www.pwc.com/jp

GDPR リスク対応のアクションプラン：

個人データの第三者提供

pwc

GDPR リスク対応のアクションプラン：個人データの第三者提供

欧州連合（EU）の一般データ保護規則（GDPR）が施行され、欧州の個人データを含むデータ処理関連の業務をアウトソーシングする際のリスクが顕著になった。

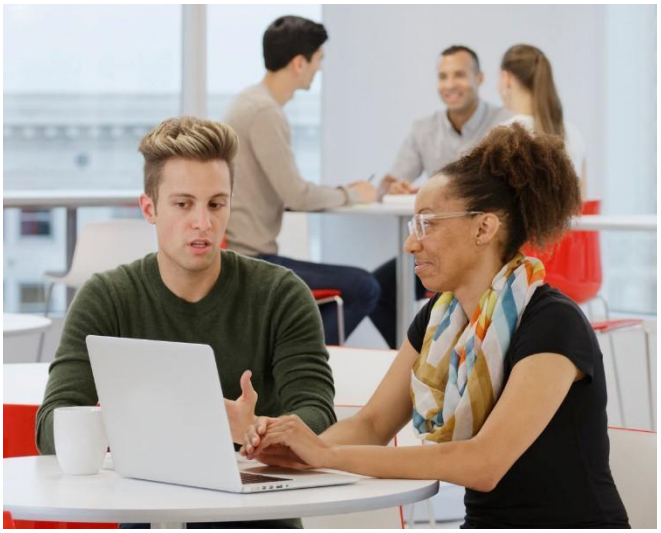
大規模な多国籍企業（以降、企業と記載。データを管理する「コントローラー」となる）は、多くの場合、数千社ものベンダーと契約し、何種類もの EU 個人データを取扱っている。そのため、GDPR によって、第三者へ個人データの取り扱い業務を委託する際にかかるリスクは、より広範かつ深刻になる。このような企業は、サプライチェーン全体における GDPR の執行と訴訟リスクを低減するため、アクションプランを検討し、推進する力が必要になる。

企業を取り巻く GDPR リスクは、より深刻かつ広範に

GDPR では5つの条文において、旧来のデータ保護指令（1995 EU Directive on Data Protect）には存在しなかった要求が加わった、あるいは、旧来の要求が強化された。

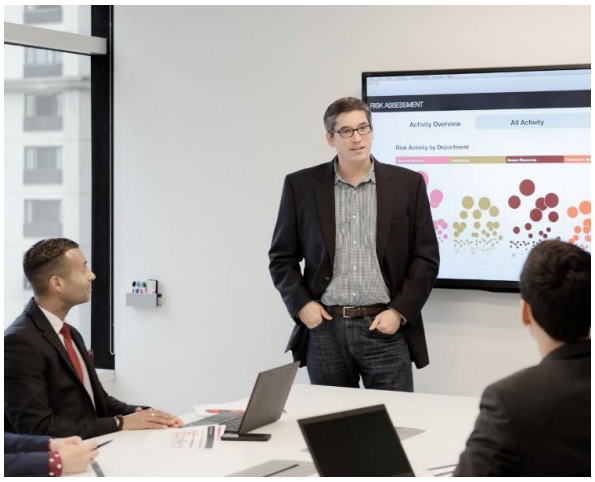
- **第 28 条 プロセッサー**：個人データの処理者（プロセッサー）と個人データの副処理者（以下、サブプロセッサー）は、適切な保護と GDPR 遵守の証拠を保全するような、契約上の保護が求められる
- **第 30 条 取り扱い活動の記録**：プロセッサーに対して、取扱う EU 個人データの詳細な台帳を維持することが求められる
- **第 32 条 セキュリティ保護の取り扱い**：プロセッサーとサブプロセッサーは、EU 個人データを保護するための、包括的な情報セキュリティ管理策を実装することが求められる
- **第 33 条 個人データ侵害の監督機関への通知**：プロセッサーは EU 個人データ侵害について不当な遅滞なしに、データ管理者（以下、コントローラー）に通知することが求められる
- **第 36 条 事前協議**：データプロセッサーは、特定の高リスクが存在するデータコントローラーの要請に応じて、データ保護影響評価（Data Protection Impact Assessments, DPIAs）を行うことが求められる

EU 個人データを処理するために第三者と契約する企業は、第三者からデータ主体要求の対応支援を得るために、そして、必要に応じて GDPR 遵守の証拠を入手するためにも、第三者との契約でサービスレベルを取り決める必要がある。



GDPR 対応施策：既存の第三者リスクマネジメントプログラムを強化

ベンダーに機微情報を提供する際の情報セキュリティリスクに対処するために、ほとんどの企業は、すでに第三者リスクマネジメントプログラム（Third-Party Risk-Management, TPRM）を運用している。このようなプログラムには、多くの場合、業務委託先やデータ処理の類型などの項目を記載した台帳を維持すること、ベンダーに情報セキュリティに関する標準契約条項を課すこと、セキュリティデューディリジェンスの質問票に対するベンダーの回答を確認することなどが含まれている。また、実地でのセキュリティレビューや監査をプログラムに加える企業も増えつつある。



GDPR のベンダーに対する要求事項に対処するために、欧州でビジネスを展開する企業は、既存の TPRM プログラムに、以下のような要素を加味し、拡張するようなアクションプランを検討すべきである。

- ベンダーの取り扱うデータを管理する台帳に、GDPR に関連するメタデータの欄を追加する
- ベンダーのリスクをランク付けする手法に、新しく GDPR に関連する事項を加える
- プライバシーに関する要求事項を標準契約条項に加え、影響する第三者に適用する
- プライバシーに関する要求事項をデューディリジェンスの質問票に加える
- プライバシー統制を外部監査に加える
- ベンダーの処理するデータ範囲の変化を特定し、DPIAs や EU 個人データの侵害の報告を促すため、ベンダーのモニタリングをより頻繁かつ厳密にする

データ保護に関するデューディリジェンスのスコープ拡大

GDPR 上の要求事項が更新された後、EU は企業が第三者に対して、より高水準のデューディリジェンスを実施することを期待していると考えられる。

個人データ処理を第三者の提供するサービスで実施する場合、企業は適切な水準のモニタリング手法を確立するために、その処理の性質や範囲、背景、規模、目的を理解しなければならない。解決方法の一つに、企業のリスクなどを総合的にまた詳細に調査して価値を査定するデューディリジェンスアセスメントの手法を修正して、DPIAs の要求事項を加え、実行することが挙げられる。このような評価手法は、第三者によるデータ主体の情報の取り扱いに対する厳格なモニタリングという目的を達成する一助となるばかりではない。GDPR 第 35 条で定められている、自然人の権利と自由に対して高リスクを及ぼしうるプロセスを特定することにもつながる。

> *“特に新たな技術を用いるなどのある種の取扱いが、その性質、範囲、文脈および取扱いの目的を考慮して、自然人の権利や自由に高リスクを生じさせる可能性がある場合、管理者は、取扱いの前に、予定された取扱い作業の個人データ保護への影響評価を実施しなければならない。独立した評価は同様の高リスクを示す同様の取扱い作業の集合で用いることができる。”*

データ保護責任者（DPO：Data Protection Officer）や適切なプライバシーリーダーと協力し、企業は最低でも以下のような事項を含むように、デューディリジェンスアセスメントを拡張すべきである。（1）プロセス運用が可視化できるような体系的な記述、（2）処理の目的、（3）該当する場合は、コントローラーが追求する正当な利益、（4）当該サービスを行うビジネス上の必要性の評価、（5）データ主体の権利と自由におよびうるリスク評価、（6）保障や安全管理措置を含む、明確なリスク対応法、（7）個人データ保護を確実にし、法令遵守するための仕組み

GDPR の下では、（例えば、ジョイントコントローラーとして）共同でデータを取扱う、あるいは、（例えばコントローラーのような）他の会社の代わりにデータを取扱うプロセッサー（第三者）は全て、新たな要求事項を満たす必要がある。もし、このような要求事項を満たさない場合、コントローラー（自社）や契約した第三者は違法とみなされ、罰金や制裁が課され、ブランド価値に影響が及ぶおそれがある。そのため、企業はデューディリジェンスのプロセスを見直し、下記のようなプライバシーに関する

要求事項を加味する必要がある。

- 第三者による侵害の通知
- 処理の記録
- 役割と責任
- セキュリティに関する統制
- 国境を越えた業務の実施
- 法令遵守の表明

企業はどのような場合にデューディリジェンスアセスメントを更新すべきか？

組織は、一般的に高いリスクがある状況下においてアセスメントを実施するが、個人データを扱う際には、従来にない処理、技術、サービス範囲を考慮したより戦略的なアプローチを検討する必要がある。どのような場合にデューディリジェンスアセスメントを実施するかは、最終的には企業が決定することになるが、自然人の権利と自由に影響を与える業務委託先を全て評価することが重要である。残念ながら、アセスメントを必要とするプロセスや活動に関する網羅的なリストは存在しない。しかし、GDPR は基本的なガイダンスやサンプルシナリオを提供している。このガイダンスには、記載する内容に限らないが、以下のような事項が含まれている：

- 第三者が、自然人の権利と自由に影響を及ぼす可能性のある高リスクプロセスまたはサービスを提供している、または提供する予定
- 第三者が、アクセス可能で大規模な公衆領域を自動的にモニタリングしている、またはモニタリングする予定
- 第9条(1)に記述されるような、有罪判決または犯罪を含む特有の大規模データおよび／または個人データを取り扱う第三者
- 第三者が、自然人に関連するプロファイリングおよび自然人に関する法的影響をもたらす決定事項を含む自動処理を評価する、または評価する予定
- 第三者が、新技術、またはデータ保護影響評価が実施されていないものを活用する、または活用する予定
- 第三者が、監督当局が定義した DPIA の実施を必要とするデータ取り扱い活動を行っている、また行う予定

考慮する取扱いに関連する活動やビジネス：

- クライアント向けの活動
- 子供に関連する活動
- マーケティングや広告
- デジタルトランスフォーメーション
- 地理位置情報
- プロファイリング
- 追跡
- 公共サービス
- マスコミ
- ジョイントベンチャー
- グローバルビジネス運用

契約を更新すべきタイミング

企業は、コントローラー（自社）とプロセッサー（業務委託先）間で役割や責任を明確にした契約を締結することが法的に要求されている。それぞれの契約書では最低でも、以下の事項を含める必要がある。

- 対象事項および取扱期間
- 性質および取り扱いの目的
- 個人データのタイプおよびデータ主体のカテゴリー
- プロセッサー（業務委託先）に対する最低限の要求事項
- コントローラー（自社）の責任および権利

新しい要求事項は、企業が GDPR の要求事項に準拠するだけではなく、コントローラーとプロセッサーがデータ主体とその個人データを適切に保護することを求めている。

モニタリングの改善を継続的に実施

GDPR が施行された後、第 28 条、31 条、32 条(d)および 39 条に記載されるような法令遵守のモニタリングと維持のため、企業や第三者が、より厳しい精査を受けることになる。業務委託先は、監督機関と協力することを求められるだけではなく、技術的・組織的な対策の有効性を判断する方法を確立することも期待される。判断する方法はリスクアセスメント、高リスクプロセス、保護するデータの種類および取り扱い方法や取り扱い担当者数の確認などが含まれている。

GDPR 上には、コントローラー（自社）やプロセッサー（第三者）と連携している DPO や指名されたプライバシーリーダーが、GDPR やその他 EU 加盟国が決定した規定の遵守状況をモニタリングすることが期待されている旨の記載がある。従って、継続的なモニタリング活動、プロセスおよび措置は、「通常業務」運用の一環として評価し、更新する必要がある。また、第三者との関係が今後も進化していく可能性があるので、企業はその関係の変化に伴って、変わるリスク水準や種類を有効に管理するために、柔軟に戦略を変化させていく必要がある。

第三者とのビジネスが終了する場合

GDPR 上には第三者とのビジネスが終了する場合の要求事項はないが、企業は、そのような状況に備えて、適切な措置を計画しておく必要がある。選択肢としては、企業がサービスを内部で提供できるよう計画を立てること、もしくは既存の第三者に代替する別の第三者と連携することが挙げられる。どちらの選択肢を選んでも、業務委託先、あるいは第三者からどのような種類のサービスを受けているかによって計画が変わってくる。そして、例示する事項に限らないが、どのような計画にも、以下のような事項が含まれるはずである。(1) 過渡期、(2) 技術およびセキュリティ要求事項、(3) データの保持および削除、(4) 法的規制要求、(5) ケーパビリティおよびリソースのニーズ、(6) サービスやビジネスへの影響度、(7) 戦略的リスク

結論

GDPR への適応は複雑かつ時間がかかる。企業が規制要件を内部で管理し、契約している第三者に対応できるような新しい戦略を採用しない限り、ビジネス全体に混乱を招く可能性がある。定義されたビジネスイニシアチブおよび目標を満たすよう、新しく強化された規制を遵守するリスク管理対策を組み込むことが、GDPR 対応を成功に導く。

お問い合わせ

この記事で取り上げたテーマについてのご相談をご希望の場合、以下までお問い合わせください。

T.R. Kane
Global Third Party Risk Leader
+ 1 (440) 390 8502
t.kane@pwc.com

Jay Cline
US Privacy Leader
+1 (763) 498 2237
jay.cline@pwc.com

日本のお問い合わせ先

PwC コンサルティング合同会社
東京都千代田区丸の内 2-6-1 丸の内パークビルディング
03-6250-1200（代表）

山本直樹
パートナー
naoki.n.yamamoto@pwc.com

松浦大
マネージャー
dai.matsuura@pwc.com

pwc.com/jp/gdpr

本報告書は、PwC メンバーファームが 2018 年5月に発行した「An action plan for tackling third-party GDPR risk」を翻訳したものです。翻訳には正確を期しておりますが、英語版との解釈の相違がある場合は、英語版に依拠してください。
オリジナル（英語版）はこちらからダウンロードできます。
https://www.pwc.com/us/en/services/consulting/cybersecurity/general-data-protection-regulation/third-party-risk-management-gdpr.html

日本語版発刊月： 2018 年 11 月