NIST プライバシーフレームワークの導入:
中小企業向けクイック ガイド

「プライバシープログラムを構築することは難しいですが、NIST プライバシーフレームワークは、大規模なプライバシー チームを編成できない場合でも使用できるツールの 1 つです。」
- アーリントン郡政府最高データ責任者、ジェイミー・リース

NIST プライバシーフレームワークとは何ですか? また、組織ではそれをどのように使用できますか?

NIST プライバシーフレームワーク は、組織がプライバシープログラムを作成または改善するのに役立つ任意のツールです。効果的なプライバシーリスク管理は、製品やサービスに対する信頼を構築し、プライバシー慣行についてより適切に伝え、コンプライアンス義務を満たすのに役立ちます。優れたサイバーセキュリティは重要ですが、すべてのプライバシーリスクに対処することはできません。

「準備、設定、実行」のフェーズのシンプルなモデルに従ってプライバシーフレームワークの使用を開始し、ビジネスまたは代理店を次の 5 つのプライバシーリスク管理領域に合わせてください: 識別、統治、制御、コミュニケーション、保護。

準備...

プライバシーフレームワークを使用してプライバシーリスクを特定および管理のための強固な基盤を築く準備を整え、プライバシープログラムを作成または改善を行いましょう。

識別：

- 処理しているデータ（収集、使用、共有、保管など）を特定し、収集から廃棄までのデータライフサイクル全体を通じてシステム内のデータの流れをマッピングします。初めは完全である必要はありませんが、プライバシーのリスクを理解するための基礎となります。
- データマップを使用して プライバシーリスク評価 を実施し、データ処理活動が個人にどのような問題 (恥ずかしさ、差別、経済的損失など) を引き起こす可能性があるかを評価します。その後、これらの問題が発生した場合の組織への影響（顧客信頼の喪失や評判の損害）が、どのように業績に悪影響を及ぼかを評価します。
- 契約のオプションや、ビジネスを運営するために使用する製品やサービスについて問い合わせて、プライバシーの優先事項を反映するように設定されていることを確認します。

契約{133ND23PNB770271}に基づきTaikaTranslations LLCはNISTの依頼のもと翻訳。

統治:

- プライバシー文化は上層部から始まります。組織が重点を置くプライバシーの価値 (たとえば、人間の自律性、匿名性、尊厳、透明性、データ制御など) を決定します。組織のプライバシーの価値とポリシーをプライバシーリスク評価と結び付けて、製品とサービスに対する信頼を高めます。
- プライバシー関連の法的義務を理解して、準拠した製品やサービスを構築できるようにします。
- 従業員が自分の役割と責任を理解できるように支援し、製品やサービスの設計と展開におけるプライバシーリスクを効果的に管理する方法について、より適切な判断ができるようにします。
- プライバシーリスクが変化したかどうかを定期的に再評価してください。これは、製品やサービスを改善したり、データ処理を変更したり、新しい法的義務を知ったりしたときに発生する可能性があります。

「プライバシーフレームワークは、組織がビジネスを成長させるための市場差別化要因となり得ます。
- メアリー・N・チェイニー、弁護士、CISSP、CIPP、情報セキュリティおよびプライバシー部長、ESPERION Therapeutics, Inc.

セット…

プライバシーリスクと法的義務を把握し、ガバナンス構造を構築したので、組織はシステム、製品、サービスに対するポリシーと技術的能力に集中できます。

制御：

- 必要のないデータを収集、共有、または保持していませんか? ポリシーが、自分や他の組織がデータに対する制御を維持するのにどのように役立つか、また個人がどのような役割を果たす可能性があるかを検討してください。
- データ処理システム、製品、またはサービスの機能を決定する際には、プライバシーのリスクと法的義務を考慮してください。変化する顧客のプライバシー設定や動的な法環境によりコスト効率よく対応できるよう、柔軟な設計を検討してください。
- どのようなデータ処理を行っていますか? データを個人やデバイスから切り離すことができればできるほど、プライバシーの保護は強化されます。非識別化、分散型データ処理、その他の技術的手段が、プライバシーを保護しながらビジネスまたは機関の目的をどのように達成できるかを検討してください。

コミュニケート：

- データ処理活動について内部および外部でのコミュニケーションに関するポリシーを策定してください。
- 明確でアクセスしやすい通知やレポートを提供したり、アラート、ナッジ、その他のシグナルを実装してデータ処理活動やその選択肢について個人に通知したりすることで、透明性と顧客の理解を高めます。
- 製品やサービスの設計に役立つアンケートやフォーカスグループを実施していますか? プライバシーを含めることで、顧客のプライバシーの好みについてより多く学ぶようにしてください。
- データ侵害が発生した場合にどうするかを検討してください。通知や、信用監視や凍結などの救済措置はどのように提供しますか?

保護：

- ネットワークにログオンしてコンピューターやその他のデバイスを使用するユーザーを制御します。
- データを保護するためにセキュリティソフトウェアを使用します。
- 保存中および転送中の機密データを暗号化します。
- 定期的にデータのバックアップを実行します。
- セキュリティソフトウェアを定期的に更新し、可能であれば更新を自動化します。
- データと古いデバイスを安全に廃棄するための正式なポリシーを用意します。

「プライバシープログラムを確立する必要がある場合、NIST プライバシーフレームワークは最適な出発点です。」
- ジェウォン・セラト, パートナー, ベーカー・ホステットラー

開始！

今、あなたが今日いる場所から、目指すべき場所へ進む時です。

- あなたのプログラムは、ここで提案したものと比べてどうですか?
- 目標とする成果を優先し、行動計画を作成してください。
- 組織として計画について話し合い、それを活用して、目標を達成するために必要なリソースの獲得と人材の育成に取り組んでください。
- 計画を実行に移しましょう!製品やサービスへの信頼を高め、パートナーや顧客とプライバシーについてより効果的にコミュニケーションを取り、コンプライアンス義務を満たすための道を歩み始めています！