EU 一般データ保護規則（EU GDPR）

ISO/IEC 27001 認証取得はどのような意味があるか？

BSI は、新たな EU 一般データ保護規則（EU GDPR）が、組織のビジネスアジェンダにおいて非常に高い優先順位であることを認識しています。組織にとって ISO/IEC 27001 情報セキュリティマネジメントシステム（ISMS）を維持するためには、この新たな法的要求事項を考慮し、適切に対応していることを示す必要があります。しかし、すでに堅牢な情報セキュリティシステムを導入している組織にとって、GDPR はどのような対応が必要になってくるのでしょうか。

EU GDPR とは何か？

EU 一般データ保護規則（EU GDPR）は、2018 年 5 月 25 日から施行される個人情報の処理と移転に関するルールを定めた新たな法令です。欧州単一市場におけるデータ保護法の調和を図り、個人データの管理を個人に戻すことを意味します。それは、国際的なビジネスを改善し、個人に対し個人情報が保護されていることを再び保証していることを意味します。

どのような組織が影響を受けるのか？

- 個人データのコントローラ（管理者）とプロセッサ（処理者）の両方
- すべての EU 加盟国、EU 市場内で活動し、欧州のデータ科目に関する情報を持つ組織

何に集中する必要があるか？

ISO/IEC 27001 の適用によって、すでに多くの要求事項が満たされているはずですが、本フライヤーでは EU GDPR の要求事項を満たすためのレビュー箇所をいくつかご説明します。

リスクアセスメント

新たな規則で施行される罰金（最大 2,000 万ユーロ、または全世界売上高の最大 4%のいずれか高い方）は、組織に多大な財政的影響を与える可能性があります。これは、組織が保有する個人情報に大きなリスクを与えます。

コンプライアンス

新たな法令は 2018 年 5 月 25 日から施行されるため、義務を再検討する必要があります。 ISO/IEC 27001 の管理策 A.18.1.1（適用法令及び契約上の要求事項の特定）では、関連する全ての法令、規制及び契約上の要求事項のリストが必要です。

データ分類

個人データは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。ISO/IEC 27001 の管理策 A.8.2（情報分類）で、組織に対する情報の重要性に応じて、情報の適切なレベルでの保護を確実にします。

違反通知の報告

企業は、個人データの侵害が発見されてから 72 時間以内にデータ当局に通知する必要があります。
ISO/IEC 27001 の管理策 A.16（情報セキュリティインシデント管理）では、適切な管理者への連絡経路を通してできるだけ速やかに報告を行うインシデント管理プロセスが要求されます。

bsi.

...making excellence a habit.™

当局との協力

EU GDPR の下では、組織はプライバシーまたはデータ保護の規制当局と協力しなければなりません。ISO/IEC 27001 の管理策 A 6.1.3 に、「関係当局との適切な連絡体制を維持しなければならない」と規定しています。

資産の管理

EU GDPR では、収集する個人情報、入手方法、保管場所、保管期間、アクセス権などを理解する必要があります。ISO/IEC 27001 の管理策 A.8（資産の管理）は個人データを含む「情報資産」に関するものです。目的は、組織の資産を特定し、適切な保護責任を定めることです。資産目録を作成し、資産の管理責任者、資産利用の許容範囲、資産の撤退方法を理解する必要があります。

デザインによるプライバシー

デザインによるプライバシーの採用は、別の EU GDPR 要求事項です。ISO/IEC 27001 の管理策 A.14（システムの取得、開発及び保守）は、情報セキュリティが情報システムの開発とライフサイクル全体の不可欠な部分として設計され実行されることを保証します。

外部委託先の関係

EU GDPR は、他者に代わって個人データを処理する外部委託先に適用されます。正式な契約に管理策と制限事項を含める必要があります。これは、ISP、CSP、及びアウトソーシングされたデータセンターに適用されます。ISO / IEC 27001 の管理策 A.15.1（供給者関係における情報セキュリティ）は、外部委託先がアクセス可能な組織の資産の保護を要求しており、A.15.2（供給者のサービス提供の管理）は、組織が情報セキュリティ要求事項に対する外部委託先のサービス提供を監視する必要があると述べています。

ドキュメンテーション

EU GDPR 下では、コントローラ（管理者）はプライバシーに関する文書を維持しなければなりません。個人情報が収集され、処理される目的、データ科目及び個人データの「カテゴリ」に分類されます。ISO/IEC 27001 の箇条 7.5（文書化した情報）では、プロセスとその相互作用の複雑さに基づいて文書を保管することを要求しています。

ISO/IEC 27001 を超えて考慮しなければならないことは何か？

ISO/IEC 27001 は EU GDPR の要求事項の多くをサポートしていますが、下記も考慮に入れる必要があります。

- **トレーニングと意識** – ビジネスリーダー及び主要なステークホルダーがこの法令の変更を認識していることを確認してください。潜在的な影響の理解を得る必要があり、さらに詳細なトレーニングの必要があるかも知れません。
- **データ保護責任者（DPO）の任命** – 大規模な個人データの監視や特別なカテゴリのデータ処理などの特定の活動では、組織に DPO を任命する必要があります。必要がなくても、情報セキュリティの知識とデータ保護法の知識を備えた DPO を任命することをお勧めします。
- **内部監査** – 内部監査を使用して、保持している個人データ、その出所、及び誰と共有しているかを評価します。
- **手順の見直し** – 組織の手順が個人の権利をすべてカバーするようにします。これには、個人情報が正確であり、収集された目的で使用され、必要以上に長く保管されないようにする方法と、要求された場合に個人データを提供または削除する方法を含みます。
- **インシデント管理プロセスの確認** – 個人情報の問題が発生した際に、新たな規則で要求される厳しいタイムスケールで対応できることを確認します。
- **導入済みマネジメントシステムのレビュー** – ISMS の適用範囲と実装した管理策によっては、BS 10012 や ISO/IEC 27018 などの追加のガイダンスが役立つ場合があります。
  BS 10012 は、個人情報マネジメントシステムの要件を概説しています。最近、EU GDPR 要求事項に合わせて更新がされました。これを裏付け文書、または追加の管理システムと見なしても構いません。また、パブリッククラウドで情報を処理したり保存する場合は、ISO/IEC 27018 が役立ちます。既存の ISO/IEC 27001 システムをベースにして、個人を特定できる情報を保護するための特定の管理策を設置します。

最新情報は下記Websiteをご覧ください。
www.bsigroup.com/ja-JP/

bsi.