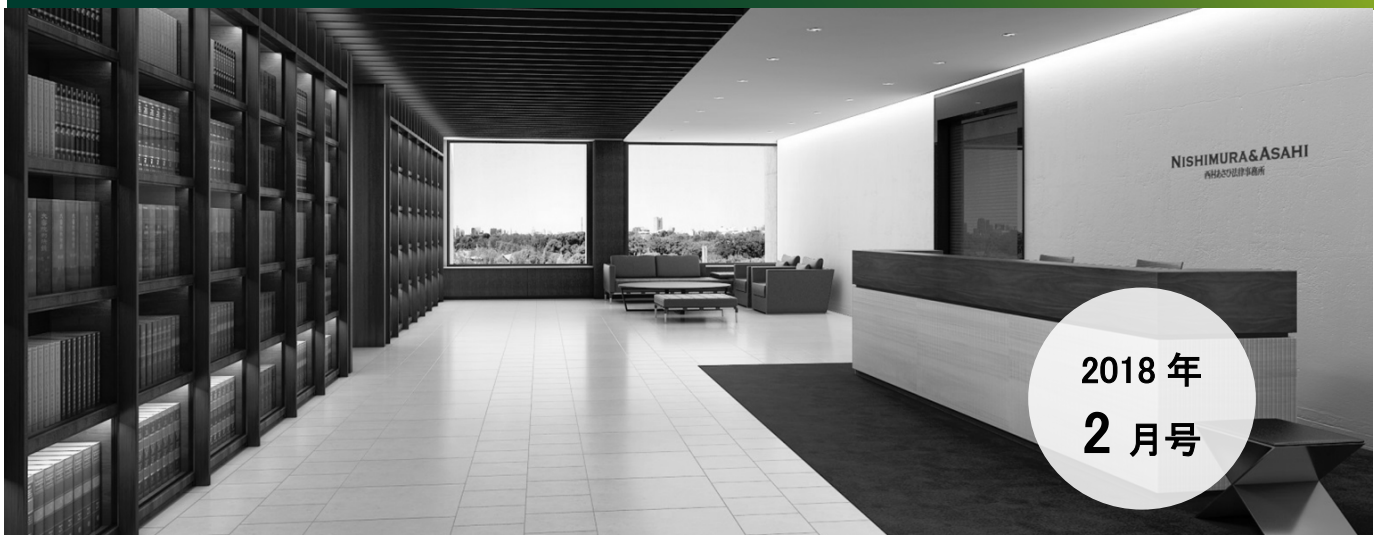
西村あさひ法律事務所
NISHIMURA & ASAHI
企業法務ニューズレター



GDPR 対応と日本のデータ越境移転規制対応の実務

執筆者：石川 智也、河合 優子、白澤 秀己

本年 5 月 25 日の施行まで 3 ヶ月を切り、GDPR に関する相談が多く寄せられています。

GDPR は、セミナー等を通じて、その概要、高額の制裁金の存在、対応の必要性を知る機会はあり、また、条文の翻訳やそれを日本語でまとめた書籍や記事等はあるものの、何をどのように対応すれば良いのかが分かりにくく、対応が進まないケースが少なくありません。一言で言えば、GDPR 対応は、欧州にいる者の個人データの処理を確認・記録化して説明できるようにすることと、情報セキュリティのためのコンプライアンス体制の構築であり、経営の課題としてトップダウンで取り組んでいくべきものです。また、コンプライアンス体制の構築である以上、いったん整備して完了となるわけではなく、その周知・運用と見直しについて不断に取り組んでいくことが求められます。

本ニューズレターでは、質問を受けることが多い GDPR 対応が必要な企業の範囲を概観した上で、個人データが収益の源泉となるビジネスであるか否かにかかわらず、あらゆる企業が取組みを求められることの多い事項を概観します。各企業の実情を踏まえて、何を、どのような順序で、どのように進めるべきかというガイダンスも行っていますので、対応が未検討である、あるいは対応が思うように進んでいない等してガイダンスを希望されるという場合には、問い合わせフォームを通じてご連絡ください。

また、GDPR との関係で個人データの域外移転規制が注目されていますが、日本の個人情報保護法上も、従業員、取引先担当者や顧客等に関連する個人データを第三者(グループ会社を含みます。)に提供する場合には所定の措置を講じる必要があり、さらに外国にある第三者に個人データを提供する場合には、同法の越境移転規制との関係で追加の措置を講じる必要があります。この点への対応が未了の場合には、日本が欧州委員会から十分性の認定を受けて欧州から日本への個人データの移転が許されたとしても、その後の日本から海外への個人データの移転が違法となり得ますので、この機会に対応を講じるべきと考えられます。各企業の実情に即した具体的な対応は、問い合わせフォームを通じてご連絡いただければと思いますが、本ニューズレターでは、一例として日本から海外のグループ会社に個人データを移転させる場合の具体的な手法を紹介いたします。

1. GDPR 対応が必要な企業の範囲

(1) EEA 域内にある拠点での対応

まず、EEA(28 の EU 加盟国と、アイスランド、リヒテンシュタイン、ノルウェーの合計 31 カ国)域内にある拠点では、個人データの処理に GDPR が適用され、必ず何らか取り組むべき事項があります。日本企業としては、EEA 域内にある拠点において GDPR への対応を検討しているか確認し、検討していない場合には検討を指示する、あるいは当該拠点が主体となっての検討が難しい場合には本社サイドで対応を検討する必要があります。また、EEA 域内にある拠点が GDPR への対応を検討している場合も、進捗と今後の見通しを確認し、状況に応じて本社サイドによるサポートを検討するべきと考えられます。

この EEA 域内にある拠点での対応は、事業の規模や従業員の人数、今後日本が欧州委員会から十分性の認定(大要、個人データの域外移転が認められる国としての認定という意味です。)を受けるか否かにかかわらず必要であることに注意してください。対応を行わない、あるいは状況を見守ることにするという判断は、個人データの保護を故意に無視するものとして、制裁金を課すか否か、また、課すとしてどの程度の金額を課すかの判断に際して考慮されることになります。

(2) 日本本社その他の EEA 域外にある拠点での対応

日本本社その他の EEA 域外にある拠点でも対応が必要になる場面があります。特に、次のいずれかの個人データの処理を行う場合には GDPR が域外適用され(GDPR 第 3 条第 2 項)、EEA 域内に子会社や支店等の拠点を有していない日本企業であっても原則として対応が必要となります。また、この場合には、EEA 域内に代表者[1]を選任する必要が生じる場合があります(GDPR 第 27 条第 1 項)。

① EEA 域内に所在する本人に対する商品またはサービスの提供に関する処理
② 本人が EEA 域内で行う行動の監視に関する処理

①は、EEA 域内に所在する本人に対して商品・サービスの提供を意図していることが明白か否かで判断されます。単に EEA 域内から日本のウェブサイトへのアクセスが可能なだけで問題になるわけではありませんが、EEA 域内に所在する市民を商品・サービスの提供先として想定してビジネスを展開している場合には、GDPR が適用される可能性があります。たとえば、EEA 域内に向けてサービスを展開するオンラインモールやサービスプロバイダーのほか、EEA 域内からの予約が可能な鉄道・交通機関や宿泊関連施設、または、EEA 域内でも利用可能なオンラインゲーム、アプリやウェアラブル端末の機能等で、検討が必要であると考えられます。

②は、本人の行動を監視しているといえるかは、本人に関する決定を行う目的で、または本人の個人的な嗜好、行動および態度を分析または予測する目的で、本人がインターネット上で追跡されているかどうかで判断されます(GDPR 前文第(24)項)。具体的には、EEA 域内に所在するアプリやウェアラブル端末等を通じて個人データを採取して分析する場合、クッキー等を用いて EEA 域内の閲覧者のウェブサイトへのアクセス状況を解析する場合、現在地測定情報を利用してユーザーの行動を分析する場合などには、その部分について GDPR への対応を検討する必要があります。

悩ましいのは、EEA 域内に子会社・支店等の拠点はあるものの、拠点主導で EEA 域内のビジネスを展開しており、本社の EEA 域内でのビジネスへの関与は限定的という場合に、本社に GDPR の適用があるか否かです。条文上は、「EEA 域内にある拠点(establishment)の活動[2]に関連する管理者または処理者による個人データの処理」について GDPR が適用されます(GDPR 第 3

---

1 代表者となることを提供するサービスを提供している業者があります。

2 「EEA 内にある」が「管理者または処理者」にかかるように読める訳文も存在しますが、その後の「処理が EEA 内で行われるか否かにかかわらず」という文言と併せて読むと、「EEA 内にある拠点」と読むのが自然であると思われます。

条第 1 項)。日本企業にとっては、EEA 域内の子会社や支店が拠点に該当する可能性があるところ、条文上は、現地に拠点たる子会社が存在し、その拠点の活動に関連して EEA 域内にいる者の個人データを本社で何らか処理している場合には、本社にも GDPR の適用があると読めます。他方で、GDPR の前身である現行のデータ保護指令の同じ文言が問題になった事件[3]において、欧州司法裁判所は、域外の企業による個人データの処理と現地の拠点の活動に密接な関係がある場合に、域外の企業に現行指令に基づく各国法が適用される旨を述べており、現地に拠点たる子会社があり、個人データの移転を受けているというだけで、常に日本本社での EEA 域内にいる者の個人データの処理に GDPR が適用されるわけではないとの考えもあり得るところです。

この点は、現時点では明確な解釈指針が示されていないため、処理の目的、本社での個人データの処理の態様、および、本社での EEA 域内にいる者の個人データの処理と現地の拠点の活動の関連性の程度を考慮し、リスクの程度を踏まえてケースバイケースで判断せざるを得ないものと思われます。

以上の検討を踏まえて GDPR の適用を受ける企業においては、日本が欧州委員会から十分性の認定を受けるか否かにかかわらず GDPR への対応が必要であることに注意してください。そのほか、GDPR の適用を受けない場合であっても、日本企業が EEA 域内にある企業から個人データの移転を受けている場合には、当該データの取扱いについて GDPR の域外移転規制への対応を検討する必要があります。この点については、日本が欧州委員会から十分性の認定を受ければ、日本の個人情報保護法および個人情報保護委員会が示す予定のガイドラインに従って当該データを取り扱うことで足りることになります。

2. GDPR 対応の実務

GDPR 対応のための作業の手順として、データマッピングを行い、その結果に基づいてリスクを分析し、必要な対応を行っていくということがいわれるものの、実際に何を行うべきかが全く見えないという声を良く耳にしますので、本項では、GDPR 対応のプロジェクトを進めていく際に検討することの多い対応項目を具体的に示します。少しでも早く作業に取りかかっていただくことを目的として、作業の項目・手順と、手がかりとなる情報を要約的に示しますが、あくまでどの企業においても問題となることの多い項目を紹介するものにすぎず、GDPR との関係で対応が必要となる可能性がある項目を網羅的に列挙しているものではないことにご留意ください。

また、ドキュメント類の作成や体制整備の前提となる個人データの処理の状況を分析すると、なかなか「データの処理」に当たることに気がつかないデータの処理やフローが見つかり、その部分についても対応が必要となるのが通常です。したがって、各社の具体的な状況を踏まえたアクションプランの策定については、専門家の助力を得ることを強くおすすめいたします。

(1) プライバシーポリシーの作成

個人データを収集する場合には、本人に一定の情報を提供するために、プライバシーポリシー(現地では、本人に一定の情報を提供し、かつ自社の個人データ処理に関する指針や手続を示す文書の呼称として、privacy policy のほかに privacy notice という呼称が用いられることも多くみられます。)を作成し、本人がアクセスできる状況におく必要があります。作成に際しては、従業員、顧客、取引先の担当者、採用候補者等、会社が取り扱う個人データのカテゴリー毎に検討していきます。

記載項目は、本人から個人データを取得する場合については GDPR 第 13 条第 1 項に、本人以外から個人データを取得する場合については GDPR 第 14 条第 1 項に、それぞれ列挙されています。記載に当たって留意すべき内容は、透明性に関するガイドライン(案)[4]に公表されています。これらの条文・ガイドライン(案)を確認しながら、専門家が提供するテンプレートや、欧州企業が公表している実例を参照して作成していくことが可能です。

プライバシーポリシーの作成に際しては、GDPR の条文に規定されている内容をそのまま記載することで足りる項目もあります

---

[3] Case C-131/12, Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) et al., ECLI:EU:C:2014:317 (May 13, 2014).

[4] Article 29 Data Protection Working Party, Guidelines on Transparency under Regulation 2016/679, wp260.

が、個人データの処理の「法的根拠」(GDPR 第 6 条第 1 項(f)号に基づいて処理が行われる場合には正当な利益の内容を含みます。)[5]、保持期間、域外移転を行っているか否かと移転方法、講じている組織的・技術的措置の内容等についての説明が求められます。そのため、個人データとしてどのようなものがあるかを洗い出した上で、プライバシーポリシーの記載項目を埋めるために必要な情報を収集する必要があり、また、記載項目について対応が未了の場合には、関連する対応を講じる必要があります。

なお、洗い出すべき個人データのメッシュ感・種類や、収集すべき情報の項目については、イギリスの監督機関が公表しているテンプレート[6]が参考になります。

(2) GDPR に準拠した同意のプロセスの確立

前記の「法的根拠」の 1 つとして、同意に基づいて個人データを処理している場合には、GDPR のルールに準拠した内容の同意であることを確立する必要があります(GDPR 第 4 条第(11)号、第 7 条など)。同意の考え方については、ガイドライン案[7]が公表されていますので、条文とガイドライン案に従って内容と体制を整備していくことになります。特にオンラインで同意を取得する場合には、表示される画面を 1 つずつ検証して、細かな点まで(チェックボックスに予めチェックされた状態のものは不可であるなど)プロセスの検証が必要となります。

いわゆるセンシティブデータについては、明示の同意がある場合等、GDPR 第 9 条第 2 項に列挙されている事由に該当しない限り、取り扱うことができないことに留意を要します。

(3) GDPR を遵守するための社内規定等の作成

従業員が、GDPR に準拠して個人データを扱うためにも、本人からアクセス権、消去権、訂正権、処理の制限に関する権利の主張を受けたときに期限内に然るべく対応するためにも、社内規定等を作成し、従業員に周知する必要があります。

(4) 個人データの処理の委託先との間の契約の確認・見直し

個人データの処理を第三者に委託する場合には、第三者が適切な技術的および組織的措置を講じていることについて十分な保証を提供する者に委託する必要があります(GDPR 第 28 条第 1 項)。委託に際しては、少なくとも下記の事項を契約内に規定しなければなりません(GDPR 第 28 条第 3 項)。

したがって、GDPR の適用を受ける企業は、個人データの処理の委託先を洗い出した上で、十分な技術的および組織的措置を講じているかを確認するとともに、契約に下記の条項が入っているかを確認し、もし入っていない場合には契約内容を修正する必要があります。

①	管理者からの文書化された指示に基づいてのみ個人データを処理すること
②	個人データの処理を許可された個人が機密保持を確約するか、または適切な機密保持義務下に置かれることを保証すること
③	32 条により要求されている全ての対策(個人データ保護のための措置)をとること
④	再委託に際して、大要、管理者の許可を取得するとともに、委託契約を締結すること

[5] 大要、①本人の同意に基づく場合、②契約の履行のために処理が必要な場合、③法的な義務を遵守するために処理が必要な場合、④本人または他の自然人の重大な利益を保護するために処理が必要な場合、⑤公共の利益等のために処理が必要な場合、⑥正当な利益のために処理が必要な場合(但し、本人の基本的権利および自由が優先する場合を除きます。)。①②⑥のいずれかに該当することが多いといえます。

[6] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/

[7] Article 29 Data Protection Working Party, Guidelines on Consent under Regulation 2016/679, wp259 (Nov. 28, 2017).

⑤	処理の性質を考慮し、可能な限りにおいて、管理者が本人の権利行使の要求に応じる義務を履行するため、適切な技術的および組織的対策によって管理者を支援すること
⑥	処理の性質および処理者の利用可能な情報を考慮し、所定の義務の遵守を確実にすることにおいて管理者を支援すること
⑦	サービス終了後の個人データの返却および、複製物の消去
⑧	本条項に定められた義務の遵守の証明と、監査の準備のために必要な情報の管理者への提供

(5) 個人データの処理活動の記録

従業員が 250 名以上いるか、または、センシティブデータを取り扱っている場合には、個人データの処理に関して下記の事項を記録する必要があります(GDPR 第 30 条)。また、従業員の人数等にかかわらず、個人データの事故(後述します。)が生じた場合には所定の事項を記録する必要があります(GDPR 第 33 条第 5 項)。そのため、これらを記録するためのフォーマットを用意し、実際に記録を行う体制を整備する必要があります。実務的には、従業員の人数にかかわらず、個人データの処理状況を説明することができるように記録を行うことが推奨されています。

なお、GDPR 第 30 条第 1 項に基づく記録は、日本の個人情報保護法により求められる確認・記録と異なり、個人データを処理する都度作成する(たとえば、個人データを譲渡するたびに作成する)のではなく、社内での個人データの処理として想定されるものを調査のうえ、あらかじめ作っておくものになります。

①	管理者の名前と連絡先の詳細。該当する場合には、共同管理者、管理者の代理人およびデータ保護責任者を含む
②	処理の目的
③	データ主体の種類と個人データの種類の概要
④	第三国または国際機関における受領者を含め、個人データが開示される、または、開示される可能性のある受領者の種類
⑤	該当する場合には、第三国または国際機関を特定した形式による第三国または国際機関への個人データ移転、および、49 条 1 項後段で定める移転の場合、適切な保護措置に関する文書
⑥	可能な場合には、データの種類毎の消去までの予測される期限
⑦	可能な場合には、32 条 1 項で定める技術的および組織的安全管理措置の概要

(6) 違反時の監督当局への通知義務・被害者への連絡義務を遵守するための態勢整備

個人データの事故が生じた場合には、気付いてから 72 時間以内に監督当局に所定の事項を通知することが求められます(GDPR 第 33 条第 1 項)。また、個人の権利や自由に高いリスクが生じるおそれがある場合には、本人に連絡することも求められます(GDPR 第 34 条第 1 項)。ここでいう事故には、情報漏えいだけではなく、情報の紛失やアクセス喪失など、情報の完全性、可用性、機密性が害された場合が広く含まれます。

したがって、それらの事故が生じたときに上記の対応ができる情報セキュリティの体制を講じる必要があります。この体制を検討するに当たり、何が事故に当たるか、何を以て気付いたといえるか、どのような場合に通知や連絡が必要かといった内容についてはガイドライン案[8]が公表されており、それらを参照しながら社内の体制を整備していくことになります。

(7) データ保護影響評価の要否の確認と(必要な場合の)実施

体系的かつ広範なプロファイリングを実施したり、センシティブデータを大規模に処理したりするなど、自然人の権利および自由

[8] Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016/679, wp250 (Oct. 3, 2017).

に対して高いリスクを生じさせる可能性の高い個人データの処理活動を行う場合には、データ保護影響評価というプロセスを実施する必要があります(GDPR 第 35 条、第 36 条)。

したがって、このデータ保護影響評価が必要か否かを判定し、必要な場合にはそのプロセスを実施する必要があります。この判定に際しての具体例や、プロセスの内容についてはガイドライン [9]が公表されており、参考になるものと思われます。

(8) データ保護責任者の要否の確認と(必要な場合の)選任

大規模な態様での定期的かつ体系的な監視を行ったり、センシティブデータの大規模な処理を行ったりする場合には、データ保護責任者を選任する必要があります(GDPR 第 37 条第 1 項)。また、GDPR 上は、各国法でデータ保護責任者の選任義務を追加することが可能であるところ、実際にドイツでは選任義務が追加されており、データ保護責任者を選任しなければならない場合が広範になっています。選任が必要な場合、社内で選任することも外部にアウトソースすることも可能ですし、グループ企業で 1 名を選任することも可能ですし、EEA 域外にいる者を選任する(日本で選任する)ことも可能です。

したがって、企業は、データ保護責任者を選任する必要があるか否かを検討し、必要がある場合には誰を当てるかを検討する必要があります。データ保護責任者についてもガイドライン [10]が公表されており、これらの検討に際して参考になりますが、特に誰をデータ保護責任者に当てるかについては様々な考慮要素を踏まえて検討する必要があり、専門家の助言を得ることをおすすめいたします。

(9) 個人データの域外移転規制への対応(SCC の締結等)

この点については、各方面で情報がありますので端的な紹介にとどめますが、EEA 域内から日本その他の十分性の認定を受けていない国に個人データを移転することは原則として禁止されており、実務的には、拘束的企業準則(Binding Corporate Rule)を策定するか、標準契約条項(Standard Contractual Clause)が含まれたデータ移転契約を締結して、域外移転のための対処を行うのが一般的です。その他にも、本人の明示の同意がある場合(ただし、従業員については依拠しにくいです)や、本人との契約の履行のために必要な場合など例外的な場面では域外移転が可能となる場合があります。

実務的によく利用される標準契約条項については雛形がウェブサイト上に公表されており、その内容は変更することができないため、あとは別紙に補充するべき内容(誰の情報か、移転目的、移転するデータの種類、センシティブデータが含まれる場合にはその内容、移転先で情報を受け取る者、最長保存期間など)を調査・補充して、契約を締結することになります。

今後、日本が十分性の認定を取得した場合には、EEA から日本への個人データの移転については域外移転規制への対応が不要となるため、これから準備をする企業にとっては域外移転規制への対応(標準契約条項の準備)を行うべきか迷われるところもあるかもしれません。しかし、日本以外の十分性の認定を受けていない国にも個人データの移転がある場合には、それらの国との関係では日本が十分性の認定を受けるか否かにかかわらず対応が必要ですし、実際に個人データの移転のフローを調べてみると、EEA から直接日本に個人データが移転しているのではなく、日本以外の第三国のサーバーを経由しているなどして対応が必要となることなどもありますので、慎重に判断する必要があります。

(10) その他

紙幅の関係で詳細は割愛いたしますが、未成年者から同意を取得する場合の特則、個人データの処理に関わる新たな製品を開発する際のプライバシー・バイ・デザインの考え方、ポータビリティやプロファイリングに関する規制など、ビジネスによっては更

---

9 Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and Determining Whether Processing Is "Likely to Result in a High Risk" for the Purpose of Regulation 2016/679 , WP 248 (Oct. 4, 2017).

10 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01 (Apr. 5, 2017).

なる対処が必要となるものがあります。

(11) まとめ

GDPR の対応が必要な企業においては、少なくとも前記の(1)から(9)までの個人データの処理に関する具体的な記録・書面化と、体制整備に向けた検討を速やかに開始することをおすすめしたいと思います。本ニューズレターでは、あらゆる企業において検討が必要となる項目を例示的に示しましたが、真に GDPR を遵守しているといえるためには、各社で処理している個人データの種類とフローを踏まえたアクションプランの検討が必要となります。

そして、GDPR 対応は、書面・体制を整備して完了ではなく、その周知・運用の徹底と定期的な見直しを通じて、個人データに事故が生じるリスクを低減していくことが重要です。その観点からは、今後は、各社のデータのフローや規定類を踏まえた社内向けのセミナーなども取り入れ、その周知・運用の徹底を図っていくことが重要となってきます(個人情報保護法の施行に際して社内セミナーを行っていれば、それと同じようなスタンスのものを GDPR についても行うべきということです)。実際、現地ではマネジメント向けのセミナー、個人データを扱う従業員向けのセミナーをそれぞれ実施するなどして、その周知・運用のプロセスにも重きが置かれています。

これらの記録・書面化のサポート、アクションプランの検討、GDPR 対応のための社内向けセミナー等についても対応していますので、問い合わせフォームを通じてご連絡ください。

3. グループ会社間で個人データを移転するために必要な個人情報保護法上の対応

個人情報保護委員会は、今後日本が十分性認定を受ける可能性を考慮し、十分性認定を根拠に EU から日本に移転される個人データの取扱いに関するガイドラインを策定する予定であり、本年 2 月 9 日にその方向性[11]が示されました。これによれば、要配慮個人情報の範囲、保有個人データの範囲、利用目的の特定、匿名加工情報について、個人情報の保護に関する法律(以下「法」といいます。)に上乗せした新たな対応が必要となる見通しです。

もっとも、日本から外国への個人データの再移転の論点との関係では、法で定められた越境移転規制(法第 24 条)への対応を講じていれば、基本的に新たな対応は不要となる見通しです。しかし、昨年 5 月の法改正時に新設された越境移転規制(法第 24 条)、すなわち外国にある第三者に個人データを移転する際の規律について、対応未了であった場合には、その点への対処を行う必要があります。

そこで、以下では、ご質問を受けることの多い事例として、従業員や取引先担当者に関する個人データをグループ会社に移転する場合について、実務的な手法を説明します。

(1) 日本のグループ会社との間の個人データの共有

まず、日本国内に所在する企業が、同じく日本国内に所在するグループ会社との間で、従業員や取引先担当者に関する個人データをやりとりする場合、当該従業員や取引先担当者本人から事前に同意を得なければならないのが原則です(法第 23 条第 1 項本文)。もっとも、この方法では、個人データの移転のたびに確認記録義務(法第 26 条)が発生する場合がありますし、事前に本人全員の個別同意を得ることが実務上困難な場合が多いと思われます。

そこで、昨年の 5 月以降は、グループ会社間での個人データの移転に際してはいわゆる共同利用の枠組みを採用する企業が増えています(法第 23 条第 5 項第 3 号)。この方法では、共同利用の制度を導入することについて本人から同意を得る必要はないと考えられますし、個人データの移転に伴う確認記録義務は生じず(法第 26 条第 1 項但書)、いわゆるオプトアウト方式による場合と異なり個人情報保護委員会への事前届出の必要もありません。

11 https://www.ppc.go.jp/files/pdf/300209_siryou1.pdf

具体的には、(i)個人データを共同利用する旨、(ii)共同利用される個人データの項目(氏名、住所等)、(iii)共同利用者の範囲、(iv)共同利用者の利用目的、(v)当該個人データの管理責任者の名称を、共同利用の開始前に「本人に通知」し、またはプライバシーポリシーや社内イントラに掲載する等して「本人が容易に知り得る状態」に置きます[12]。なお、上記(iv)または(v)を変更したい場合には、当該変更についてあらかじめ本人に通知し、または本人が容易に知り得る状態に置く必要があります(法第 23 条第 6 項)[13]。これに対して上記(ii)または(iii)を変更したい場合は、事前の通知等では足りず、本人の同意を得る必要があると解されていますので、留意が必要です。この点で、上記(iii)については、将来的な M&A や組織再編によりグループ会社が増減する可能性を見据えて、「株式会社 XX およびその直近の有価証券報告書に記載されている連結子会社」といった記載を行い、共同利用する範囲の定義を明確にした上で、該当する各連結子会社の名称を表示した URL のリンクを貼る等の工夫をする例が多く見られます。この方法によれば、グループ会社が増減しても、その定義の範囲内である限りは本人の同意は不要です。

(2) 海外のグループ会社との間の個人データの共有

共同利用の枠組みを採用したとしても、日本国内の企業が海外のグループ会社との間で個人データを共同利用するためには、法第 24 条が定める越境移転規制との関係で追加の措置を講じる必要があります。法第 24 条は、「外国にある第三者」[14]に個人データを提供するためには越境移転に関する本人の同意を得ることを原則的なルールとしており、これは、法第 23 条第 5 項が定める共同利用の枠組みによる場合でも同様です。

グループ会社間の場合の実務的な対応としては、グループ会社間で契約を締結し、または共通内規やプライバシーポリシーを利用して、法第 4 章の各規定を海外グループ会社に遵守させる方法が一般的です。これにより、海外のグループ会社は「個人情報保護委員会規則で定める基準に適合する体制を整備している者」(法第 24 条)に該当し、そもそも「外国にある第三者」ではなくなるので、個人データを当該グループ会社に越境移転させることについての本人の同意が不要となり(法第 24 条の第三者に関する括弧書、個人情報の保護に関する法律施行規則第 11 条第 1 項、個人情報保護委員会「個人情報の保護に関する法律についてのガイドライン(外国にある第三者への提供編)」3 をご参照)、かつ、上記(1)の場合と同様に共同利用の枠組みを利用することができます。

契約は和文でも英文でも構いません。実務的には、新たな内規やプライバシーポリシーを適用することについて現地法人の理解が得にくいために、契約で手当する方法を採用するケースが比較的多いものの、海外のグループ会社の数や所在国によっては、各社に適用される内規や各社のプライバシーポリシーを一括改訂することも、十分検討に値します。グローバルに活動している海外企業の中には、グローバルでのプライバシーポリシーを策定しているところも多く見られます。

(3) まとめ

EU から日本に移転される個人データを日本から外国に再移転する際には、GDPR への対応や十分性認定の動向を把握するだけではなく、日本の法および関連ガイドラインに基づいた検討も欠かせません。越境移転規制について対応未了の場合には、GDPR の施行や十分性認定を待つことなく、速やかに検討に着手することをおすすめいたします。

以 上

---

12 共同利用される個人データの取得当初の利用目的と上記(4)の利用目的の具体的内容によっては、本人の同意を得るべき場合もあります。

13 なお、変更後の利用目的が、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えるような場合には、本人の同意を得る必要があると考えられます(法第 15 条第 2 項)。

14 海外のグループ会社の法人形態やビジネス形態によっては、「外国にある第三者」に該当せず、上記(1)記載の対応で足りる場合もあります。

いしかわ　のりや
石川　智也　　西村あさひ法律事務所　パートナー弁護士
n_ishikawa@jurists.co.jp

2006 年弁護士登録、2017 年ニューヨーク州弁護士登録。データの保護と利活用に関する法制度を専門としており、日本の個人情報保護法、EU 一般データ保護規則(GDPR)を含む、グローバルでのデータ規制への対応について日本企業にアドバイスを多数提供。ドイツでの留学・出向経験があり、欧州の知的財産法、データ規制、E コマース、消費者保護法、ポータビリティ、欧州のデジタルマーケットの統一に向けた動向に詳しく、欧州での M&A も手がける。

かわい　ゆうこ
河合　優子　　西村あさひ法律事務所　弁護士
y_kawai@jurists.co.jp

2006年弁護士登録、2014年ニューヨーク州弁護士登録。個人情報/データ保護法制や電子商取引に関するアドバイスを国内外の企業に多数提供するほか、M&A、組織再編、ライセンス、クロスボーダー取引、コーポレートガバナンス等を含む企業法務全般を幅広く担当。情報法制学会会員。

しらさわ　ひでき
白澤　秀己　　西村あさひ法律事務所　弁護士
h_shirasawa@jurists.co.jp

2016年弁護士登録。M&A のほか、会社法、金商法、株主総会対応、コーポレートガバナンス等を含む企業法務全般を幅広く担当。