EU GDPR（一般データ保護規則）の概要

西村あさひ法律事務所 パートナー　岩瀬 ひとみ

日本では、2017年５月に改正個人情報保護法が全面施行となったが、近時の経済のデジタル化の急速な進展や、それに伴うビッグデータの利活用の進行を背景として、個人情報保護の法制は、日本以外の諸外国でも大きく動いている分野の一つである。世界的にみても最も厳しいといわれる欧州のデータ保護法（1995年に採択されたEUデータ保護指令95/46/ECに基づく各国法）を統一して書き換えることとなるGDPR（General Data Protection Regulation：一般データ保護規則）が2018年５月25日に施行となる。

GDPRは、EU域内（厳密にはEU加盟国及びEEA加盟国）の事業者と国民だけでなく、EU域外の事業者にも適用され得るものである。新たに導入された、最高額2000万ユーロ又は全世界年間売上の４％のいずれか高い方という非常に高額の制裁金の定めもあるせいか、近時、新聞等で取り上げられることも増えてきたが、施行を目前とした現在でも十分な対応ができていない企業は少なくなく、またGDPRについて正しく理解がされていないことも珍しくない。本稿では、GDPRが何を求めているのか、その概要をできるだけわかりやすく説明することを試みたい。実際のGDPRの遵守対応は、各企業の事業内容、組織構成、取り扱うデータやその流れなどによって大きく異なるが、その前提として正しくGDPRを理解することの一助となれば幸いである。

１．GDPRの制定

EU加盟国において、個人データの保護は、欧州基本憲章において定められた基本的権利の一つとされており、GDPRもこの基本的権利を保護するための法律である。GDPRは、2012年１月に欧州委員会により最初の規則案が提案されてから４年以上もの間議論が行われた後、2016年４月に最終案が採択され、2018年５月25日から施行されることとなっている。GDPR施行前は、1995年10月に採択されたEUデータ保護指令（Directive 95/46/EC）に基づき、EU加盟国各国において個人データの保護に係る国内法が制定されているという状況である。各国のデータ保護法は、データ保護指令に基づいているため一定程度内容の統一は図られているものの、国によって異なるため、EU域内の複数国にまたがって事業を展開する企業にとって欧州のデータ保護法遵守は、異なる各国の法律に個別に対応する必要があるという意味で負担が重いものであった。GDPRは、EUデータ保護指令とは異なり、EU加盟国において直接適用され、各国のデータ保護法は廃止されることとなるため、GDPR施行後はデータ保護のルールがEU域内で統一されることとなる（なお、労働者の個人データの処理に関する規定、データ保護オフィサーの設置基準に関する規定、未成年者の年齢基準に関する規定、健康関連データに関する規定など、加盟国が独自に定めることのできる項目もあるため、その限りでは完全に統一されるものではない点には留意が必要である）。

1995年にデータ保護指令が採択されて以降、社会経済のデジタル化やグローバル化が急速に進み、新しい技術やビジネスモデルが登場するなか、古いルールの下では個人データの処理についてEU加盟国の国民の信頼を得られなくなってきたことから、これらの状況の変化に対応するルールが必要であるということで制定されたのがGDPRである。従って、GDPRではデータ保護に関する義務が強化され、またその適用範囲も拡大されている。

２．GDPRの適用範囲

冒頭にも記載したとおり、GDPRはEU域外の事業者にも適用され得るものである。すなわち、GDPRは、まず、①EU域内の管理者（controller）又は処理者（processor）の拠点（establishment）の活動に関連して行われる個人データの処理に適用される（管理者、処理者の概念については後述）。また、GDPRは、②

EU域内に拠点を有さない管理者又は処理者によるEU域内に所在するデータ主体の個人データの処理についても、処理活動が、(a)EU域内に所在するデータ主体に対する商品又はサービスの提供か、(b)EU域内で行われるデータ主体の行動の監視に関するものであれば適用されると規定されている。

このうち②がいわゆる域外適用であり、GDPRの適用範囲を広くするものと説明されることが多いが、①に関し「拠点」が広い概念であることも忘れてはならない。すなわち、この「拠点」は、EU域内において、安定的な仕組みを通じて、実効的かつ現実の活動が実施されていれば、拠点であると判断される。従って、日本企業がEU域内に支店を有する場合のみならず、EU域内に子会社を有していれば、親会社である日本企業が上記①によりGDPRの適用対象となることが多いであろう。また、支店や子会社の形でなくとも、業務遂行できるオフィスとともに駐在員がEU域内にいるという場合にも拠点ありということで上記①によりGDPRの適用対象となる可能性がある。なお、②の域外適用の場合はもともとEU域外でのデータ処理が想定されているが、①の場合も、データ処理がEU域外でなされたとしてもGDPRの適用はある。

上記②の域外適用については、例えば、EU域内から日本に出張したり旅行している者について日本でサービスを提供すれば上記②(a)に該当するのではないかと誤解がされていることがあるが、その出張・旅行をしている者はEU域内に所在するデータ主体ではないため、上記②(a)には該当しないと考えられる。上記②(a)で想定されているのは、例えば、日本企業がウェブサイトを設けてEU域内にいる者に対して商品を販売したりサービスを提供したりするような場合である。インターネットは国を超えてアクセスできるものであるため、どのような内容であればEU域内にいる者に対して商品やサービスが提供されているとされるかは必ずしも明確でないが、EU域内にいるデータ主体に対して商品やサービスを提供する意図が明白である場合にはGDPRが適用されると考えられており、EU域内で一般的に使われている言語又は通貨を使用していたりすれば該当する可能性は高くなるといえる。上記②(b)の行動の監視は、例えば、ウェブサイト上の行動履歴や購買履歴の追跡、自動車や家電の使用状況の把握をするような場合にはこれに該当する可能性がある。

なお、GDPRでは、日本の個人情報保護法と異なり、データ処理に関する義務を負う者として「管理者(controller)」と「処理者（processor)」という２つの概念が用いられている。管理者とは、単独で又は他の者と共同して個人データの処理の目的（日本の個人情報保護法における利用目的に相当するもの）及び手段を決定する者であり、処理者とは、管理者のために個人データの処理を行う者である。処理者は、データ処理サービスを提供するベンダーなどがこれに該当するが、日本企業（親会社）がEU域内にある子会社や関連会社の従業員データを受領してこれに関してバックオフィス業務を行うような場合には処理者に該当することがあろう（なお、親会社が、さらに自らの目的のために当該従業員データを利用する場合には処理者ではなく管理者となる)。

３．GDPR上の義務の概要

GDPRの関連では個人データの域外移転に注目が向けられていることが多いという印象を受ける。これまでの欧州のデータ保護法関連の実務において、日本企業が行ってきた対応が主に標準契約条項（Standard Contractual Clause：SCC）の締結であったということがその要因の一つかもしれないが、GDPRには個人データの域外移転以外にも重要な事項が定められており、GDPRの適用を受ける日本企業はそれを正しく理解しておく必要がある。

GDPRは、基本的権利である個人データの保護に関する法律であり、個人データの処理とEU域外への移転に際しての管理者及び処理者の義務と法執行のルールを定めている。以下ではGDPRの適用を受ける日本企業として理解しておくことが重要な管理者及び処理者の義務を中心に説明する。この義務は、大きく分けると、①組織的な措置、②データ処理及び域外移転に関するルール、③データ主体の権利（データ主体から求められたときに応じなければならない事項）からなる。

（1） 組織的な措置

GDPRの適用を受ける企業は、データ処理活動の記録を保存し、適切かつ合理的な技術的・組織的保護措置を講じ、個人データの侵害があった場合に必要とされる通知を行えるようにしておくなど、GDPRの規定に従った社内の体制を整えておく必要がある。また、データ保護オフィサー（所定の基準を満たす場合）や、代理人（GDPRの域外適用を受ける場合）を選任し、

さらに、個人データの処理活動の内容によっては、データ保護影響評価を行い、プライバシー・バイ・デザインやプライバシー・バイ・デフォルトの原則に適合する措置を講じる必要がある。以下では、GDPRの適用を受ける企業が行う必要のある組織的な措置のうちの主要なものについて説明する。

データ処理活動の記録

GDPRにおいては、管理者及び処理者（あるいはその代理人）は、データ処理活動の記録を保存しなければならないとされている。記録の内容は、管理者・処理者の名前及び連絡先、データ処理の目的、データ主体の種類、個人データの種類等と具体的に定められており、これを書面（電子的な形でもよい）により保存する必要がある。最も基本的な組織的措置であり、監督当局からこの記録の開示を求められた際にこれに応じられなかった場合にはGDPR上の基本的な措置が講じられていないということになるため、留意が必要である。なお、従業員が250名未満の小規模事業者については適用が除外されることがある。

データ保護影響評価（Data Protection Impact Assessment：DPIA）

データ保護影響評価とは、体系的かつ広範なプロファイリング（個人的な側面を評価するために、特に個人に関する分析又は予測をするためになされる、個人データの自動化された処理）又はセンシティブデータの大規模処理を行う場合など、自然人の権利及び自由に対して高度の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、これに先立って実施しなければならない当該データ処理活動のリスク評価である。GDPRで新たに導入された。具体的にどのようなデータ処理活動が「自然人の権利及び自由に対して高度の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」に該当しDPIAの対象となるか、DPIAの実施方法などについては、ガイドラインが制定されている。ガイドラインでは、自然人の権利及び自由に対して高度の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に該当するか否かの判断基準として、①評価又は採点、②法的又は同種の重大な影響を伴う自動化された意思決定、③体系的なモニタリング、④センシティブデータ又は高度に個人的な性質を有するデータ、⑤大規模なデータ処理、⑥データセットの照合又は結合、⑦脆弱なデータ主体に関するデータ、⑧新しい技術的若しくは組織的なソリューションの革新的な利用又は適用、⑨データ主体が権利行使し、サービスを受け又は契約を締結することを妨げる可能性のあるデータ処理という９つの基準（原則として、このうちの２つ以上に該当すれば、自然人の権利及び自由に対して高度の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に該当する。もっとも、１つしか該当しなくてもDPIAが必要な場合もあり得る）と、当てはめの具体例が示されている。これによれば、例えば、企業が従業員の職場やインターネット上の活動を体系的に監視する場合や、プロフィールを作成するためのソーシャルメディアデータの収集などがDPIAが必要な具体例として上げられている。なお、データ処理に先立って監督当局との協議が義務付けられる場合がある。

データ保護オフィサー（Data Protection Officer：DPO）の選任

管理者及び処理者は、その主要業務に、大規模なデータ主体の定期的かつ体系的な監視が含まれる、あるいは、センシティブデータの大規模な処理が含まれる場合にはDPOを選任しなければならないとされている。EU加盟国の国内法でDPOを選任すべき場合が追加的に定められることもある点には留意が必要である。DPOに関してもガイドラインが公表されており、DPOの選任、地位、任務等の詳細が示されている。DPOは、GDPR及び各国のデータ保護法の遵守について監視し、通知・助言をし、また監督当局などとのやりとりも行うこととなるため、データ保護法とその実務について専門的知識を有するとともに、必要に応じて現地の言語でコミュニケーションができる必要があろう。DPOは従業員のなかから選任することもできるが、外部委託することも可能である。独立性が保障されており、業務遂行によって解雇又は処罰を受けないとされていることもあり外部委託の形をとる企業もある。なお、企業グループの場合は、グループで共通のDPOを１名選任するということも認められる。

EU域内に拠点を有さない管理者・処理者の代理人の選任

上記２の②に記載した域外適用を受ける管理者及び処理者は、所定の例外に該当しない限り、EU域内の代理人を書面により選任しなければならない。代理人は、データ処理に関して監督当局やデータ主体とのやりとりの窓口となる。

個人データの侵害の通知

GDPRにおいては、個人データの侵害、すなわち、

偶発的又は違法な個人データの破壊、滅失、変更又は許可されていない開示若しくはアクセスがあった場合には、管理者は、原則として、侵害を認識してから72時間以内に監督当局に通知しなければならないとされている（ただし、侵害により自然人の権利又は自由に対するリスクが生じる可能性が低い場合、通知は不要とされている）。管理者が個人データの処理を処理者に委託している場合、処理者が侵害を認識すれば管理者も認識したとみなされる点には留意が必要である。また、侵害により自然人の権利又は自由に対するリスクがある場合には、遅滞なくデータ主体に通知することも必要である。監督当局への通知は72時間というかなり短時間での対応が求められているため、データ侵害が起きたときにその事実について速やかに把握することができるよう体制を整えておく必要がある。なお、この個人データの侵害の通知に関してもガイドラインが公表されている。

適切な技術的・組織的保護措置の実施

日本の個人情報保護法における安全管理措置に相当するものであり、管理者及び処理者の基本的な義務の一つである。リスクに適した安全性のレベルを確保するために適切かつ合理的な技術的・組織的保護措置を講じなければならない。

プライバシー・バイ・デザイン（Privacy by Design）、プライバシー・バイ・デフォルト（Privacy by Default）の原則

いずれも、技術の進展を踏まえてGDPRにおいて新たに導入された概念であり、とりわけデジタルデータの処理に関して、これらの原則に適合する措置を講じなければならないというものである。プライバシー・バイ・デザインは、個人データの処理を含む商品やサービスを提供するに際して、その設計段階から、必要最小限度でのみ個人データを処理するなど適切な個人データの保護措置を組み込むべきという原則であり、プライバシー・バイ・デフォルトは、初期設定においてそのような措置をとるべきという原則である。なお、監督当局がこれらをどのように執行するかは明らかでない。

（2）データ処理及びデータの域外移転に関するルール

データ処理のルール

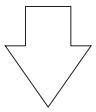
日本の個人情報保護法は、個人情報取扱事業者に対して、個人情報を取り扱うに当たって利用目的を特定し、取得に際して利用目的を本人に通知又は公表すること、また、個人データの第三者提供に当たっては原則として本人の同意を取得することといった形で、比較的具体的に行為規制を定めている。これに対して、GDPRにおいては、個人データの収集、記録、編集、構造化、保存、修正又は変更などあらゆる作業が、個人データの「処理」として一括りにされたうえ、個人データの処理は原則として禁止されており、適法性（legal justification）が認められる場合にのみできる、と定められている。この適法性は、以下の場合に認められる。

①データ主体が、一または複数の特定の目的のために、自己の個人データの処理に同意をした場合
②データ主体が当事者となっている契約の履行のために処理が必要な場合、又は、契約の締結前にデータ主体の求めに応じて手続きをするために処理が必要な場合
③管理者が従わなければならない法的義務を遵守するために処理が必要な場合
④データ主体又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公共の利益又は管理者に与えられた公的権限の行使のために行われる業務の遂行において必要な場合
⑥管理者又は第三者によって追求される正当な利益のために処理が必要な場合（ただし、データ主体の個人データの保護を求める利益又は基本的権利及び自由が当該管理者等の利益に優先する場合を除く）

実務上は、これらのうち①②⑥に依拠する場面が多いのではないかと思われるが、①に関しては、同意が自由に与えられ、特定の、情報提供を受けたうえでの、かつ不明確でない意思表示である必要があることから、どういう状況下であれば同意が任意・自発的になされたか、ケースバイケースで検討する必要がある。特に、従業員の個人データに関しては、従業員が使用者に対してする同意は任意性がないということで、データ処理の適法性として同意には依拠できないと考えられている点には留意が必要である。⑥の正当な利益についても、データ主体の個人データの保護を求める利益又は基本的権利・自由と、管理者などの利益とを、個別に利益衡量（こうりょう）することが必要であることから、判断は容易ではなく、慎重な判断が求められる。現行のデータ保護法下においても存在していた概念であり、過去事例が参考になるようであるが、実務上は弁護士の意見を取得することもあるようである。

個人データの「処理」には、適法性（legal justification）が認められる必要

- 同意
- 契約の履行等のために必要
- 正当な利益　等



個人データの「域外移転」には、さらに、データ移転のための要件を満たす必要

- 十分性認定
- SCC
- BCR
- 明確な同意　等

データのEU域外への移転に関するルール

日本の個人情報保護法では、個人データの国外移転に関しては、外国にある第三者に個人データを提供する場合に原則として同意が必要とされており、外国にある支店に個人データを移転する場合は同一の法人内であるから第三者への提供には当たらず、同意取得は不要とされている。これに対して、GDPRにおいては、同一法人格内であるか否かを問わず、個人データがEU域外の第三国に移転する場合には域外移転規制が及ぶ。なお、EU域内のサーバに保管した個人データに第三国からアクセスを許す場合もまた域外移転として規制対象となる。

GDPRにおいては、個人データの域外移転は、基本的に、以下のいずれかの方法により正当化された場合にのみ認められる（ただし、一定の例外事由は定められている）。なお、この適法化要件は、前述したデータ処理に関する適法性に加えてさらに必要なものである。

①欧州委員会が、移転先である第三国について十分な水準の保護が確保できていると認定している場合（十分性認定）
②標準契約条項（SCC）の締結
③拘束的企業準則（Binding Corporate Rules：BCR）の策定
④承認された行為規範（Code of Conduct）
⑤データ保護認証制度（Data Protection Certification Mechanisms）
⑥明確な同意の取得

このうち、④行為規範と⑤データ保護認証制度は、まだその詳細が明らかになっていない。③BCRは、これを利用する日本企業も出てきているものの、グループ企業間に限定される上、策定に時間とコストを要することから、利用事例はそれほど増えていないように思われる。

実務的にもっともよく利用されるであろう②SCCについては、今後GDPR下でのSCCが公表されることが想定されているが、それまでは現行法下におけるプラクティスが継続すると思われる。⑥の同意は、前述したとおり、自由に与えられ、特定の、情報提供を受けたうえでの同意であることに加えて、明確な同意である必要があり、少なくとも従業員の個人データの域外移転は同意に依拠すべきでないと考えられている。

①の十分性認定については、日本は現在これを受けるべく欧州委員会との間で交渉を行っているようである。仮に日本が十分性認定を受けたとしても、それに基づいて日本に移転される個人データについてはその取り扱いについてガイドラインが策定される見込みであり、2018年４月25日よりガイドライン案がパブコメに付されている（http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=240000050&Mode=0 参照。なお、当該ガイドラインは2018年前半に公布・施行が予定されているようである）。具体的には、GDPRにおける個人データの保護水準のほうが、日本の個人情報保護法における個人情報ないし個人データの保護水準より高いと考えられる、①要配慮個人情報（いわゆるセンシティブデータ）の範囲、②保有個人データの範囲、③利用目的の特定、利用目的による制限、④外国にある第三者への提供の制限、⑤匿名加工情報の範囲などについて規定されることが想定されている。なお、日本が十分性認定を受けたとしても、それはEU域内から日本への個人データの移転についてのみ適法化するものであり、データ処理をするに当たっては別途適法性が認められる必要があることは言うまでもない。

個人データの国外ないし域外移転に関しては、上述した日本の個人情報保護法、GDPR以外にも、香港、豪州、シンガポールなどにも規制があり、その他の国でも類似の規制を設けるところが増えてきている。規制の内容は国ごとに異なるため、複数国にまたがって事業を行っている企業においては、これら規制の有無・内容を確認し対応することが必要である。

また、個人データの国外ないし域外移転とは別に、これと似て非なる規制として、データ・ローカライゼーションというものがある。データ・ローカライゼーションとは、データを国内に保存しなければならないとい

う規制である。プライバシー保護というよりは、国家の安全保障、自国産業保護、法執行・犯罪捜査などの目的で設けられており、対象データは個人データに限られない。最近では、中国のインターネット安全法が話題になった。本稿の主題からは外れるため詳細は割愛するが、海外に事業を展開している企業においては、GDPRその他外国の個人情報保護法制のみならず、データ・ローカライゼーションの規制にも留意する必要がある。

（3）データ主体の権利

GDPRは、データ主体の権利としてさまざまな権利を定め、その詳細について規定している。具体的な権利としては例えば以下のようなものがある。

①情報に関する権利
②アクセス権・消去権・訂正権・処理の制限に関する権利
③異議を唱える権利
④データポータビリティの権利

①の情報に関する権利は、管理者が個人データを収集又は取得する場合に、DPOの連絡先、データ処理の目的・法的根拠、同意をいつでも撤回できる権利があることなど一定の情報をデータ主体に提供しなければならないというものである。日本の個人情報保護法下にも個人情報取扱事業者の義務として類似の定めがあるが、GDPRにおいてはより広範な情報が提供される必要があり、また、提供の仕方についても詳細な定めが置かれている。

②や③の権利も、日本の個人情報保護法にも類似の権利が定められているが内容は異なるところがある。例えば、消去権は、一定の場合に、データ主体に関する個人データを消去することを求める権利であるが、管理者が個人データを公開している場合には、利用可能な技術及び費用を考慮して、当該個人データを処理している他の管理者に対して、データ主体が当該個人データのあらゆるリンク又は写し若しくは複製の消去を求めている旨を通知するために合理的な手段を講じなければならないとされている（これを含むため「忘れられる権利」とも呼ばれる）。

④データポータビリティの権利は、データ主体が、管理者に提供した当該データ主体にかかる個人データについて、構造化され一般的に利用され機械可読性のある形式で受け取る権利と、当該個人データを個人データが提供された管理者の妨害なく他の管理者に移行することができる権利であり、GDPRで新たに設けられたものである。日本の個人情報保護法では類似の権利は定められていない。管理者は、データポータビリティの権利があることをデータ主体に知らせなければならないとも規定されている。一般的には、ソーシャルネットワーキングサービス（SNS）などにおいて、あるSNSから別のSNSに乗り換えることができるというように説明されることがあるが、雇用関係において、雇用契約終了に際して従業員から当該従業員に関する個人データについてこの権利が行使されることがあり得る点に注意が必要である。

企業としては、GDPR上のデータ主体の権利を理解し、権利が行使された際に対応できるよう体制を整えておく必要がある。

4．まとめ

以上、GDPRの適用を受ける日本企業として理解しておくことが重要な管理者及び処理者の義務を中心にGDPRの概要を簡単に整理・説明した。冒頭に記載したとおり、GDPRには、高額の制裁金の定めがある。すなわち、違反累計に応じて、上限が、1000万ユーロ若しくは前会計年度における全世界売上高の２％のいずれか高額のほう、又は、2000万ユーロ若しくは全会計年度における全世界売上高の４％という高額の制裁金を課すことできることとなっている。この制裁金の額の決定に際しては、違反の性質・重要性・期間、故意又は過失、データ主体の被った損害を軽減させるために採られた行動、過去の関連する違反行為などのファクターが考慮される。また、GDPRを遵守する企業はGDPRを遵守できていない企業との取引を避けることになるため、制裁金のリスクもさることながら、遵守できていないことによる企業の競争力への影響のほうが重大であろうとの指摘もある。多額の制裁金を課されないためにも、また、競争力を失わないためにも、欧州が関係し得る日本企業で、GDPRの遵守に向けた検討・対応を開始していない企業は、これら検討・対応に着手することが重要であろう。

（2018年５月21日記）

＊本稿は、2018年２月19日開催のJOIセミナーを一部記事化したものです（共催：西村あさひ法律事務所、Taylor Wessing法律事務所、後援：JBIC）。