TEALIUM

データガバナンス:

セキュリティとプライバシーを守る

はじめに

私達の社会は益々国際化しており、オンラインブランドの多くは世界中にプレゼンスを持っています。しかし、異なる国でビジネスを行うためには、その国に合わせたアプローチをとる必要があり、それはデータの保護やプライバシーについても同様です。本社がアメリカにあり、そこで全てをコントロールしているとしても、他国のデータプライバシー法制には十分な注意を払う必要があります。

2016年7月、アメリカとヨーロッパの間でSafe Harbor協定に代わってEU-US Privacy Shieldが発効しました。そして2年以内にGeneral Data Protection Regulation (GDPR) が発効し、全ての企業は特定の手続きに従わなければならなくなります。これまでのデータ保護法制ではアカウンタビリティと透明性の原則が絶対的な要件でしたが、これからはGDPRの新しい法的枠組みをきちんと理解することが、現代の国境を越えたデジタルエコノミーに係わる企業と消費者の双方にとって重要だといえます。

増え続けるデータプライバシーとセキュリティへの責任を果たすことと、シームレスな顧客エクスペリエンスを提供することの間で、どのようにバランスをとるべきでしょうか? 用心こそが重要だという意見がありますが、それは企業がこれらの新しいガイドラインによる法的なリスクだけでなく、情報漏洩やセキュリティ事故が起こった際にブランドに与える影響も考慮しなければならないからです。業界の一員として、私達はエンドユーザーに対してデータの透明性と倫理性に責任を持ち、どのような情報が収集されているのか、そしてそれらはエンドユーザーによりよい顧客エクスペリエンスを提供するために使われているのであるということを丁寧に説明していかなければなりません。適切な解析と計画に時間を投資することで、リスクを最少化し、信頼を構築し、ブランドを保護することができます。

これから起こるであろう大きな変化の予兆が現れてきました。私達は業界の一員として、先手をとってこの問題に対処していかなければなりません。

本ホワイトペーパーは、効果的なデータガバナンス戦略の構築のために協業すべきベンダーの選定からポリシーや手続きの設定まで、すぐに取り組むべきステップについて解説します。そして、現在の法規制を理解し、組織内を成功裏に統合し、顧客に対してこれらの安全策をどのように提供すべきかについて検討します。

目次

1. ビジネスを取り巻く環境

データガバナンスに関する大きな法的変化がEUで起こっており、その動きは全世界に広がろうとしています。

デジタルマーケティングに関わるベンダー、チャネル及び顧客とのタッチポイントが急速に増えていることに加え、プライバシーを取り巻く環境が世界的に変化していることが、デジタルスペースにおけるデータガバナンスに深刻な問題を産み出しています。2015年10月にSafe Harbor協定[*1]に無効判決が出され、2016年7月にEU-US Privacy Shieldがそれに代わり、それから2年以内にさらに厳しいGDPR規制が法制化される見通しで、企業はこれらの新しい規制を遵守できない場合には、厳しい罰則を与えられるリスクに直面します。

Safe Harbor協定を置き換えたEU-US Privacy Shieldは、EUとアメリカの間でビジネスに関係する個人データを大西洋を越えて交換するためのフレームワークです。これはEU市民に高いレベルの保護を与えるために作られた規範的なガイドラインで、General Data Protection Regulation (GDPR)による罰則規定を含んでいます。GDPRは2018年5月に法制化される見通しです。

これらの新しい規制について、企業が理解しておくべき重要なポイントがいくつかあります。まず最初に、EU市民に物品やサービス(それらが無償であったとしても)を提供する際、あるいはEU市民の行動を監視するために個人データを処理する場合には、GDPRが適用されるということです。第2に、これらの規制はデータを管理する主体(お客様)がどこに居るかに関係なく、EU域内でのビジネスであるかどうかにも限定されずに適用されるということも重要です。

Privacy ShieldとGDPRを遵守しなかった場合の罰則は非常に厳しいものです。ビジターに対して明示的なオプトインを行わなかったなどの重大な違反の場合、罰則は2000万ユーロまたは企業の年間売上高の4%となっています。軽微な違反の場合でも、1000万ユーロまたは年間売上高の2%です。

EUのe-Privacy指令 (「クッキー指令」とも呼ばれる) は最近、GDPRとの整合性を確保するために改正が必要であることがわかり、再び注目されています。現在のe-Privacy指令は、企業のデジタル資産がEU市民のデータを集める方法を規定し、個人データの保存または取得にあたっては本人の同意を得る必要があると定めています。指令の改正時期はまだ確定していませんが、改正案を見る限り、このプロセスは企業にとってさらに複雑で混乱を招くものになりそうです。

*1 このEUからUSへのデータ移送を可能にするための7つの原則に基づくUSベースの法的フレームワークは、2015年に無効にされました

2. 主な推測

GDPRの規定では、規制に違反した場合に罰則を適用されるのはお客様の組織であり、違反したのが外注のベンダーであったとしても同様です。GDPRは個人データの取扱いにあたって管理者(お客様)とデータ処理者(ベンダー)の責任と義務について明確に定めていますが、データ保護の責任のほとんどは管理者(お客様)が負っています。

ブランドとデータの管理者として、お客様の組織はEU-US Privacy Shield及びGDPRを、直接または第3者を通じてベンダーに遵守させる責任があるのです。

EUで起こっていることは「炭鉱のカナリア」のように今後起こることの前兆です。近い将来、世界中のどの地域の顧客であるかに関わらず、同様のことがお客様のビジネスに影響を及ぼすでしょう。

また、EU市民のデータを守るための規制変更をEUが主導していることから、アメリカでもアメリカ市民のデータを守るための動きが出てくることは間違いありません。

アメリカのあるテレコム企業は、2012年に広告ターゲティングにおいてモバイル顧客を追跡するためにUIDH (unique identifier header)と呼ばれるユニークで削除不可能な識別子(スーパークッキーとも呼ばれています)の使用を開始しました。彼らはプライバシーポリシーで限定的な開示を行っていましたが、プライバシーポリシーにスーパークッキーに関する情報を含める改正を行ったのは2015年5月になってからでした。

その間に、オンライン広告企業がそのスーパークッキーの使用を開始しました。UIDHに関連付けられたクッキーIDは、エンドユーザーがそれを消去したとしても、ベンダー側で復元することができます。

FCCは、このテレコム企業がスーパークッキーについて正確で適切な情報をエンドユーザーに提供しなかったことは、FCCが2010年に出したネット透明性のルールに違反していると指摘しています。このテレコム企業は今後3年間に及ぶコンプライアンス計画を立てなければならず、UIDH情報を第3者と共有する前に、エンドユーザーからオプトインの同意を得なければなりません。

3. Tealiumが考える価値ある提案とは

Tealiumはデータのサプライチェーンにおいてユニークな地位を築いており、お客様がビジネスを進めるにあたってデータを適切かつ適法に管理できるようにお手伝いできる、信頼のおけるパートナーです。

デジタルマーケティングベンダーやデータ解析ベンダーに依存することなく、プライバシー規制を遵守することができます。特に、Tealiumは同意のための適切な設定を行い、データの収集と使用に関する透明性を確実に提供できるようサポートすることができます。どちらの要件もe-Privacy指令にとって重要です。

各国ごとのコンプライアンスに対応

国によっては、組織がオンラインビジターから収集できる情報のタイプや用意すべきプライバシーオプションの種類について定めた固有の法律を持っています。これにはデータ収集のためのタグも含まれ、すべての要素がその国のプライバシー規制を遵守する必要があります。

Tealium iQ Tag Managementは、地域ごとのプライバシーコンプライアンスをサポートしており、国毎に異なる規制を適用して各ベンダーのデータ収集過程を厳格にコントロールできます。このようなTealiumの柔軟性は、各国が選択的に対応することになるe-Privacy指令について、特に重要です。

エンドユーザー側でのコントロール機能

Tealiumは様々なお客様とのお付き合いを通じて深く幅広い実績を積んでおり、エンドユーザーと相対する最前線でいかにして明示的なオプトインを行うべきかを理解しています。

地域によるデータ制限

自動化された地域ごとのデータ収集及びデータガバナンスのための Server-to-Serverのストレージは、Tealiumと競合他社を大きく差別化しているポイントです。

「忘れられる権利」のサポート

Tealiumは、マーケティングテクノロジーのエコシステムにデータを供給するというユニークな立場にいるため、全てのマーケティングチャネルを統合してエンドユーザーのオプトアウトを処理するための理想的なポジションといえます。ユーザーが「忘れられること」を選択したとき、Tealiumのサーバーサイドコネクターが APIを通じて「削除」指示を起動します。これが、GDPRの「忘れられる権利」規定をサポートするための第一歩なのです。

4. Tealiumのソリューション

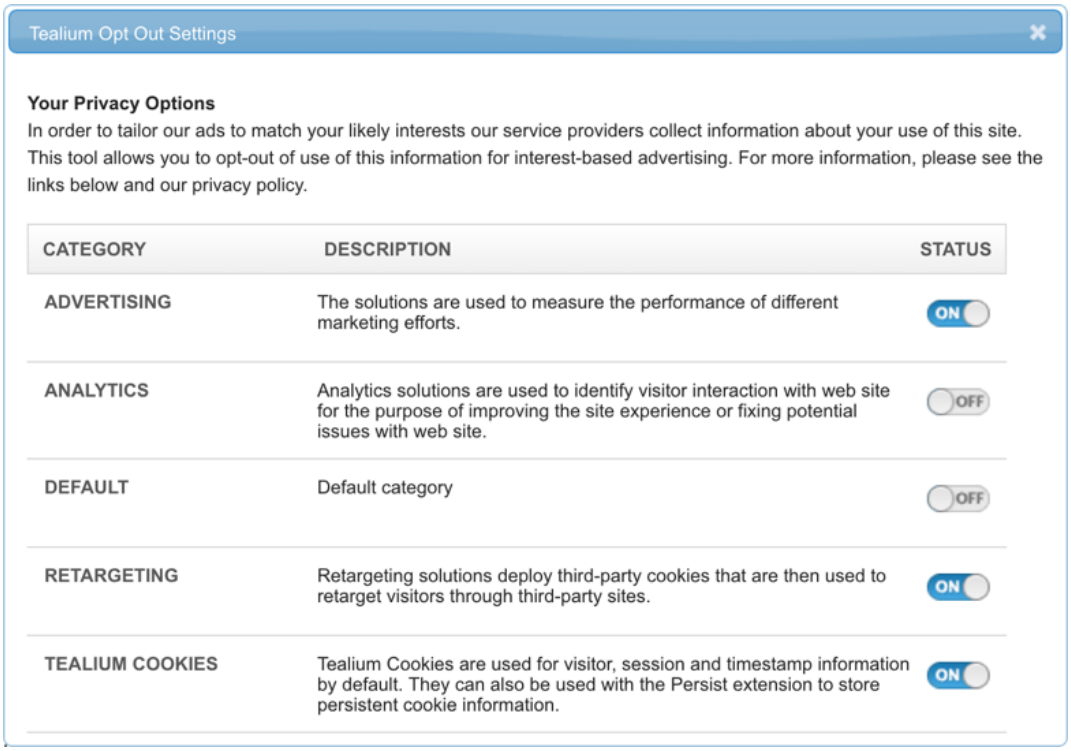
データセキュリティとプライバシーに関する新しい法規制が適用されることは確実です。高度化するセキュリティとプライバシーへの要求を組織がどのように管理していくべきかについて、Tealiumは時代を先取りしてサポートを提供します。データがどのようにして収集されているのか、どこへ転送されているのか、そして誰がそのデータを使うのかをきちんと理解しておくことが、組織にとって益々重要になっています。Tealiumのアプローチにより、お客様はデータをソースレベル(Webサイト、モバイル/IoT及び接続デバイス)でコントロールして管理できます。

Tealiumはお客様のデータガバナンスへの要求に応えるために、Tag Marketplace Policy、リソースロック、バージョン管理、複数の開発環境への配備、個別ユーザー毎のパーミッション設定、ワークフロー管理及びPrivacy Managerなどの強固なプライバシー制御機能及びきめ細かいベンダー管理機能を数多く提供しています。

Tealium iQ Privacy ManagerはData Governance Packageの中核となるコンポーネントで、お客様はオンラインビジターに対して簡単にオプトイン/オプトアウトの選択肢を与えることができ、ビジターはブラウジング中にどのWeb要素についてどのサードパーティベンダーまたはクッキーを許可するかを全て管理することができます。

突き詰めていうと、プライバシーとはエンドユーザーに選択権を与えることであるということができます。TealiumのPrivacy Managerを使えば、個々のタグ毎やタグのカテゴリ毎にオプトイン/アウトを選択できます。

以下にTealium iQ Privacy Managerの主な機能をご紹介します:



データ収集からの除外: 下の画面のように、Tealium iQを使ってWebページで動いている様々なベンダータグを無効化したり、ページにダウンロードされるベンダーコードを停止したりして、エンドユーザーのプライバシー及び「Do Not Track 」設定を尊重します。

カスタマイズ: 以下は、Privacy Manager内で表示や機能設定をカスタマイズする様々な方法を示したものです。

1. クッキーが設定されていないエンドユーザーがページを読み込んだ際に、JavaScriptコードを使って「プライバシー設定を変更」ボタンをクリックすることを求めるのではなく、自動的にPrivacy Managerを表示します。この場合、お客様のご要望に応じてTealiumのデプロイメントチームが実装をお手伝いします。
2. Privacy Managerには、変更可能なレイアウトテンプレートが使われていますので、タグテンプレートと同様にHTMLとCSSを使ってこれを修正することができます。
3. 「デフォルトでオプトアウト」モードでは、エンドユーザーが明示的にカテゴリーやタグをオプトインしない限り、いかなるタグも有効化されません。

まとめ

お客様は、どのようにデータを守っていますか?

Tealium Data Governance Packageを使うことで、お客様は世界中の様々な地域の規制やポリシーに準拠したデータガバナンスとプライバシーコントロールを実現できます。

Tealiumと提携することで、企業がいかにしてデータとプライバシーを保護できるかについての詳しい説明を聞きたい場合は、こちらをクリックしてデモをお申込みください。

データガバナンスパッケージ

Tealiumのデータガバナンスパッケージは、お客様のシステム構成管理をサポートし、お客様のデータガバナンスとプライバシー管理が国および地域のポリシーに確実に準拠できるようお手伝いします。Tealiumは業界のベストプラクティスに従って、Tealium iQ (TMS)、検証、サイトスキャンおよびEventDBの設定およびモニタリングを行います。*

最初の設定 (1回のみ)

- Privacy Managerの設定 (5ドメインまで)
  この設定により、Tealiumが導入されてPrivacy Managerが有効になっているAuthorized Domainへのビジターは、ビジターのWebブラウザに読み込まれるテクノロジータグ (およびそれによるドロッピングクッキー)に従ってオプトインまたはオプトアウトを行うことができます。
- オプトイン告知 (5プロファイルまで)
  Webサイトでクッキーが使われていることをエンドユーザーに知らせるためのバナーと、「明示的」ポリシーによる承認取得のための追加文言をご用意します。
- Tag Marketplace Policyの設定 (5プロファイルまで)
  Tag Marketplace Policyで利用可能なベンダーを、お客様の情報セキュリティチームが承認したベンダーのみに制限し、設定します。
- データレイヤーのエレメントをロックするための暗号化拡張および/またはデータラベルを適切に設定 (5プロファイルまで)
- アクセスを最小限に抑えるベストプラクティスに従い、ユーザーのロールとパーミッションをレビューして設定 (5プロファイルまで)
- タグレポートの収集とデータベースの設定
- 検証用のファネルを設定

持続的提出物 (毎四半期)

- アカウントベストプラクティスのレビューとアップデート
  5つまでのプロファイルについて、Tealium Data Governanceベストプラクティスによる定期的なコンプライアンスチェックを行います。
- データレイヤーの検証
  5つまでのプロファイルについてユーザーファネルを5つまでスキャンし、データレイヤーを適切に設定します。
- ユーザー管理の監査
- その時点でのユーザーアクセスレベルと権利に間違いが無いかレビューします。
- サイトスキャン
  5つまでのアカウントプロファイルについて、タグマネジメントが適正にインストールされているかどうかをスキャンします。TMSインストールが間違っているかインストールされていない場合、およびサードパーティタグがTMSにインストールされていない場合にレポートします。
- 5つまでのプロファイルについてデータレイヤーをレビュー
  自動チェッカーを使ってデータレイヤーをレビューし、REDのアイテムについてエクステンションの設定をサポートします。
- 四半期毎のタグロードレポート
  上記の他、タグのロード状況、タグの基本的パフォーマンス、タグエラーおよびピギーバックタグURLについての警告などをまとめた補足的なレポートを提出します。

* パッケージ内容の詳細は変更されることがあります

データガバナンスチェックリスト

プライバシー/セキュリティと顧客エクスペリエンスをバランスさせるための5つのステップ

2018年5月にGeneral Data Protection Regulation (GDPR)が発効し、すべての組織が新しいガイドラインと手続きを遵守するよう求められます。これまではアカウンタビリティと透明性の原則がデータ保護法の絶対的な要件でしたが、GDPRの法的重視点を理解することは、現代の国境を越えたデジタルエコノミーに係わる組織にとって重要です。

これは同時に、積極的にセキュリティとプライバシーを守り消費者の信頼を得ることで、組織が自社のブランドを差別化する大きなチャンスです。協業するベンダーの選定からポリシーと手順の設定まで、これらの5つの手順を実行することで、お客様の組織を統合し、データガバナンス戦略を一気に進めることができます。

ステップ 1: デューデリジェンス(評価)の実施

誰がどこにアクセスしたかを知るためにデータフローを監査

ビジネスチーム
- ☐ 利用中のベンダーを特定
- ☐ ベンダーのアクセスを検証
- ☐ 現在の契約内容を確認

技術チーム
- ☐ ベンダーテクノロジーを監査
- ☐ ベンダーポリシーをレビュー
- ☐ 不適合な、あるいは使われていないベンダーを排除

ステップ 2: データの棚卸し

どのようなタイプのデータが処理されているか、それは必要かを理解するために棚卸しを実施

ビジネスチーム
- ☐ 法的及び経験的な観点からデータの機密度について合意
- ☐ マーケティングと運用におけるデータの必要性について合意
- ☐ ビジネスのためのデータ要件を文書化

技術チーム
- ☐ データの保存場所を文書化:
  - ☐顧客 ☐キャンペーン ☐企業 (財務・人事)
- ☐ データの取り扱いがビジネスポリシー及び法的要件を満たしていることを確認
- ☐ ベンダー統合についてチェック

ステップ 3: コントロールの構築

データ利用についての明快で正確な通知を出すための手続きを規定 (内部向けにはポリシーとプロセスとともに、外部向けには通知と契約により)

ビジネスチーム
- ☐ ベンダーとの契約が適正かを確認
- ☐ ガバナンスポリシーとプロセスを作成
- ☐ 外部及び内部のコミュニケーションをアップデート

技術チーム
- ☐ 「最小のアクセス」のためにベンダーを構成
- ☐ データ監査ガイドラインとテストを作成
- ☐ コンプライアンスのために内部的なテストと監査を実施

← 組織全体で従業員教育を徹底 →

ステップ 4: データガバナンスチームを設立

ビジネス及び技術チームの活動を後押しするためのチームを結成

ビジネスチーム
技術チームと以下の点についてコミュニケート:
- ☐ マーケティング及び顧客エクスペリエンスをドライブするニーズ
- ☐ コンプライアンス違反時の法的リスク
- ☐ ビジネスから技術への期待

技術チーム
ビジネスチームと以下の点についてコミュニケート:
- ☐ データへのアクセス、転送、保存に関するベストプラクティス
- ☐ データと顧客を「悪者」から守る
  - ☐内部 ☐外部 ☐パートナー
- ☐ 無理のないビジネスイネーブルメント

ステップ 5: 明快で正確な通知を発信

データに関するポリシーを組織内、対顧客、そしてベンダーへ向けて発信することが全員の責任

ビジネスチーム
- ☐ データ利用に反映させるためにプライバシーポリシーをアップデート (例: クッキーポリシー、IPの利用など)
- ☐ 全てのマーケティング活動でオプトアウトの手段を提供
- ☐ データ活用を進めるために技術チームとコミュニケート

技術チーム
- ☐ 顧客に対して明確なオプトイン・アウトを提供
- ☐ 「忘れられる権利」及び一般的なデータ削除の指針を堅持
- ☐ コンプライアンスの変化や非準拠についてビジネスチームとコミュニケート

データプライバシーに、新たな法規制と巨額の罰則が適用されようとしています。
Tealiumは、お客様が適正かつ適法にデータを管理できるようお手伝いする、
お客様ビジネスにおける信頼できるパートナーです。
詳しい情報はtealium.com/jaでご覧下さい。

詳しくは
tealium.com/ja

Tealiumは全世界にオフィスを展開しております。お問い合わせページに電話番号と住所が記載されています。