TOPCERTIFIER
www.topcertifier.com

サービス方法論
GDPR
一般的なデータ保護 規制

TOPCERTIFIER
www.topcertifier.com

はじめに GDPR

GDPR 要件は欧州連合の各加盟国に適用され、より多くの要件を実現することを目指しています。EU諸国全体で消費者データと個人データを一貫して保護します。鍵の一部
プライバシーとデータ保護の要件 GDPR 含む：

- データ処理のために被験者の同意を必要とする
- 収集されたデータを匿名化してプライバシーを保護する
- データ侵害通知の提供
- 国境を越えたデータ転送を安全に処理する
- 特定の企業にGDPR準拠を監督するデータ保護責任者の任命を義務付ける

GDPR は、EU 国民のデータを扱うすべての企業に規制要件を義務付けています。国民の個人データの処理と移動をより適切に保護する.

キックオフ

キックオフ ミーティングは、プロジェクトの実行に向けたコミュニケーションと計画を立てるための重要なツールです 障害を最小限に抑え、計画された時間とコスト内でプロジェクトを完了します。キックオフミーティングの議題は、:

- プロジェクト計画のディスカッション: これには、責任と責任に関するディスカッションが含まれます。 利害関係者。プロジェクトのマイルストーンと成果物
- サービスの範囲
- 法的および規制上の要件

コアチームの創設

- データ保護責任者 (DPO) の任命
- 社内 GDPR / GRC 委員会 (ガバナンス リスクおよびコンプライアンス) の任命 (* 必要な場合)

GDPR 意識向上トレーニング

GDPR あなたの組織の従業員に対して意識向上トレーニングが実施されます。トレーニング
このセッションは、従業員が知識を獲得し、GDPR の概念を理解し、調整できるようにすることを目的としています。 達成と確立、実装、維持、および達成に向けたプロセスと実践
コンプライアンスに基づいたシステム作業環境を継続的に改善します。スタッフがいるとき
訓練された彼らは、目標の達成に向けて考え、行動し、貢献することができます。

TOPCERTIFIER
www.topcertifier.com

GDPR - 段階的な実装

フェーズ **I -** ギャップ分析
このフェーズでは、ギャップ分析を実施して、現在の実践がどの程度適切であるかを確認します。要件に沿って。あなたの現在の実践は以下の 2 つに対して検証されます
参照基準、
▪ GDPRの要件
▪ 法律、規制、法定の要件 この分析の結果は、ギャップ分析レポートの形式で表示されます。この報告書 プロジェクトを思い出させるためのアクションアイテムのリストとして機能します

フェーズ **II -** 情報フローの評価
この段階では、情報源の特定と処理を支援します。人材、技術、物理的インフラを含むインフラストラクチャ GDPR

フェーズ **III -** データ プライバシー影響評価 **(DPIA)**
データ保護影響評価 (DPIA) は、潜在的なプライバシー問題と リスクはすべてのステークホルダーの観点から特定され、検討されます。これにより、組織は、新たな取り組みによって起こり得る影響を、具体的な方法で予測し、対処する必要があります。リスクを最小限に抑える/軽減するための措置。DPIA は、危害のリスクを最小限に抑えるように設計されています。
データ保護と対策に取り組むことで、個人情報の使用/悪用が原因で発生する可能性があります。プロジェクトの設計および開発段階におけるプライバシーの懸念

私たちは、部門と連携して、DPIA 手順と DPIA 登録の開発を支援します。リスクを管理し、損害を回避することで組織に利益をもたらすように努めます。評判を高め、法的義務を確実に遵守し、ステークホルダーとの関係を改善します。

フェーズ **IV -** 安全な個人データ転送分析
どのような個人データが社外に転送されているかの分析を支援します。また、適切に保護するために必要なセキュリティ対策の設計も支援します。個人データおよび社外に転送される個人データ

フェーズ **V -** データ侵害インシデントのプロセスの設定
当社は、個人データ侵害を特定して対処するためのプロセスの設定を支援します。(例:データ違反通知手順)、またインシデント報告に関する手順の作成も支援します。
関係監督当局へのメカニズム

フェーズ **VI -** 文書化サポート
私たちは、個人を保護するために必要な組織的および技術的措置の実施を支援します。
データ主体の個人データを収集し、関連文書の設計支援にも役立ちます。GDPR が適切に組み込まれていることを保証する管理ポリシーと手順を備えています。組織プロセス

TOPCERTIFIER
www.topcertifier.com

データ保護責任者 内部監査研修

GDPR 内部監査人 (IA) トレーニングが DPO に提供されます。このトレーニングでは、次のような能力を身につけます。IAの必要性を分析し、IAを計画およびスケジュールし、監査チェックリストを作成し、監査を実施する担当者 IAを作成し、観察結果を文書化して経営トップに報告する

GDPR 内部監査

当社の専門家が、DPO による内部監査の実施を監督します。 この内部監査は、システム内にまだ存在するギャップを特定し、問題に直面する準備のレベルを実証する コンプライアンス監査。 この監査により、組織はすべての不適切な問題を特定し、修正する機会が得られます。コンプライアンス監査に進む前に、適合性を確認してください。 経営トップに通知される 内部監査の結果。

GDPR - 根本原因の分析 (RCA) と是正措置

内部監査、クライアントまたは第三者の監査中に特定されたすべての不適合、または
リスク登録、DPIA 登録、インシデント ログ、データ バックアップ ログ、データ侵害通知レポート、脆弱性評価および侵入テスト (VAPT)、データ保持ログ、およびその他のソース 列挙する必要があります。RCA は、ブレインストーミングやフィッシュボーン手法などの手法を使用して実行されます。最適な修正と是正措置が実施され、その有効性が確認されます。
措置は GDPR 是正措置報告書 (CAR) を通じて文書化され、レビューされます。

当社の専門家が貴社のチームに同行し、プロセスをガイドします。

TOPCERTIFIER
www.topcertifier.com

GDPR管理のレビュー ミーティング (MRM)

MRM は、すべての関係者が予定された間隔で集まり、レビューや議論を行う機会です。
以下の議題についての行動を計画します。

- DPIA レポート
- コンプライアンス面での逸脱
- 納品後の活動報告
- 未解決の項目を解決するための行動計画
- システムに必要な改善と変更の機会

GDPR コンプライアンス監査

準備レベルが適切なレベルに達すると、コンプライアンスのプロセスが開始されます。
認証が始まります。認証機関 (CB) の任命された監査人が準備状況を検証します。外部監査を通じて。 これには、監査人がポリシー、プロセス、SOP、重要な事項をレビューすることが含まれます。
運用記録、IA および MRM 記録。 CB の期待からの大きな逸脱 この時点で必要な修正を行うよう通知されます。これにより、次の可能性が減少します。 認証審査中の重大な不適合。
TOPCertifier はすべてのユーザーと連携します。 利害関係者と連携し、監査が円滑に完了するよう監督します。

コンプライアンスの継続

TOPCertifier は、組織のコンプライアンスへの取り組みの一部となり、定期的なコンプライアンスの遵守を支援します。 必要なトレーニング、システムサポートと蛹化、内部および外部監査の間隔
コンプライアンス認定の定期的な更新。