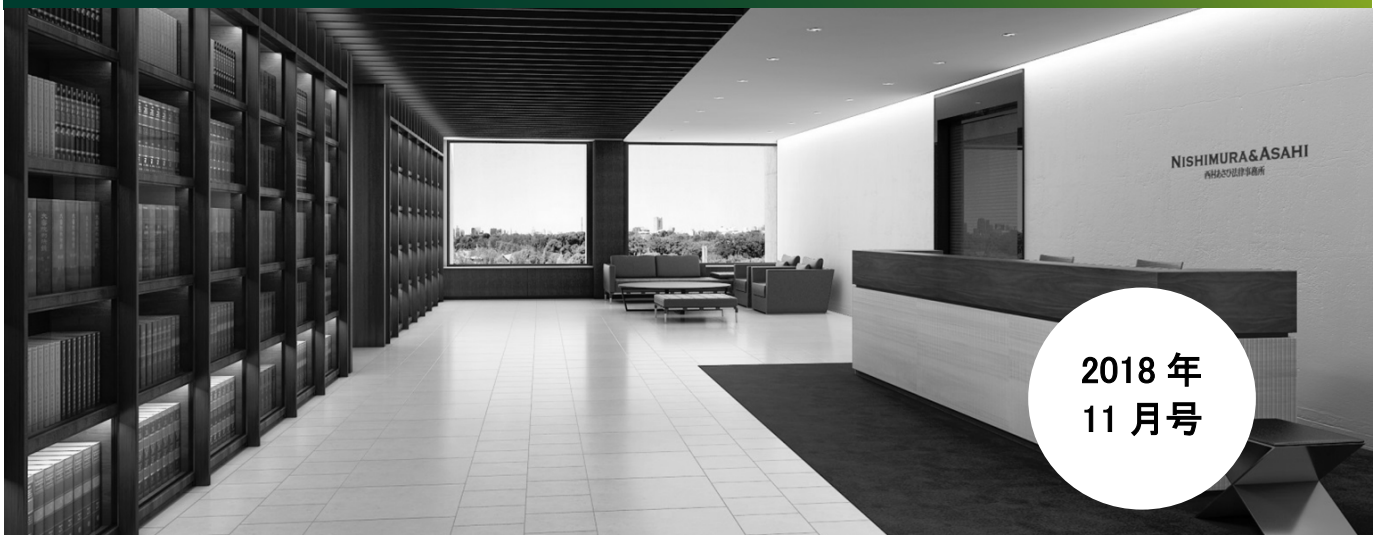
西村あさひ法律事務所
NISHIMURA & ASAHI
企業法務ニューズレター



GDPR 適用の地理的範囲に関するガイドラインの公表

執筆者:石川 智也、菅 悠人

2018 年 11 月 23 日、欧州データ保護評議会(European Data Protection Board。以下「EDPB」といいます。)より、GDPR が適用される地理的範囲と、域外適用を受ける場合に選任することが義務付けられる EU 代表者について解説した「地理的範囲についてのガイドライン」(以下「本ガイドライン」といいます。)[1]が公表されました。本ニューズレターでは、本ガイドラインの内容について解説いたします。条数については、特段の断りのない限り、全て GDPR の条文を指します。

なお、本ガイドラインは、本ニューズレター公表日時点では、2019 年 1 月 18 日までパブリックコメントに付されることが予定されており[2]、その結果を踏まえて今後変更があり得るものであることにご留意ください。また、本ガイドラインに、自社で想定している個人データの処理についての判断基準・具体例がない場合には、パブリックコメントの手続を通じて意見や質問を提出することで EDPB に明確化を求めるということも考えられます。

I. 日本企業にとっての本ガイドラインの重要性

地理的範囲は、ある個人データの処理が GDPR の適用対象となるか否かを決めるためのものです。日本企業が GDPR 対応を行う範囲を決定するに当たっては、この地理的範囲を踏まえて GDPR の適用対象となる個人データの処理を確定する必要がありますが、本ガイドラインは、これまで必ずしも明確ではなかった論点について解釈基準を示すものとなっていますので、GDPR 対応を行う日本企業にとっては、検討することが必須の資料であるといえます。また、具体例が多く紹介されていますので、理解の助けになることが期待されるとともに、EDPB がどのような業種・データ処理での GDPR 対応に注目しているのかを窺い知ることができます。

既に GDPR の適用範囲を整理して GDPR 対応に取り組んでいる企業においては、その整理が正しいかを確認するために、ま

[1] 採択は 2018 年 11 月 16 日。Guidelines 3/2018 on the Territorial Sscope of the GDPR (Article 3) – Version for Public Consultation.

[2] https://edpb.europa.eu/our-work-tools/public-consultations/2018/guidelines-32018-territorial-scope-gdpr-article-3_en

た、これから GDPR 対応を検討する企業においては、対応が必要な範囲を確定するために、本ガイドラインを活用するべきであると考えられます。以下では、地理的範囲(下記 II.)、EU 代表者[3](下記 III.)について本ガイドラインの要点を説明した上で、本ガイドラインで紹介されている具体例を踏まえて、業種別に特に注目すべきポイント(下記 IV.)を紹介します。

II. 地理的範囲(Territorial Scope)

GDPR においては、①個人データの処理が EEA 域内の拠点の活動に関連する(in the context of)[4]場合(下記 1.)か、②EEA 域内にいるデータ主体に対する商品もしくは役務の提供(有償か否かを問わない。)、または、EEA 域内で行われるデータ主体の行動の監視に関連して個人データの処理を行う場合(下記 2.)に GDPR が適用されます。

以下ではこの地理的範囲の枠組みを前提に本ガイドラインの内容を説明します。GDPR の条文から理解できる地理的範囲の考え方については、既に当事務所のニューズレターでも紹介しており[5・6]、本ガイドラインの公表後も参照できる内容となっていますので、そちらもご参照ください。

1. 拠点基準(Establishment Criterion)の適用(3 条 1 項)(本ガイドライン 4～12 頁)

GDPR は、個人データの処理が EEA 域内で行われるか否かを問わず、管理者[7]または処理者[8]の EEA 域内の拠点の活動に関連する個人データの処理に適用されます(3 条 1 項)。この点について、本ガイドラインでは以下の 3 ステップに分けて検討することを推奨しています。

① EEA 域内の拠点
② 拠点の活動に関連して行われる個人データの処理
③ その個人データの処理が EEA 域内で行われるか否かを問わない

以下では、日本企業による検討に際して問題となることが多い①と②について説明した上で(下記(1)(2))、処理者に 3 条 1 項に基づいて GDPR が適用される場面について説明します(下記(3))。

(1) EEA 域内の拠点(本ガイドライン 4～6 頁)

「拠点」とは、安定的な仕組みを通じて行われる実効的かつ現実の活動を示唆するものをいい、支店または法人格を有する子会社を通じて行われるかなど、その仕組みの法的形式は決定的要素ではありません(前文(22)項)。

本ガイドラインでは、GDPR の前文に示されたこの「拠点」の考え方を確認した上で、旧データ保護指令の下で出された欧州司法裁判所の判決によって「拠点」の概念が広げられてきたことを説明しています。そして、それらの判決を参照して経済活動の性質と問題となっているサービスを踏まえた上で、EEA 域内での仕組みの安定性と処理の実効性の程度を考慮して EEA 域内に拠点があるか否かを決定する必要があるとしています。その結果として、特にオンラインサービスの提供の文脈では、EEA 域外にある企業の従業員またはエージェント 1 名であっても、仕組みの安定性としては十分な場合がある(つまりは、拠点になる可能性が

---

3 EU 代理人と訳されることもありますが、同じものを指します。

4 「拠点の活動の過程で」と訳されることもあります。

5 石川智也＝河合優子＝白澤秀己「GDPR 対応と日本のデータ越境移転規制対応の実務」企業法務ニューズレター2018 年 2 月号

6 石川智也「日本企業のウェブサイトにおける GDPR 対応」ヨーロッパニューズレター2018 年 7 月号

7 管理者とは、大要、単独でまたは他の者と共同して、個人データの処理の目的および方法を決定する者を意味します(4 条(7)号)。

8 処理者とは、大要、管理者の代わりに個人データを処理する者を意味します(4 条(8)号)。

ある。）としています。

実務的には、EEA 域内にある子会社、支店または現地事務所は「拠点」に当たる場合があると考えられます。事務所すら構えていない場合には、上記観点からケースバイケースで判断すべきということになります。

(2) 拠点の活動に関連して行われる個人データの処理（本ガイドライン 6～8 頁）

いかなる場合に拠点の活動に関連しているといえるかについて、本ガイドラインは旧データ保護指令の下で出された欧州司法裁判所の判決に照らして理解するべきであるとし、EU 域内において商業的活動が存在するだけで、（EEA 域外にある管理者または処理者が）EU のデータ保護法の適用を受けるべきではないとしています。そのため、EEA 域内に子会社、支店または現地事務所があるというだけで、親会社・本社である日本企業における個人データの処理に GDPR が適用されるわけではありませんし、適用される場合もあくまで拠点の活動に関連する個人データの処理についてのみ GDPR が適用されると考えられます。

その上で、本ガイドラインは、(i)EEA 域内の拠点の活動と、EEA 域外の管理者または処理者によるデータ処理の活動が密接に関連している（inextricably linked）場合には、EEA 域内の拠点がデータ処理に関して役割を担っていなくても、EEA 域外の管理者または処理者のデータ処理に GDPR が適用されるとしています。また、(ii)EEA 域外の管理者または処理者のデータ処理により、EEA 域内の拠点において売上が生じる場合には、EEA 域内の拠点の活動に関連して EEA 域外の管理者または処理者のデータ処理がなされたことを示唆するものであり、当該データ処理に GDPR が適用される可能性があるとしています。そして、評価の方法としては、以下のような手順が推奨されています。

① （EEA 域外において）個人データの処理がなされているか
② その個人データの処理活動と、EEA 域内における拠点の活動との間に潜在的な関連があるか。もしある場合には、上記(i)(ii)の要素に照らして評価する必要がある

実務的には、何を以て密接な関連があるとするかの判断は容易でありませんが、たとえば、日本企業が EEA 域内の子会社から顧客や取引先に関する情報の移転を受け、自社のために保管する行為については、その保管行為と EEA 域内の子会社の活動との間に密接な関連があるとまではいえないことから、GDPR が適用されるとは考えないのが通常であると思われます。

なお、3 条 1 項に基づいて GDPR が適用される場合には、データ主体が EEA 域内にいるか否かにかかわらず、あらゆる個人に係る個人データに GDPR が適用されることが明確にされています [9]。この点は、下記 II.2.において述べる標的基準の適用に基づいて GDPR が適用される場合と異なります。このため、例えば、フランスに本拠を置く会社がモロッコ・アルジェリア・チュニジアのみで利用可能なアプリを提供する場合であっても、かかる提供に関して行われる個人データの処理が当該フランスの会社によって行われる限り、フランスの拠点に関連して処理が行われる場面に該当するため、GDPR が適用されることになります [10]。

(3) 処理者による個人データの処理に GDPR が適用される場合（本ガイドライン 9～12 頁）

本ガイドラインは、3 条 1 項に基づいて処理者による個人データの処理に GDPR が適用されるのは、処理者が自身の EEA 域内の拠点に関連して個人データの処理を行う場合であり、EEA 域内の管理者から個人データの処理の依頼を受けることのみを理由として、処理者による個人データの処理に GDPR が適用されるわけではないことを明確にしています。その上で、本ガイドラインは、EEA 域内の管理者が、EEA 域外の処理者を用いて個人データの処理を行う場合について説明していますが、この点は日本企業にとって非常に重要な点ですので、下記 IV.1.において別途詳細に説明します。

次に、EEA 域外の管理者が、EEA 域内の処理者に対して個人データの処理を依頼する場合については、両者に特段の関係が

9 本ガイドライン 9 頁。

10 本ガイドライン 8 頁。

ない限り、EEA 域外の管理者は自らの拠点の活動に関連して個人データを処理することにはならないとされています。すなわち、EEA 域内の処理者は、EEA 域外の管理者が EEA 域内に有する拠点とはみなされず、当該処理者へ個人データの処理を依頼したことのみを理由として管理者に 3 条 1 項が適用されることはないというのが原則です。ただし、当該 EEA 域外の管理者が EEA 域内に自らの拠点（例えば駐在員事務所）を有している場合には、当然のことながらその拠点の活動に関連する個人データの処理には 3 条 1 項が適用されます。また、EEA 域内に拠点を持たない管理者が EEA 域内の処理者へ個人データの処理を依頼した場合、管理者に 3 条 1 項の適用はないとしても、下記 II.2.で述べる 3 条 2 項の適用を受けるかについては別途確認する必要があります。なお、これらいずれの場合も、EEA 域外の管理者から処理の依頼を受けた処理者は、EEA 域内に拠点を有する限り、3 条 1 項の適用を受けます。

2. 標的基準（Targeting Criterion）の適用（3 条 2 項）（本ガイドライン 12～18 頁）

日本企業を含む EEA 域外にある企業でも、EEA 域内にいるデータ主体に対する商品もしくは役務の提供（有償か否かを問わない。）、または、EEA 域内で行われるデータ主体の行動の監視に関連して個人データの処理を行う場合には、GDPR が適用されます（3 条 2 項）。

本ガイドラインは、EEA 域外にある企業が GDPR の域外適用を受ける場合にはワンストップショップ [11]の仕組みの適用がないこと、および、GDPR 以外の EU または EEA 加盟国の法制についても考慮に入れる必要があることについて述べた上で、EEA 域内にいるデータ主体（下記(1)）、EEA 域内にいるデータ主体に対する商品または役務の提供（下記(2)）、EEA 域内で行われるデータ主体の行動の監視（下記(3)）の意義について、それぞれ説明しています。

(1) EEA 域内にいるデータ主体（本ガイドライン 13～14 頁）

本ガイドラインは、3 条 2 項の域外適用の有無の判断に当たっては、データ主体の国籍等は関係なく、商品もしくは役務の提供または行動の監視が行われる時点において EEA 域内にいるデータ主体に向けられているかが問題であることを明らかにしています。

たとえば、EEA 域内の居住者が日本に来た際に日本で個人データを取得したとしても、その個人データの処理に GDPR が適用されるわけではないことになります。

(2) EEA 域内にいるデータ主体に対する商品または役務の提供（本ガイドライン 14～17 頁）

EEA 域内にいるデータ主体に対する商品または役務の提供に該当するためには、EEA 域内にいるデータ主体に対して商品またはサービスを提供する意図が明白であることが必要です（前文(23)項）。意図が明白かを判断するに当たっては、言語、通貨、EEA 域内の顧客またはユーザーに関する言及があるか等を通じて判断するべきと解されています（同項）。

本ガイドラインではこの点を確認した上で、その他の判断要素として新たな要素を列記しています。

- 提供する商品またはサービスに関連して、EU または EEA 加盟国を個別に指定しているか
- EEA 域内の消費者がウェブサイトにアクセスすることが容易になるように、サーチエンジンの運営者に依頼しているか、または、EEA 加盟国の閲覧者に向けたマーケティングや広告活動を行っているか
- 旅行者の活動などの、検討対象の活動の国際的性質
- EEA 加盟国からアクセスできる専用の住所または電話番号への言及
- 「.de」のように、管理者または処理者が設立されている国以外のトップレベル・ドメインの利用、または「.eu」のようなトップレ

[11] 大要、1 つの監督当局のみを自社の監督当局として取り扱えば足りること。

ベル・ドメインの利用
- EEA 加盟国からサービスが提供される地までの行き方が記述されている場合
- 様々な EEA 加盟国に居住する利用者から成る顧客層への言及、特にそれらの利用者により書かれた説明を紹介・掲示している場合
- 取引を行う者の国で一般的に利用されていない言語や通貨、特に 1 つ以上の EEA 加盟国の言語や通貨の利用
- EEA 加盟国への商品発送の申出

また、本ガイドラインでは、ウェブサイトにアクセスできることや、ウェブサイトに e-mail や住所の記載や、国番号のない電話番号の記載があることでは、EEA 域内にいるデータ主体に向けて商品またはサービスを提供する意図を明白とするには足りないという前文(23)項の記載が改めて確認されています。

実務的には、以上のとおり判断要素が増えたものの、大きな判断枠組みは変わらないため、本ガイドラインの公表による大きな影響は見込まれないように思われます。もっとも、後記 IV.2.で述べるとおり、観光関連については GDPR が域外適用される方向に導く判断要素が増えていることから、GDPR が域外適用されないと判断する場合には、慎重な検討が必要になると考えられます。

(3) EEA 域内で行われるデータ主体の行動の監視(本ガイドライン 17～18 頁)

EEA 域内で行われるデータ主体の行動の監視に当たるか否かは、データ主体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(前文(24)項)。本ガイドラインは、この点を確認した上で、インターネット上での個人の追跡を通じた行動の監視のみならず、ウェアラブル端末やスマートデバイスを通じたデータ主体の監視についても 3 条 2 項(b)号に基づいて GDPR が適用される旨を明らかにしています。

次に、本ガイドラインは、3 条 2 項(a)号の適用場面では、EEA 域内のデータ主体に向けて商品またはサービスを提供する意図が明白かが問題とされている一方で、同項(b)号の適用場面ではこのような意図は問題にされていない点を指摘した上で、「監視(monitoring)」という用語は、EEA 域内の個人の行動について関連するデータを取得し、その後利用する具体的な目的を含むとしています。そして、EEA 域内の個人に係る個人データのオンラインでの取得および分析だけでは「監視」に該当せず、データの処理と、その後の行動分析やプロファイリングなどを行う目的も必要であるとしています。この目的が必要であること自体は、前文(24)項で既に示されていたため、特段新たな留意事項となるものではないように思われます。

そして、本ガイドラインでは、3 条 2 項(b)号に基づいて GDPR が適用される個人データの処理には広い範囲の監視活動が含まれるとし、特に以下のものを掲げています。

- ターゲット広告(Behavioural advertisement)
- 位置情報の取扱い。特にマーケティング目的のもの
- Cookie 等を利用したオンラインでの追跡
- パーソナライズドされた食事または健康のオンライン分析サービス
- 監視カメラ
- 個人のプロファイルに基づく市場調査その他の行動調査
- 個人の健康状態の監視と定期的な報告

実務的には、大きな判断枠組みには変更はなく、また、新たに斟酌すべき要素もほとんど見当たらないため、個人データには IP アドレスや Cookie 等が広く含まれ、「監視(monitoring)」には上記のような処理活動が含まれることを前提に GDPR 対応を行ってきた企業にとっては、本ガイドラインの公表による大きな影響は見込まれないように思われます。他方で、3 条 2 項(b)号に基づい

て GDPR が適用される個人データの処理については、本ガイドラインの公表まで GDPR 対応をいったん見送ってきた企業も少なくなく、それらの企業にとっては新たに影響範囲を確定して、GDPR 対応に取り組む必要があると考えられます。

III. EU 代表者(EU Representative)(本ガイドライン 19～23 頁)

日本企業を含む EEA 域外の企業に、3 条 2 項に基づいて GDPR が域外適用される場合には、管理者または処理者の何れも、原則として書面により EEA 域内に代表者を選任する必要があります(27 条 1 項)。なお、本ガイドラインでは、EU 代表者を指定したことによって EU 代表者が管理者または処理者の EEA 域内の拠点になるわけではないことが明確となりました[12]。以下、本ガイドラインの内容を説明します。

1. 書面による EU 代表者の選任(本ガイドライン 20～21 頁)

EU 代表者の選任は、管理者または処理者の代わりに GDPR 上の義務に関して行動することについて書面により明示的に委任される必要があります(前文(80)項)。本ガイドラインでは、この書面による委任は EU 代表者と管理者または処理者との間の関係と義務を規律するものでなければならないとされています。

本ガイドラインでは、法人等の組織を EU 代表者とする場合であっても、その中で自然人の担当者を定めておくことが推奨されるとともに、一般的には、その点を委任に際しての契約に明記しておくことが有益であるとされています。

また、実務的には知られた論点ではありますが、データ保護責任者(DPO)が利益相反的地位(38 条 3 項参照)に置かれることを理由に、EU 代表者がデータ保護責任者(DPO)の役割を兼ねることについては否定的な見解が示されています。

2. EU 代表者の選任義務が免除される場合(本ガイドライン 21～22 頁)

27 条 2 項には、以下のように EU 代表者の選任義務が免除される場合が規定されています。

① 一時的なものであり、9 条 1 項に定める特別な種類のデータの処理または 10 条に定める有罪判決および犯罪行為と関連する個人データの処理を大規模に含まず、かつ、その処理の性質、過程および目的を考慮に入れた上で、自然人の権利や自由にリスクを及ぼすおそれが低い処理
② 公的機関または公的組織(によって行われる処理)

企業にとっては、「一時的」「大規模にセンシティブデータを含むものではない」「自然人の権利や自由にリスクを及ぼすおそれが低い」の 3 要件を全て満たさなければ EU 代表者の選任義務が免除されない点で、適用除外の要件は限定的であるといえます。本ガイドラインでは、このうち「大規模(on a large scale)」の考え方について、データ保護責任者(DPO)に関するガイドライン[13]で示されていた、データ主体の数(人数や人口に占める割合)、データの量、データ項目の種類、データ処理活動の期間または永続性、処理活動の地理的範囲などを考慮すべきとしています。この点については、データ保護責任者(DPO)のガイドラインの文脈でもこれらの考慮要素に基づき大規模が否かを判断することは容易でないといわれてきたほか、その他の要件については考え方が示されていないこともあって、適用除外に依拠する場合には引き続き慎重な検討と説明が必要であると考えられます。

なお、3 条 2 項に基づいて GDPR が適用される場合には EU 代表者が誰であるかをプライバシーノーティスに記載することが求められており(13 条 1 項 a 号、14 条 1 項 a 号)、本ガイドライン上も、これを怠った場合には GDPR に基づく透明性の義務に違反する可能性があると本ガイドラインに明記されるに至っています。

---

12 本ガイドライン 20 頁。

13 Article 29 Data Protection Working Party, Guidelines on Data Protection Officers (‘DPOs’), WP243 rev.01.

3. どこの加盟国に選任すべきか（本ガイドライン 22 頁）

GDPR 上、EU 代表者は、域外適用の対象となる個人データの処理が対象とするデータ主体のいる加盟国のうちの 1 つに選任する必要があります（27 条 3 項）。

本ガイドラインでは、データ主体が複数の国に存在する場合には、その中でデータ主体が所在する割合の高い（significant portion）EEA 加盟国に EU 代表者を選任することが推奨されています。もっとも、ブレグジットのことを考えますと、英国に選任することについては慎重に検討する必要がありそうです。

4. 代表者の義務と責任（本ガイドライン 23 頁）

GDPR 上、EU 代表者は、GDPR の遵守を確保するために、処理と関連する全ての事項に関して監督機関とデータ主体への対応を行うために選任を受けるものとされています（27 条 4 項）。

この点について、本ガイドラインは、監督機関は EU 代表者に連絡する可能性があり、EU 代表者としては監督機関と、自身を選任した管理者または処理者との間のコミュニケーションを容易にすることが求められるとしています。また、EU 代表者は、データ主体とのやりとりも効率的にこなす必要があるとしています。その上で、本ガイドラインは、これらのコミュニケーションや、やりとりは、現地で用いられている言語で対応することが求められるとしています。しかしながら、現地語での対応が可能な EU 代表者を選任することは、実務的には困難を伴うことが多いと予想され、悩ましい問題であるといえます。

また、EU 代表者は、データ処理の記録を保持することが求められていますが（30 条 1 項）、本ガイドラインでは、この保持義務は管理者または処理者との共同責任であり、管理者または処理者は、正確かつ最新の情報を EU 代表者に提供しなければならないとされています。

なお、EU 代表者を選任したからといって、管理者や処理者の法的責任が軽くなるわけではありません（27 条 5 項）。他方で、本ガイドラインでは、EU 代表者についても管理者または処理者と同様に執行対象になり得ると明示的に言及がなされており、EU 代表者が制裁金または罰金の対象となり、責任を負う可能性があるとされています。この点については、EU 代表者を選任するに当たって重要な考慮要素になると考えられます。

IV. 業種別に注目すべきポイント

以下では、本ガイドラインで紹介されている具体例を踏まえて業種別に特に注目すべきポイントを紹介します。具体例で紹介されている業種とデータ処理のタイプは、監督当局が特に関心を持っていることの現れでもありますので、これらの業種・データ処理を行っている企業においては、適切に GDPR 対応のスコープを確定し、取り組んでいくことが望まれます。

1. データ処理の委託先

Example 6、7において、データ処理を委託する事例が紹介されています。

本ガイドラインでは、EEA 域内の企業から個人データの処理の委託を受ける場合には、GDPR が適用される個人データの処理の委託を受けることのみを理由として、処理者である委託先が GDPR の適用を受けるわけではないことが明確にされました[14]。この点は、3 条 1 項に基づいて GDPR の適用を受ける管理者から個人データの処理の委託を受けると、それだけで処理者にも GDPR が適用されるというアドバイスを行う業者もあったようです。実際にかかるアドバイスに基づいて対応を強いられた日本企業も少なくなかったことから、解釈が明確化されたことは日本企業にとって朗報であるといえます。

[14] 本ガイドライン 9 頁。

もっとも、処理者として何もすることがなくなるわけではありません。すなわち、GDPR の適用を受ける管理者としては、処理者との間で GDPR 所定のデータ処理契約を締結しなければデータ処理を処理者に委託することができないため、処理者としてもその契約の締結に応じ、契約上の義務[15]を遵守する必要があり、この点が本ガイドラインで明確にされています[16]。また、本ガイドラインでは、管理者によっては、自身が 28 条 1 項に基づく管理者の義務[17]を遵守するために、(GDPR との関係では、処理者に GDPR が適用されるわけではないものの)GDPR 上処理者が負う義務で、28 条 3 項各号に列挙されている以外の義務も契約によって処理者に課す可能性があることについても指摘しています[18]。実際に、海外企業が取引相手となる場合には、このような契約のアレンジを要求されることはしばしばあるようですが、この場合に遵守すべき処理者の義務は、本ガイドラインの 11 頁に列挙されています。

したがって、データ処理の委託先としては、管理者の個人データの処理が GDPR の適用対象となる場合には、少なくとも 28 条 3 項の契約を締結し、契約上の義務を遵守することが必要です。また、グローバルにデータ処理の委託を受けることを想定しているビジネスの場合には、GDPR を遵守できる処理者なのかということが選定の条件とされる場面が多くなることが見込まれるところ、短期間でのシステム対応等は容易でないため、しっかりと準備を進めていくことが必要であるといえます[19]。このデータ処理契約については、処理者として、全ての管理者との間で異なる契約を締結するのは容易でないことから、処理者の側でひな形を用意する事例が多くなっています。

なお、データ処理の委託先と書きましたが、日本の個人情報保護法における委託先の概念と、GDPR の処理者の概念は必ずしも一致しないため、そもそも GDPR にいうデータ処理を行っているのか、何らかデータ処理を行っているとして管理者と処理者の何れに該当するのかといったところは、慎重な検討が必要となります。

2. 観光関連(ホテル、旅客運送(航空、鉄道、バス)など)

Example 3において、ホテルの事例が紹介されています。2020 年の東京オリンピックや、2025 年の大阪万国博覧会をひかえて、EEA 域内を含め世界からの観光客の増加が見込まれる中で対応が急務となっているのが観光関連であるといえます。

本ガイドラインとの関係では、EEA 域内からの予約に伴って取得する個人データの処理について、EEA 域内に向けてサービスを提供する意図が明白であるとして、3 条 2 項(a)号に基づいて GDPR が適用されることになるかを検討することが重要です。これまでは、前文(23)項で、言語、通貨、EEA 域内のデータ主体への言及が判断要素として列挙されるにとどまっていましたが、本ガイドラインでは、観光に関連する可能性のある判断要素として、以下の項目が判断要素に追加されている上に、「旅行者の活動などの、検討対象の活動の国際的性質」という形で「旅行者の活動」が特に例示されていることから、GDPR が適用されないとの判断は、これまで以上に慎重に行うことが必要になったといえます。

- EU 域内の消費者がウェブサイトにアクセスすることが容易になるように、サーチエンジンの運営者に依頼しているか
- EU 加盟国の閲覧者に向けたマーケティングや広告活動を行っているか
- 旅行者の活動などの、検討対象の活動の国際的性質
- EU 加盟国からアクセスできる専用の住所または電話番号への言及
- EU 加盟国からサービスが提供される国までの旅行の情報の記述

---

15 28 条 3 項に列挙されています。

16 本ガイドライン 9～10 頁。

17 管理者は、処理が GDPR に定める義務に適合するような態様で適切な技術上、および、組織上の保護措置を実施することについて十分な保証を提供する処理者のみを用いるものとし、かつ、データ主体の権利の保護を確保するものとされています。

18 本ガイドライン 10 頁。

19 石川智也「GDPR 対応の現状」ヨーロッパニューズレター2018 年 4 月号においても、この点については触れていたところです。

また、観光関連では、①旅行代理店（Online Travel Agent を含みます。）、ウェブサイトの運営者、ホテルや旅客運送等のサービス提供者のうち、誰が管理者になり、処理者になるのか、②それを踏まえて、EEA 域内からのデータ移転として整理すべきか、日本企業が直接データを取得しており、GDPR の域外適用を受けると整理すべきか、③システムやサーバの委託先との契約関係をどのように規律すべきかといったところの整理が対応の出発点となります。特に②の点について、実務で混乱が見られますが、消費者の重要なデータを大規模に処理する可能性があり、かつ、外部への委託を要素とする点でリスクの高い類型ですので、確実な整理が望まれるといえます。

3. アプリ開発

Example 4、8、9、16において、アプリ開発の例が紹介されています。

Example 8では、アメリカで位置情報に関する消費者の個人データを処理する地図アプリを開発し、そのアプリが EEA 域内の都市で利用可能である場合には、EEA 域内にいる者に対するサービス提供に関連する個人データの処理であることを理由に、3 条 2 項(a)号に基づいて GDPR が適用されると紹介されています。他方で、Example 9では、アメリカ市民が、休暇でヨーロッパを旅行中にアメリカ企業によって提供されているニュースアプリをダウンロードし、利用したとしても、そのアプリがアメリカ市場のみに向けられたものである場合には、そのアメリカ企業には GDPR が適用されないと紹介されています。また、Example 16では、カナダのアプリ開発業者が、EEA 域内のデータ主体の行動を監視している場合には 3 条 2 項(b)号に基づいて GDPR が適用され、その業者がアプリの最適化とメンテナンスの目的でアメリカの処理者を利用したときには、アメリカの処理者との間で 28 条に基づくデータ処理契約が必要であると紹介されています [20]。これらの例は、オンラインゲーム、ニュースアプリ、健康アプリなど、アプリを開発する日本企業にとっても、参考になる点が少なくありません。

また、インターネット上での個人の追跡を通じた行動の監視のみならず、本ガイドラインでは、ウェアラブル端末やスマートデバイスを通じたデータ主体の監視についても 3 条 2 項(b)号に基づいて GDPR が適用される旨が明記されている [21]ことに注意が必要です。

4. 広告・マーケティング関連

Example 2、15において広告・マーケティング関連について言及されているほか、3 条 2 項(b)号に基づく「EU 域内にいる個人の行動の監視」の例として広告・マーケティング関連の事例が数多く列記されている点で、この分野についての当局の関心の高さが窺えます。

まず、3 条 2 項(b)号に基づく「EU 域内にいる個人の行動の監視」に、ターゲット広告（Behavioural advertisement）、マーケティング目的での位置情報の取扱い、Cookie 等を利用したオンラインでの追跡、個人のプロファイルに基づく市場調査その他の行動調査が含まれることが明記されています。実務的には、どのようにウェブサイトやアプリに組み込まれているマーケティングツールについて開示を行うか、同意取得をどのように行うかといったところが対応の鍵となります。

また、マーケティング関連では、ウェブサイトの構築・運営についても、データ処理を伴う場合には GDPR への対応が必要となる可能性があることに注意が必要です。

5. 製薬企業

Example5、20において製薬企業の例が紹介されています。

特に重要なのは、Example 20において、EEA 域内に拠点を有さず、かつ、3 条 2 項に基づいて GDPR が適用される EEA 域外に

---

[20] この場合に、アメリカの処理者に GDPR が適用される場合があるのかについては、本ガイドライン上は明確に示されていません。

[21] 本ガイドライン 17～18 頁。

ある企業が試験依頼者になって EEA 域内の病院で臨床試験を行う場合の考え方が示されている点です。このことから明らかなのは、EEA 域外にある企業が試験依頼者になって EEA 域内の病院で臨床試験を行う場合に、3 条 2 項に基づいて GDPR の適用を受ける場合があるということです。また、本ガイドラインによれば、かかる試験依頼者の EU 代表者は、臨床試験に関する EU の規則(2018 年 11 月現在未施行)[22]に定めるところの代表者(legal representative)と同一の者であってもよい場合があるとされています[23]。

EEA 域内における臨床試験により取得する個人データについては、別稿でも紹介したように[24]、①関係者のうち、誰が管理者になり、処理者になるのか、②それを踏まえて、EEA 域内からのデータ移転として整理すべきか、日本企業が域外適用を受けると整理すべきか、③CRO(Contract Research Organization)や委託先との契約関係をどのように規律すべきかといったところが対応の出発点となります。こちらも、センシティブなデータの処理を含み、かつ、外部への委託を要素とする点でリスクの高い類型ですので、確実な整理が望まれるといえます。

6. 教育機関(大学、語学学校など)

Example 14において、EEA 域外の大学が GDPR の域外適用を受ける場面について説明がなされています。具体的には、スイスの大学が、十分な英語とドイツ語の能力を有する学生をオンラインで募集する事例において GDPR の適用がないというものですが、英語を含む欧州の言語が母語でない学生が大多数を占める日本の大学についても同様に考えることができるかについては、具体的な事実関係を踏まえて慎重な検討が必要です。また、この事例で説明されている内容を踏まえると、EEA 域内の大学との間で交換留学等のプログラムを実施している場合には、その留学生が日本に渡航してくるまでに取得する個人データについては、GDPR が適用される可能性があると考えられますので、注意が必要です。以上のことは、語学学校などについても同様にあてはまると考えられますし、何れの場合も、海外向けのウェブサイトの構築や学生の紹介について GDPR が定めるデータ処理契約の締結などが問題となる可能性があります。

なお、EEA 域内から日本への個人データの越境移転については、十分性認定に向けた手続が進められていますが、十分性認定の対象は個人情報保護法が適用される個人情報取扱事業者のみであり、独立行政法人については十分性認定に基づいて EEA 域内から個人データの移転を受けることができない点に留意が必要です。独立行政法人については、EEA 域内からの個人データの移転につき、標準契約条項(SCC)に基づくデータ移転などその他の措置を検討する必要があることになります。

7. クルーズ船

Example 18では、EEA 域内に登録されたクルーズ船が国際水域航行中に行う船内のエンターテイメント提供のための乗客の個人データの処理については、3 条 3 項(国際公法を理由として EU 加盟国法が適用される場合における個人データの処理について GDPR が適用される旨を述べた条文)を根拠に GDPR が適用される旨が紹介されています。

V. 最後に

GDPR 対応に当たっては、地理的範囲を踏まえて GDPR が適用される可能性のあるデータ処理を適切に確定することが必要です。GDPR が既に施行されており、かつ、当局の調査等も各国で始まっている現状に照らすと、リスクの高いデータ処理(従業員データの処理、センシティブデータの処理、大規模なデータ分析など)から順に、リスクの高く、かつ、早期に対応が可能な項目(プ

---

22 Regulation (EU) No 536/2014 of the Europe Parliament and of the Council of 16 April 2014 on Clinical Trials on Medicinal Products for Human Use, and Repealing Directive 2001/20/EC.

23 本ガイドライン 22 頁。

24 石川智也「〔講演録〕施行と十分性認定を踏まえた、日本企業の GDPR 対応」リーガルマインド No.402(2018 年 10 月号)参照。

ライバシーノーティスの提供、データ処理契約の締結、記録義務の遵守、越境移転規制への対応など）について応急的な処置を行い、リスクを早期に下げることが極めて重要であると考えられます。

当事務所では、上記 IV.に掲げた業種はもちろんのこと、多くの日本企業・多くの業種の GDPR 対応を支援してきており、欧州の事務所とのネットワークを通じたグローバルでの対応のみならず、域外適用を受ける日本企業の国内での対応まで、広く皆さまのニーズに沿った支援が可能ですので、ご遠慮なく問い合わせフォームを通じてご連絡ください。

以　上

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。2015 年バージニア大学ロースクール卒業(LL.M.)、2016 年マックス・プランク イノベーション・競争法研究所併設のミュンヘン知的財産法センター卒業(LL.M.)、Noerr 法律事務所ミュンヘンオフィスに出向、2017 年ニューヨーク州弁護士登録。IP とデータの保護と利活用に関する法制度を専門とし、グローバルでのデータ規制への対応について多くの日本企業にアドバイスを提供。欧州での M&A も手掛ける。情報法制学会会員。

すが　ゆうじん
菅　悠人　　西村あさひ法律事務所　弁護士
y_suga@jurists.co.jp

2009 年弁護士登録。2017 年パリ第二大学修士課程卒業(LL.M. de droit français, européen et international des affaires)、フランス・パリ弁護士会登録。2017 年よりウィルマーヘイル法律事務所(ロンドンおよびブリュッセルオフィス)へ出向。国際案件の経験が豊富で、外国の法令に関する知見も広い。特に EU における規制関連法全般について現地実務や法令改正等、最新の動向を踏まえた助言を行っている。

（当事務所の連絡先）　東京都千代田区大手町 1-1-2 大手門タワー 〒100-8124
Tel: 03-6250-6200（代） Fax: 03-6250-7200
E-mail: info@jurists.co.jp URL: https://www.jurists.co.jp