GDPRコンプライアンス概要

protiviti®
Face the Future with Confidence

欧州連合(EU)における新しい個人データの保護規則

GDPRとは?

EUにおける一般データ保護規則(GDPR)は、1995年のデータ保護指令(DPD)に代わる、2016年4月27日に採択された新しい規制です。GDPRは**2018年5月25日に適用開始**となり、全てのEU加盟国にて直ちに法令として施行されます。この更新された規則は、EUを含む欧州経済領域(EEA)内の所在者(以下「EEA居住者」)が、あらゆるデジタル形式による個人情報をより詳細に管理できるように統一されたルールセットです。この変更の重要な要因は、モバイル機器使用の増加、ビッグデータ分析の採用、そして、グローバルに渡りデジタル生成、処理、共有が行われる個人データ量の増加に伴い、EEA居住者のデータが漏えいするリスクが増加しているということです。

主な懸念事項

GDPRの対象かどうか	• 新しい規則の対象が、企業の物理的所在地に関係なく、EEA内に所在する個人の個人データを収集し取扱う「全て」の組織に拡張されている
なぜGDPRに準拠しなくてはいけないのか	• 違反時の制裁金:**2000万ユーロ**または**年間のグローバルの売上高の4パーセント**(いずれか高額な方)
社内のデータ状況を把握しているか	• GDPRでは、収集される個人データに対するより高い認識と、それらのデータの生成、取扱い、保存に関するアカウンタビリティについて、組織が持つべき必要性が強化されている • 組織はどのベンダーがデータをどのように扱っているかをしっかりと理解しなければならない
施行された場合、データ主体の権利を守ることができるか	• GDPRは、個人データを扱う組織に対して強制力のある、プライバシーの権利一式をデータ主体に与えている。これらの権利は、個人データを法的に取扱う組織の能力を制限し、組織のビジネスモデルに重大な影響を与えるかもしれない

GDPR における「個人データ」とは

GDPRは「個人データ」を、識別子への参照による特定できるものも含め、
直接的又は間接的に特定の個人(「データ主体」という)を識別できるあらゆる情報と定義している。
**企業が認識すべき新しい対象として、名前や住所といった公開情報や
MACアドレスやクッキーといった一般的な技術データが含まれる**

GDPRにおける個人データの例

- 名前
- 住所
- 電話番号
- Eメールアドレス
- パスポート番号
- 財務情報
- 誕生日
- 医療情報
- 生体データ
- 社員番号
- IPアドレス(固定/動的)
- Macアドレス
- Cookie
- GPSデータ
- 金融・銀行口座情報

© 2017 Protiviti Inc. All rights reserved. 複写禁、転載禁

GDPRコンプライアンス概要

protiviti®
Face the Future with Confidence

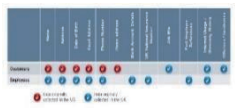
欧州連合(EU)における新しい個人データの保護規則

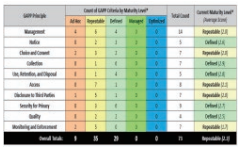
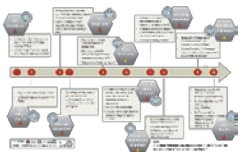
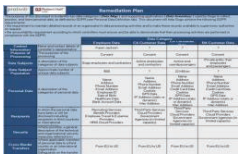
主なGDPR要求事項

侵害時の通知	個人データの侵害発生を管轄監督機関へ**72時間**以内に、また可能性のあるデータ主体へ報告する義務
プライバシーのバイデザイン及びバイデフォルト	企業は、新しいプロジェクトの開始時にプライバシーを考慮し、全ての開発工程を通して適切なセキュリティ統制を実装しなければならない
データ主体の権利	新たな権利として、忘れられる権利、データポータビリティーの権利、プロファイリングを含む異議を唱える権利が含まれる
同意	曖昧でない同意を取得する義務(例:明確な同意)
データ保護オフィサー(DPO)	「公的機関・団体」や、特別な種類の個人データの監視や取り扱いを大規模に行う組織にはDPOが必要とされる

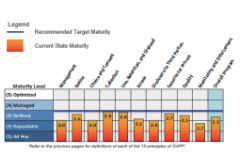
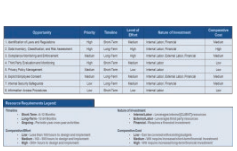
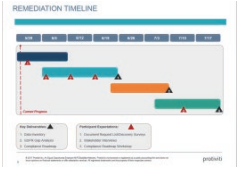
プロティビティの支援内容

Discovery & Planning 0	Current State 1	GDPR Gap Analysis 2	Compliance Roadmap 3	Gap Remediation 4
GDPR対象データソースの重要度テンプレートによる棚卸	現状分析	GDPRギャップ分析結果	準拠計画ロードマップ及び補足レポート	改善及び実装支援





© 2017 Protiviti Inc. All rights reserved. 複写禁、転載禁