GDPR対応プロジェクト簡易診断

本簡易診断は、「GDPR対応プロジェクトの運営」、「管理組織と業務プロセスの整備」、「安全管理対策の導入」、「個人データ国際移転に係る対応」、「ルールの浸透・点検活動」といった観点から、自社におけるGDPR対応プロジェクトに重要な漏れがないことを点検するものです。

I. GDPR対応プロジェクトの運営状況

Q 診断項目　A 診断シートの回答が「グループ全体で実施済み」でなかった場合に検討すべき事項

1

Q **貴社のグループ内で収集、処理、保存されているEU在住者の個人データ* を網羅的に把握できていますか。**

* GDPRはEU域内企業だけの問題ではなく、日本も含めすべての国の企業が対象になりうる規制です。
EU在住者の個人データには、顧客情報だけでなく、EU域内の従業員や取引先担当者等の情報も含まれます。

A EU域内の拠点だけでなく、すべてのグループ会社を対象として、EU在住者に関する個人データの取り扱い状況を棚卸調査する必要があります。調査を行う際には、GDPRが求める処理の記録義務に係る項目や、国際移転の標準契約上に記載が必要となる項目についても、一度に情報を収集・整理しておくと効率的にプロジェクトを進められます。

2

Q **GDPR対応プロジェクトの責任部署の役割が定められ、IT部門等の関連部署との協力体制や経営陣への報告体制が整備されていますか。**

A グループ本社においてGDPR対応の主管部署を定め、組織横断的な対応プロジェクトを立ち上げることが必要です。通常は、法務・コンプライアンス、リスク管理・内部統制、IT・総務・セキュリティ、海外事業統括などの関連部門が連携し、各子会社と調整しながらプロジェクトを推進します。

3

Q **2018年5月のGDPRの施行に向けて、課題・タスク・対応部署が網羅的に洗い出され、課題等に対応するためのスケジュールが設定されていますか。**

A プロジェクトを運営していくための具体的な計画策定は不可欠です。まずはGDPR遵守のために到達すべきゴールを設定し、そこから必要となるタスクを洗い出して、その実施責任者及び実施期限を定めていきます。必要な関連部門との協議日程や正式な社内オーソライズを受ける会議体の予定なども計画に組み込みます。

II. 管理組織と業務プロセスの整備

4

Q **EU在住者の個人データを取得する際の同意取得に係るルール・手順を定め、確実に実施していますか。**

* EU在住者からの同意取得については、国内法令よりも細かい条件が設定されています。

（例）
- 同意の取得は明瞭で平易な文言により、誰もが容易に理解・判別できるような方法で行うこと
- データ主体に対して同意の撤回が可能であることを通知すること
- 同意の撤回を行う方法を十分に容易なものにすること
- 同意の取得について、取扱い目的の達成に必要のない事項を条件としないこと
- 同意取得の証跡を残すこと　など

A EU在住者に関する個人データを取得する際の同意取得に係るルール・手順を見直す必要があります。GDPR上で、同意が有効であるための条件として定められている項目をリストアップし、現在の同意取得がそれらを満たしているかどうか点検して見直しを行います。通常は、これに連動してホームページ上の個人情報保護方針・プライバシーポリシーの見直しも必要となります。

II. 管理組織と業務プロセスの整備（続き）

5

Q **EU在住者本人から様々な要求があった場合に、適切に対応できる体制とルール・手順を整備していますか。**

* データ主体の権利に基づく開示等の要求に対しては、原則として無償で1ヶ月以内に回答する必要があります。

A EU在住者であるデータ主体からの要求事項に対して、適切に対応できる体制・ルール・手順を整備する必要があります。消去権やデータポータビリティの権利など、GDPR上で明記されているデータ主体の権利一つ一つについて、実際にその要求を受けた場合にどのような対応を行うのか、それで対応上の問題はないのか、具体的にシミュレートして検証してみることが重要です。

6

Q **貴社におけるEU在住者の個人データの取扱いについて、その記録を作成・保存し、必要に応じて監督機関へ提示できる状態としていますか。**

* 原則として従業員が250名以上の企業は、管理者、処理者のいずれの立場でも記録の作成義務があります。

A EU在住者に関する個人データの取り扱い状況を、管理台帳として取りまとめておく必要があります。管理台帳のフォーマットを見直し、GDPR上で処理の記録を義務付けられている項目についてすべてカバーできるように修正すると良いでしょう。

7

Q **データ保護オフィサー（DPO: Data Protection Officer）* の設置要否を判定し、設置の場合その役割・責任を定めていますか。**

* 社内の法令遵守状況をモニタリングし、データ主体や監督当局との対応を統括する役割です。

A EU加盟国の各国法令におけるDPO設置要件も考慮しながらDPOの設置要否を判断し、任命する場合は、正式な役職として職務規程に役割と責任を明記することが必要です。既に既存の役職で重複する責任や役割を担っているものとの調整も必要となります。

8

Q **EU在住者の個人データを新たに取り扱う場合のデータ保護影響評価*（DPIA：Data Protection Impact Assessment）を実施するルール・手順を定めていますか。**

* データ主体の権利侵害につながるリスクを評価し、必要な場合は監督当局と協議することが必要です。

A 今後新たにEU在住者に関する個人データを取り扱う場合に備えて、データ保護影響評価を実施するためのルール・手順を定めておくことが必要です。そもそもアセスメントを行う必要があるのかどうかを判断するための基準・プロセスについても、予め整備しておくことが必要です。

9

Q **EU在住者の個人データを複数事業者で共同管理する場合、その責任分担等を契約の締結により取り決めていますか。**

*共同管理における責任分担は、文書として整備し、データ主体の求めに応じて提示できる必要があります。

A EU在住者に関する個人データを複数事業者で共同管理する場合には、当該事業者間でその責任分担等を定める協定文書を締結する必要があります。既に契約文書が存在する場合でも、その内容がGDPRの関連条項の主旨に照らして適切なものであるかを点検することが必要です。

III. 安全管理対策の導入

10

Q **取扱う個人データのリスクレベルに応じて、暗号化や仮名化、物理的安全管理措置、データ侵害を阻止するためのシステムセキュリティ対策、障害発生時の復旧対策などを講じていますか。**

*リスク区分とそれに応じた安全管理策の要件を定め、その合理性を対外的に説明できることが重要です。

A 個人データの取り扱いに関するリスクのレベルを定義し、そのレベルに応じたセキュリティ対策及びプライバシー保護対策をグループ共通方針として策定する必要があります。また、この方針に基づき、特に既存の取り扱いで方針を満たせていない高リスクのものについて、システムの改修対応等も含め、具体的な対応計画の策定と実行が必要です。

11

Q **EU在住者の個人データの取扱いを外部に委託する際の方針やルール等を定め、方針等に則った契約を締結していますか。**

* 委託先においても自社と同等の取り扱いが行なわれるよう、適切な管理措置を指示する必要があります。

A 委託先においてもGDPRを遵守した取り扱いが確実に行われるよう、委託先に適切な管理義務を課すための契約条項等を整理し、委託契約を締結する際には、これらを含めるようにすることが必要です。また、既存の委託契約内容についても点検を行い、必要に応じ契約の見直しや覚書の締結等を行います。

12

Q **EU在住者の個人データ漏洩などの事故が発生した場合、事故を認識してから72時間以内に監督機関へ報告できるよう、報告基準、報告者等のレポートライン等の具体的な報告手順を定めていますか。**

* 委託先で生じた事故でも、貴社が管理者となっているものは72時間以内に報告しなければなりません。

A GDPRの要件を満たせるかどうかという観点で、個人データ漏洩などの事故発生時における対応手順を見直すことが必要です。グループ各社で事故が発生した場合に、EU在住者に関する個人データが含まれているかどうかの識別、含まれていた場合の連絡・報告ルート、エスカレーション基準、監督当局やデータ主体等への報告に係る具体的な役割と責任などを明確にしておくことが必要となります。

IV. 個人データ国際移転に係る対応

13

Q **EU在住者の個人データをEU域外へ移転する場合のルール・手順*を定め、運用を開始していますか。**

* 域外へ移転する場合、EUが定める標準契約条項(SCC)により契約締結を行う等の措置が必要です。
*日本へ移転されたEU在住者の個人データを、更に別の日本企業へ提供する行為も国際移転となります。

A EU在住者に関する個人データをEU域外へ移転する場合のルール・手順について、明確に文書で定めておくことが求められます。尚、一度EU域外へ移転されたデータを、更に別のEU域外の企業へ提供する場合も、同様のルールが適用されるようにしなければならない点に注意が必要です。

14

Q **グローバルで利用されるITシステムにおいて、意図せずにEU在住者の個人データが国際移転してしまうリスクの評価とその対策は十分に行なわれていますか。**

* 自国のサーバ上のデータを他国から閲覧可能な状態である場合も国際移転と見なされます。

A EU在住者に関する個人データがITシステム上にある場合、そのアクセス制御の状況を確認し、意図しない国際移転が生じていないことを確認する必要があります。これは通常の利用者についてだけではなく、開発、テスト、保守、その他関連サービスに関与する担当者のアクセス可能範囲の確認を含みます。もし、想定外の国際移転が生じていた場合は、アクセスの遮断か、国際移転に関する適切な措置を講じることが必要です。

V. ルールの浸透・点検活動の状況

15

Q **上記設問のような個人データの取り扱いルールを社内規程等として文書化し、従業員に周知・教育していますか。**

A 上記で言及されている方針やルール等は、正式な社内規程等として文書化し、関連する従業員に周知・教育を行う必要があります。また、異動や新規採用などで今後新たにEU在住者に関する個人データの取り扱いを行う者に対しても、確実にそのルールが伝達されるよう計画されていなければなりません。

16

Q **貴社グループ内におけるEU在住者の個人データの取扱いについて、GDPRの要件を遵守していることが証明できるよう、定期的に適切な点検・監査を実施するよう計画していますか。**

A GDPRの遵守状況について定期的に適切な点検・監査が行われるように、予め実施体制や手順等を計画しておくことが必要です。また、定期的な点検・監査を行うためには、現場で適切に取り扱いに関する記録の保持も行われなければならない点に留意が必要です。

KPMGコンサルティング株式会社
サイバーセキュリティアドバイザリー

〒100-0004
東京都千代田区大手町1丁目9番7号
大手町フィナンシャルシティ サウスタワー
TEL ： 03-3548-5111

cybersecurity@jp.kpmg.com
kpmg.com/jp/cyber-security