EMMが GDPRコンプライアンスに貢献

世界の多くの地域で、合理的で常識に基づくセキュリティ規格が法律化されつつあります。ヨーロッパでは、一般データ保護規則（GDPR）が2016年4月に制定され、2018年5月25日に施行されます。GDPRは、欧州連合（EU）全体でデータ保護とプライバシーに対応する1つの包括的かつ協調的な法制度です。GDPR違反は、多額の罰金と信用低下をもたらします。罰金の最高額は、2,000万ユーロまたは企業の世界売上高の4%のいずれか高いほうとなります。

GDPRは、EU内の管理者/処理者に加え、EU在住者の個人情報を処理するEU外の管理者/処理者に適用されます。「管理者」とは、個人データを処理する目的と手段を決定する組織と定義されます。「処理者」とは、管理者の代理として、管理者の指示

MobileIron

japan@mobileiron.com
www.mobileiron.com
Tel: +81.03.6426.5301
Fax: +81.03.6426.5302

「EMMはGDPRへの適合に必須です。」

IDC（2017年2月）*

に従い、処理を実行する組織と定義されます。本書の目的では、管理者と処理者を同じ組織、すなわち従業員または顧客をEU内に持つ企業と想定します。

包括的で構造の整ったエンタープライズモビリティ管理（EMM）プログラムは、企業のGDPRコンプライアンスにおいて重要な役割を果たすと期待されます。本書では、企業が自社のモバイルプライバシー/セキュリティポリシーと実行モデルを積極的に評価するためのフレームワークを提案します。本書は法律的な指導書ではありません。自社のEMM体制が社内の法務/コンプライアンスフレームワークに適切に対応しているか、各社でご確認ください。

GDPRにおける個人データ処理の原則は、標準規格に基づき、他の地域の新しいプライバシーフレームワークにも適合しています。

GDPRの原則

従業員は全員が何らかの個人データを保持しています。GDPRコンプライアンスの基本的な出発点は、保持する個人データを必要最小限に抑え、個人のリスクを軽減するよう妥当な予防措置を取ることです。

ヨーロッパは世界で最もデータプライバシーに力を入れていますが、GDPRにおける個人データ処理の原則は、標準規格に基づき、他の地域の新しいプライバシーフレームワークにも適合しています。この原則には以下が含まれます。

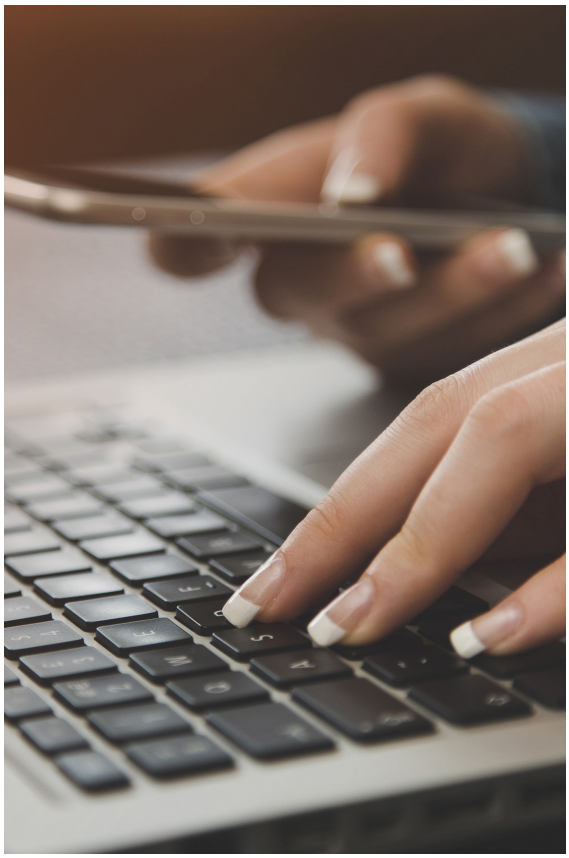
- **合法的、公正、プロセスの透明性：**企業は、個人情報処理の有効な基盤を持ち、個人にその情報を提供する必要があります。
- **目的の限定：**個人データを処理する明確で曖昧さのない理由が必要です。データは、収集した目的でのみ処理することが許されます。
- **同意：**処理される個人データの持ち主は、通常、同意を提供する必要があります。
- **データの最小化：**処理されるデータは、具体的な目的だけに厳しく限定する必要があります。アクセスは、その目的のために必要とする人間にのみ付与します。
- **正確性：**データは正確でなければなりません。不正確な点は直ちに修正する必要があります。個人はそのような修正を要求する権利を有します。

* "Market Analysis Perspective: Western Europe Enterprise Mobility, 2017（市場分析の視点：2017年 西ヨーロッパの企業モビリティ）"、IDC Europe、2017年2月。

- **保存の限定：**データは、指定された目的に必要な期間だけ保持します。
- **完全性と機密性：**データは、無許可での処理や意図しない紛失からの保護を含め、データの適切なセキュリティを確保する方法で処理する必要があります。
- **アカウンタビリティ：**企業は、上記の原則に対するコンプライアンスや改善を実証する必要があります。

企業は、適切なセキュリティ対策があり、コンプライアンスを適切に監視していることを証明する必要があります。

プライバシーは後からでは間に合いません。



プライバシー・バイ・デザイン/バイ・デフォルト ー GDPR第25条

プライバシーは後からでは間に合いません。GDPR第25条は「データ保護バイデザイン/バイデフォルト」（プライバシーバイデザイン/バイデフォルトとも呼ばれる）の概念を定義しています。

プライバシー・バイ・デザイン：企業は、処理やシステムの初めのデザインからサービス終了とデータ削除まで、業務のライフサイクル全体にわたってプライバシーを保護する必要があります。

プライバシー・バイ・デフォルト：企業は、必要な量の個人データだけを収集し、処理することをデフォルトとする必要があります。他の情報を提供しないことをユーザーが選択する必要があってはなりません。企業が、「万が一」後で利用するかもしれないという理由で情報を収集することはできません。

最先端 ー GDPR第32条

GDPRの第32条は、情報ガバナンスをサポートする上で、最新かつ最高の技術を利用することの重要性を概説しています。

*「**最先端**を考慮し……管理者と処理者は、リスクに適切に対応するセキュリティレベルを確保するため、適切な技術的および組織的対策を講じるものとする。」*

GDPRは具体的な技術を規定してはいませんが、第32条には、暗号化、完全性、可用性、テストが対策の例として挙げられ、企業が最先端のソリューションを評価すべきであると記載されています。

GDPRに対応する EMMフレームワークの確立

MobileIronのようなEMMソリューションは、GDPRの要件を満たすセキュリティプログラムの重要な要素です。EMMを有効に活用しない企業は、なぜ最先端の技術的対策を採用して情報漏洩のリスクを緩和しなかったのか、管轄当局に正当な理由を述べるのに苦労するかもしれません。

EMMを有効に活用しない企業は、なぜ最先端の技術的対策を採用しなかったのか、管轄当局に正当な理由を述べるのに苦労するかもしれません。

GDPRに対応するEMMフレームワークには、以下のMobileIronの機能が必要です。

1. MobileIronプラットフォームは、デバイスの暗号化設定を監視し、ビジネス用のアプリやデータには二次的な暗号化機能を提供することにより、デバイス上での**データ暗号化を強制**できます。

2. MobileIronプラットフォームにより、企業はデバイス上で**個人データとビジネスデータの明確な境界を確立**できます。企業は、個人用アプリや個人用メールアカウントのコンテンツにアクセスできません。また各企業は、アプリインベントリやデバイス位置情報など、他の種類の個人データへのアクセスがセキュリティまたは業務上の目的に適切かどうか審査する必要があります。適切である場合は、その目的を明確に文章化および伝達し、プライバシーバイデフォルトと同意の適切な対策を事前に設ける必要があります。

3. MobileIronプラットフォームにより、企業は**ビジネスサービスへの信頼できるアクセスを強制できます。** MobileIron Accessでは、企業が、どのモバイルデバイスとアプリがバックエンドサービスに接続しようとしているかを可視化できます。このため不正なアクセスはブロック可能です。MobileIron Sentryはデータトラフィックを保護し、必要であれば、さらなるセキュリティ/検査ゲートウェイに通すことができます。

4. MobileIronプラットフォームにより、企業は**監査ログを使用**して、どんなアクションがデータ侵害につながったか、その後にどんなアクションがあったかを判断できます。GDPRの強制通知期間は72時間しかない場合もあり、迅速な対応が必要です。

5. MobileIronプラットフォームにより、企業は**情報漏洩防止（DLP）対策を実行できます。**たとえば、紛失したデバイスから機密データをリモートワイプする、デバイス上のビジネスアプリが無許可のアプリとデータを共有できないようにするなどです。脱獄やルート化を目的としてモバイルオペレーティングシステムの完全性を損なう攻撃も特定できます。コンプライアンス上の問題があった場合は、MobileIronプラットフォームを通じて通知、検疫、データワイプなど適切な是正措置を実行します。

非マネージドデバイスは多層防御戦略をサポートできません。

GDPRに対応するEMMの導入

GDPRの影響を受ける企業はすべて、導入済みのEMMと構成モデルを査定すべきです。この査定により、まず、GDPRコンプライアンスにおいて十分に活用されていない点が明確となります。次に、継続的な監視と是正を計画し、実施するための基盤ができます。

以下に、GDPR対応のセキュリティプログラムの一環としてEMMを導入する手順を紹介します。

1. ビジネスデータにアクセスするすべてのモバイルデバイスを管理下におきます。非マネージドデバイスは、紛失したり侵害を受けたりしたデバイスに妥当なレベルのデータセキュリティ対策を実行する多層防御戦略をサポートできません。
2. 最新の構成プロファイルを適用します。パスワード、暗号化、デバイスセキュリティ、接続、重要なビジネスイネーブルメント機能に関するポリシーを実行します。
3. すべてのビジネスアプリをマネージドアプリとして企業向けアプリストア経由で配布し、企業が管理するセキュリティフレームワーク内で動作するようにします。
4. 適切な情報漏洩防止（DLP）ポリシーを実行し、デバイス上のアプリデータを保護します。
5. すべてのビジネスサービスについて信頼できるアクセスを強制します。無許可、非マネージド、コンプライアンス違反のデバイス、アプリ、ユーザーからのアクセスはブロックします。企業が管理も可視化もできないデバイスへの機密データ保存を許可してはなりません。
6. プライバシー/セキュリティポリシーを確立し、定期的に従業員に明確に伝えます。
7. 適切なインベントリ、利用状況、監査ログを収集し、侵害への迅速な反応をサポートします。

最後に

企業が個人データ向けに適切なセキュリティを提供するには、適切なEMM管理と手続きを導入していることを実証する必要があります。これらは、ビジネスに必要な個人データを外部の脅威や不正利用/開示から確実に保護します。MobileIronプラットフォームは、データの最小化、完全性、機密性、そしてGDPRのアカウンタビリティ原則により、安定したコンプライアンスフレームワークを提供します。