキャナーを例に挙げてみましょう。患者の画像保存用に、暗号化処理された 4 テラバイトの SSD を装備しているとします。保存容量が限界に達したらどうするのでしょうか？

テクノロジープロバイダのみならず組織が、組織内で、および外部サプライヤーやパートナーと提携する際、デジタルコヒージョンおよびデータコヒージョンの環境を確保する必要があります。例えば NHS など、多角的に運営し、多数の部門を持ち、拠点が複数ある組織にとって、これは不可欠な対策です。

Miriam Brown
@Kingston_MBrown

Kingston Technology B2B
戦略マーケティングマネージャー

「当社は NHS に多くの製品を販売しました。しかし、どのようなデータ保護ポリシーとプロトコルが設けてあるか聞くと相手によって違う答えが返ってきます。」

ホライズン・スキャニング

テクノロジーの進化はセキュリティのペースを超えることがあります。例えば中国の顔認識技術を使った決済など、企業はセキュリティやデータ保護のリスクが明確化される前にテクノロジーをわれ先と取り入れようとします。浸透が進んでいる 5G ネットワークにおいては後 1、2 年でエッジコンピューティングや分散データサイロが現実となります。テクノロジープロバイダは既存のデータ保全性や IT セキュリティを犠牲にすることなく、新生テクノロジーのメリットを安全に享受できるよう企業を支援していかなければなりません。

Sally Eaves
@sallyeaves

Sally Eaves Consultancy -
CEO/ディレクター

「GDPR については、導入時の苦慮よりも、強化された IT プロセス、バックアップと復元、セキュリティ改善、競合他社との差別化といった利点をより重視する傾向に向かうと思います。

まとめ

GDPR は、企業経営陣や消費者などにデータプライバシーとネットワークセキュリティの重要性を促すことで改善をもたらしました。しかしコンプライアンスにおいては組織の全員がデータセキュリティを日々欠かさず継続的に監視していく必要があります。常に進化し続けるテクノロジーとサイバー脅威に対応するには、確かなセキュリティインフラストラクチャと充実したトレーニング、さらにテクノロジーとデータプライバシーに関するコンサルティングサポートが欠かせません。組織全域にわたってデータ保護の文化を浸透させる上で、データの背後には常に人がいることを各自に認識させることで優れた結果につながります。文化の変革は選択肢方式の問題にチェックを入れる演習型のトレーニングよりもはるかに効果があるのです。

Kingstonの紹介

32 年の実績を持つ Kingston は、企業が直面するテレワーキングの課題を特定し、解決する知識を有しており、
組織をリスクにさらすことなく従業員がどこにいても安全に業務に従事できるようにします。

#KingstonIsWithYou