protiviti®

GDPR 準拠対応における確認事項のガイダンス – 質問集と解説

April 19, 2017

一般データ保護規則（GDPR）が示すものは、過去 20 年における個人情報保護におけるおそらくもっとも大きな変化であろう。88 頁で構成される GDPR 文書は、個人データを取扱うための正当な根拠を示す義務、データセキュリティに対する義務、そして、個人データにより誰が何をできるかを厳密に説明する義務を含む、一連の実施領域を示している。期限である 2018 年 5 月 25 日が迫りつつあることと、違反に対する 2000 万ユーロまたは年間のグローバルの売上高の 4 パーセントという制裁金の可能性により、効果的なデータ保護プログラムの重要性はこれまでになく高まっている。ロバートハーフのリーガルサービスとプロティビティは、本書にて今後の道筋を示すものである。

いくつかの GDPR に関する一般的な誤解：

- [GDPR は EU を拠点とする事業のみが対象である] GDPR は、EU を含む欧州経済領域（EEA）内の所在者の個人データを取扱うすべての組織にグローバルで適用される。
- [プライバシー・シールドと GDPR は同じものである] GDPR が個人データの保護におけるほぼすべての面に対応するのに対し、プライバシー・シールドは EU からアメリカへの個人データの移転を促進するために設計された、データ移転の方法である。たとえ、個人データが EU に留まる場合においても、GDPR は変わらず適用されることになる。
- [すべてのデータは暗号化が求められる] GDPR の第 32 条にて、暗号化、仮名化といった、個人データの保護方法が提言されているが、特定の方法が要求されているわけではない。最終的には、何が最も適しているのか組織が決定することになる。**GDPR のその他の解釈については、ゆくゆくは第 29 条作業部会が更なるガイダンスを提供することになる。**

以下、GDPR 準拠に向けた改善対応準備にあたり、全ての組織が確認すべき一連の質問が列挙されている。決して網羅的ではないものの、グローバルデータ保護プログラムの多くに関連するコンポーネントの概要として機能するものである。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
データ保護に関する必要な支援を受けているか？ ☐ データ保護の運営委員会またはデータ保護を担うであろう関連の委員会があるか？ ☐ 委員会の後ろ盾となる経営層がいるか？		組織全体にデータ保護を広める機能を持つ委員会や、委員会の後ろ盾となる経営層の関与がない場合、データ保護プロジェクト及びプログラムが失敗する可能性が高くなる。	委員会規程の策定、主管となるべき部署、事業単位の特定、委員会のキックオフ及びアジェンダの作成を支援します。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
自身が GDPR の対象となるかどうか？ EU のデータ主体の個人データ（または特別な個人データ）を取り扱うか？ EU データ主体に関する「行動の監視」を行っているか？	Rec. 24; 第 3, 4 条	個人データの取扱いとして見なされる可能性がある作業の例：取得、記録、編集、構造化、保存、修正又は変更、復旧、参照、利用、移転による開示、周知又はその他周知を可能な ものにすること、整列又は結合、制限、消去又は破壊。 「監視」とは、誰かが Web サイトをクリックした場所を監視するなどの単純なものを超えるものであると定義される可能性がある一方で、どの程度にまで定義されることになるかは現時点では不明である。実際問題として、もしユーザー解析に関係しているのなら、自身が GDPR の対象になると仮定するのが良策である。	プロセス・内容領域専門家、ビジネスオーナー、IT、関係者へのインタビューにより、組織内で行われている取扱いの対象範囲を特定し、これまで知られていなかった取扱いを明らかにすることができます。
個人データの収集、利用、共有、廃棄を管理するための規程、手続、通知はあるか？		プライバシーポリシーとプライバシーに関する通知は、異なる二つの文書である。ポリシーは違反が懲戒の対象となる個人データに関する広範な行動基準を定め、通知は特定の情報をデータ主体に伝えるものである。 次に該当する方針や関連する手続・通知も含まれる。： • プライバシー • 利用規程 • BYOD • データ分類	GDPR 及びそれ以外の組織が準拠すべき規則やその他の義務に沿ったポリシーや関連文書の策定を支援します。当社の幅広い領域の方針や様々な業種にわたる関連文書策定の経験を基に、準拠すべき環境に対して適切な文書の策定を提供します。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
各々の個人データの取扱いごとに、適法性の根拠があるか？	第 6,9 条	従業員に対しては、同意は典型的な最も悪い選択である。同意はいつでも取消すことができ、もしそれが取扱いの根拠なのであれば、取消しの通知を受け取り承認する仕組みが必要である。	取扱いの詳細を分析し、テーマに対してデータ保護機関や業界の有識者が述べた見解を共有することができます。
データ保護オフィサー(DPO)の任命が要求されているか？ ☐ データ主体の定期的かつ体系的な監視を大規模に行う取扱いがあるか？ ☐ 第 9 条の対策として特別な種類の個人データを大規模に処理する取扱いが含まれているか 該当しない場合、誰が主にデータ保護と経営層への報告について責任を持っているか？	第 37-39 条	DPO は必須ではないとしても、データ保護要求事項の理解、組織のデータ棚卸、データ利用といった事項に関する責任者を任命すべきである。当該責任者は経営層への報告責任も有する。	現在、DPO にはどのような資格要件や経歴があるべきかという議論があります。当社としては、それは組織特有の必要性に応じて異なり、その結果、職務内容が作成され、望ましいスキルと資格要件が特定されるものと考えます。
グローバル企業内の個人データまたは特別な種類の個人データをこれまで検索し、また、以下を識別したことがあるか？ ☐ どこに存在するか？ ☐ 誰がアクセスできるのか？ ☐ 誰がビジネスオーナーか？ ☐ 誰が各々のデータの責任者または管理者か？ 下記が定義されているか？ ☐ データの保持期間	Rec. 30; 第 4(1) 条	企業内の機微情報を検索する過程を「データディスカバリー」という。一度検出されると、不要になったデータは削除される。残りのデータはユーザーアクセス制御（UAC）、暗号化等といった、特定のコントロールが適用される。	データマップはグローバルの情報のエコシステムを通して個人データの場所を簡潔に文書化するのに有効です。ご要望に応じて多様なフォーマットにてデータマップを提供します。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
データにアクセスできる全ての第三者（共同の管理者または取扱者）は識別されているか？ 誰がどのデータ要素（名前、国民識別番号等）にそれぞれアクセスできるか？ 法的に可能となるデータ利用方法は何か？ データを実際何に利用しているのか？	第 28 条	第三者の契約で適用されている範囲を確認するためには、ビジネスオーナーへのインタビューと、ソフトウエアアプリケーションの目録が役立つであろう。通常、すべてを見つけるには数回の調査の実施が必要となる。	どの第三者が個人データにアクセスしており、それで何をしているのかの識別を通じ、法務部と人事部が驚きの事実に気づくことがしばしばあります。当社では、適切な部署のメンバーと第三者にインタビューし、必要な詳細をすべて明らかにすることができます。
個人データの各利用において、通知、選択、同意の要件はすべて満たされているか？	第 7, 9 条	従業員に対しては、同意は一般的に個人データの利用において有効な手段ではない。そのため、契約履行のような、別の根拠が必要となる。第三者によってデータが取扱われる場合は、通知、選択、同意の要求事項を第三者とレビューし、準拠事項を文書化することが重要である。特別な種類の個人データについては、通知、選択、同意について、独自の要件がある。	通知、選択、同意の要求事項を遵守するためには、契約内容のレビューだけでは不十分です。現実には個人データの取扱いが、契約書に記載されている内容と異なることが大いにありえます。組織内すべてにおいて、どのようなデータの流れになっており利用されているのか、規程と実務の連携が促されるように監査を実施します。
組織は、データ主体からのアクセス要求に応え、要求された変更や削除を遅延なく行うことができるか？	第 15, 16, 17, 20 条	いわゆる「忘れられる権利」もこれに含まれている。	データ主体からのアクセス要求は、事前に十分に用意していない組織にとって、時間がかかることがあります。当社のアプローチは、アクセス要求への応答計画策定にあたり、要求される可能性が最も高い情報や、どのようなフォーマットで生成すればよいかといったことを考慮します。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
個人データに適用している「技術的及び組織的なセキュリティ対策」を示す手段があるか？	第 32 条	構成要素は以下を含むものである： 暗号化または仮名化 機密性、完全性、可用性、そして取扱いシステム及びサービスの復元力の保護 停止後の個人データへのアクセスを復旧する能力 対策の効果を定期的に点検するプロセス	書面での情報セキュリティ計画の要求は、米国では珍しいことではありません。セキュリティプログラムの有効性を示すために、当社の情報セキュリティ計画の策定サービスの経験を活かすことができます。 もし貴社で、ISO/IEC 27001 のような第三機関の情報セキュリティ認証があれば、有効性の一部として活用することができます。
EU 圏外に個人データを移転しているか？ 「十分」な保護施策があると認められた国への移転であるか？ そうでない場合、EU 圏外に移転する個人データの全ての利用において、Privacy Shield (米国)、標準契約、拘束的企業準則（Binding Corporate Rules）といった移転のメカニズムはあるか？	第 35-39 条	「十分」な保護施策が確認されている該当国の一覧： http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm	データ移転メカニズムが正常に起草されている場合、個別の契約内容改訂の必要性を緩和できます。 どの契約条件が最もよい候補かを確認し、貴社の法務責任者へご提言します。

質問	Recitals（背景）/条文番号	解説	プロティビティの支援
組織は、侵害の疑いから７２時間以内に監督機関へ通知する、侵害通知計画があるか？その計画は意味のある詳細を提供できるものであるか？	第 33, 34 条	GDPR では 72 時間ルールについて詳述していないものの（取扱者においては「遅延なく」）、アメリカ国立標準技術研究所（NIST）による SP800-61 では、商業セクターが容易に採用できる有意義なガイダンスが提供されている。	72 時間という時間の制約は、医療や通信業界といった、運用が高度に規制されていないような組織にとっては、特に難しいでしょう。 当社は、独立した文書または大規模なインシデント対応計画として、侵害通知の全てのパターンに対処する計画をご用意します。
データ保護影響評価（DPIA）の必要性はあるか？ データ主体の高いプライバシーリスクをもたらす可能性のある新技術があるか？ 自動処理とデータ主体に対する法的効果があるか？ 特別な種類の個人データの大規模な取扱いはあるか？ 公共エリアの体系的で大規模な監視はあるか？	第 35 条	侵害の通知と同様、GDPR には DPIA についての詳細はほとんどない。：SP 800-122 のような NIST のガイドラインが非常に役立つものである。	当社では全ての種別に対する評価と監査についての深い経験をもっているため、最も問題が起こり得そうなポイントや、問題解決方法などを可視化できる DPIA を実施します。
第三者は下記においてデータ管理者と同様の基準を採用しているか？ 通知、選択、同意 情報セキュリティ 海外へのデータ移転 侵害の通知	第 28 条	データ保護指令とは異なり、第三者の共同管理者と取扱者は、データ管理者として効果的に同様の基準を採用することとしており、監督機関による直接管理対象である。	貴社に関与する第三者は、最大のデータ保護リスクを担っています。さらに、多くの第三者はどのように個人データを守るのか、書面により保証することはほとんどなく、侵害や文書に対する法的要求にどのように応えるのか明確になっていません。当社では、貴社向けに行った基礎的な作業による情報を基に、第三者と話し合うことによりこれらの懸念に対処します。

protiviti®