

「十分性認定後の日本企業の GDPR 対応」に関する Q&A

ひかり総合法律事務所
弁護士 板倉 陽一郎氏

最初に：移転とは、先方が管理者または処理者の場合であり、相手がデータ主体の場合は移転の問題は起きない。

Q：人材育成サービスを提供しているが、グローバル展開している日本企業の EU 子会社等の従業員満足度調査実施を受託し、当社で EU 従業員のメールアドレスリストの提供を受け、メールを一斉配信して各従業員に回答してもらった場合、適正に個人情報を取得するためには、委託元が EU 子会社との間で何をすれば問題ないか

A：EU 子会社の従業員データを送るために、日本企業が従業員に対しどのような説明がなされているか、処理の根拠は GDPR6 条のうちどの項目としているかを確認しておくことよい（従業員の雇用管理そのものであれば、雇用契約（1 項(b)）を適法化根拠とすることも可能であろう。）

Q：以前の解釈では、EU 内の拠点の有無に関わらず、日本内でデータを処理すると GDPR 対象という認識だったが、EU 内に拠点が無い企業でも、日本人が処理して OK な状況を教えてほしい。

A：ガイドライン案が出て解釈が変わった。条文を素直に読むと、直接適用は拠点の有無に関わらないと読めたが、ガイドライン案でそれぞれの拠点があるかどうかで判断するようになったため、現時点ではそのように解釈してよいであろう。

Q：同意の撤回については保護法でも検討されていると思うが、具体的にどのように対応していくのが良いか？

A：日本法では同意以外の処理方法が明確に定められていないため、同意の撤回が認められてしまうと実務では厳しい状況となる。これに関しては、同意の撤回を認めるのであれば契約に基づく利用を入れる等要請していく必要がある。GDPR では契約による利用を認めており（1 項(b)）、これは一方的には撤回できない。双方合意による契約解除が必要になる。

Q：日本本社が EU 支店在勤者（現地採用なし 顧客拠点での開発・設計業務であり、EU 一般市民の個人データの取扱いなし）の人事管理、給与計算を行っている場合、日本本社は GDPR 直接適用の対象とな

るか。

A：対象となるが、親会社というよりは子会社で行われている処理に対して適用される範囲に含まれるということになる。

Q：GDPRでは、管理者-処理者間の契約に「管理者の書面による指示、またはEU法、加盟国の国内法のみに基づいて処理を行う」ことを定める必要があるが、日本の処理者は日本の国内法に基づいた取り扱いも必要となるか？

令状に基づく情報提供など日本の国内法特有の取り扱いを行った場合、例えば管理者からの書面による指示として「日本法に基づく取扱い」を明記することで対応可能か？

A：日本法の例外処理がEU法上の例外事由に当たる場合はEU法で処理が可能と考えられる。それ以外の場合、データ主体から管理者からの指示として「日本法に基づく取扱い」を入れたとしても、事前にデータ主体に利用目的として通知し処理に同意を得なければ抵触することになってしまう。「抵触する可能性がある」と割り切るのも一つの判断だろう。

外国法と抵触する場合に参考になるものとしては、SOX法と内部通報制度の構築との関係についての29条作業部会意見書（Opinion 1/2006 on the application of EU data protection rules to internal whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, banking and financial crime, WP117, 1 February 2006）がある。

Q：Cookie 利用に関する通知・同意は一般的な記述のみでよいか？あるいは「Cookie A は〇〇に利用」「Cookie B は□□に利用」というレベルで記述する必要があるか？

A：欧州司法裁判所でCookieを争点に行われているPlanet49に関する裁判について、先月出された法務官意見では、Cookieポリシーを用意する等かなり詳細に通知することが求められている。また、CNILは広告に関する通知が不十分としてGoogleに5000万ユーロの制裁金を課しており、現在の流れはかなり丁寧に書くことを求められている。

Q：EUの管理者から匿名加工の委託を受けた日本の処理者が、管理者に加工データを戻す場合、処理者として守るべきルールはあるか？

A：管理者-処理者間の契約に必要な内容はGDPR28条に規定されている。また特別カテゴリーデータを扱う場合は、9条に基づき管理者が同意を取る必要があるため、心配な場合は管理者に確認すると良い。また、加工済みデータを日本から送る場合は個人データではないので、通常のデータとしての扱いで良い。

Q：日本に移転した EU の個人情報を元に、DM を送付する場合気を付ける点は？

A：十分性認定に基づいて移転したデータは、補完的ルールに基づいた取り扱いを行えばよい。ただし、日本法では第三者提供で取得したデータの利用目的は問われないが、補完的ルールにより EU から移転されたデータに関しては元の利用目的を超えて利用することはできないとなっている点に留意が必要となる。

Q：ネット通販で EU の消費者から取得した個人情報の取扱いの注意点は？

A：欧州内のデータ主体に物品を送付するにあたり直接データを取得する場合は GDPR の域外適用となるので（3条2項(a)）、当該処理に関しては GDPR 全体を遵守する必要がある。

Q：EU の管理者からの委託により、日本でデータ処理しそのデータや結果を EU 側に返却する際にも日本⇒EU のデータ移転に関する手続きがあるか、またはしなくてもよい根拠などはあるか？

A：日本法 24 条は個人データを外国にある第三者に提供する場合のことであり、委託に伴う提供は提供にあたるが、委託元に戻す場合が提供にあたるかは不明確。ただし、同等性認定の元では、委託に伴う提供は同意がいらないという解釈になると思われる。

Q：同意の撤回がなされた場合、同意の下で AI の学習等に提供するサービスでは撤回以前の学習結果も使用できなくなる可能性はあるか？

A：あくまでも客体の個人データに関する同意の撤回なので、学習により個人データでなくなったものに対しては権利が及ばない。

Q：会員番号を仮 ID にして処理・分析を行う際に EU（GDPR 対象）の個人データが含まれる可能性がある場合、匿名加工情報の取扱いとして問題があるか？

A：日本では仮 ID をつけた匿名加工情報を認めているが、EU ではデータが集積されることにより追跡可能になる可能性のあるデータは、あくまでも個人データとしての扱いとなる。
仮 ID を削除する、または毎回仮 ID を変更するなどの処理を行ったものに関しては EU も匿名加工情報としての取扱いをとやかく言わないようである。

Q：EU 域内の個人が、日本法人（例えば旅行代理店）の Web サイトから旅行の申し込みをした場合、当該 Web サイトが EU 域内にある場合は（表記等も英文）GDPR は適用されないのでしょうか？

A：日本法人の拠点が EU 域内にあれば直接適用となり、日本法人の拠点が EU 域内になくサーバーのみが置かれている場合は、GDPR3 条 2 項(a) (b) に該当すれば域外適用となる。

Q：EU 内に拠点はあがるが、直接営業行為を行っていない場合に、GDPR で留意すべき点はあるか？

A：拠点での活動に関連する個人データの取扱いがない場合は、GDPR 適用外となる。

Q：十分性認定に基づく移転の場合、第三国への再移転の根拠として「EU から見て適法な移転先かどうかは無関係」とあるが、従来方式（SCC や BCR による移転など）の場合は、これは当てはまらないという理解で良いか（例：プライバシーシールドの参加企業に対するデータ再移転）

A：SCC (SDPC) に基づく移転で来たデータは補完的ルールの対象とはならないが、保護法 24 条、規則 11 条の 2 が適用されるのであって、再移転先がプライバシーシールドに参加しているかどうかは関係がない。

Q：日本法24条により移転が可能ということは、EU 十分性認定がない国・地域への再移転も可能か？

A：日本が EU の十分性認定を持たない国を同等性認定すれば、24 条により移転可能となる。その際に、その国が GDPR に対応しているかどうかは関係がない。

Q：Cookie を用いたプロファイリングは可能か？

A：GDPR3 条 2 項(b)に該当するため、GDPR の域外適用となる。

Q：十分性認定、標準データ保護約款、BCR 等それぞれの根拠による越境移転のメリット・デメリットを教えてください。

A：十分性認定の最大のメリットは個別の事業者が何もせずとも移転ができるということ。ただし移転さ

れた後の上乘セルールが厳しい場合は充分性認定による移転は向かない。SCC のメリットは書けばよいこと、ただし移転元の法律に準拠するため法律が良く分からない国では難しい。また、処理ごとに締結しなければならない点が煩雑になる。BCR のメリットは、充分性のような上乘セルールがなく、グループ企業間でデータのやり取りができる点。デメリットは取得までの時間と費用。

Q：企業グループ内で EU、日本、それ以外の国（米国等）の拠点で例えば顧客データを相互に移転している場合の対応の実務的なヒントについて

A：データ移転を行う前にスキームを固めることが重要。最初にどういった処理になるかを整理し、それに対して同意を取得すればそれ以上の負荷はかからない。後からいろいろな根拠に基づき移転しようとするとなりがかかることになる。

以上