「EU 一般データ保護規則（GDPR）」に関わる実務ハンドブック（入門編）

2016 年 11 月

日本貿易振興機構（ジェトロ）
ブリュッセル事務所
海外調査部　欧州ロシア CIS 課

「EU一般データ保護規則（General Data Protection Regulation：GDPR）」は、2016年5月4日付のEU官報に掲載、2016年5月24日に発効した。ただし、行政罰を伴う適用開始は2018年5月25日と定められており、これが実質的な「施行日」となる。

GDPRは､EUを含む欧州経済領域（EEA）域内で取得した「氏名」や「メールアドレス」「クレジットカード番号」などの個人データをEEA域外に移転することを原則禁止している。ここでいう「個人」とは、EEA域内の所在者全般を指し、現地進出の日系企業に勤務する現地採用従業員や、日本から派遣されている駐在員も含まれるため、注意が必要だ。行政罰規定があり、違反行為に対しては、高額の制裁金が課されるリスクもある。

GDPRの適用対象には、営利活動に従事する企業のみならず、公的機関・地方自治体・非営利法人なども含まれる（外交・防衛・警察などについて例外あり）。すなわち、EEA域内に現地法人・支店・駐在員事務所を置くすべての企業・団体・機関が、GDPRへの対応を検討することが求められている。また、中小・零細企業も対象であり、EEA域内に現地法人・支店・駐在員事務所を置かない事業者であっても、インターネット取引などで EEA 所在者の顧客情報を取得・移転する場合、適用対象となり得る。また、こうした事業者にはEUにおける代理人の選任義務が課せられるケースがあり、その場合の義務違反にも高額の制裁金が課されるリスクがあるので要注意だ。

このため、EEAと個人データをやり取りする日本のほとんどの企業や機関・団体が適用対象となり、適用が開始される2018年5月25日までに適切な準備を進めることが必要だ。他方、GDPRの内容は、法解釈を伴う専門的なものであるため、EEAでビジネスを行う企業の間でも正確に理解されていない側面もある。特に、EEAにビジネスを展開しようとする中小企業には、大きな負担となることが想定される。

こうした問題意識の下、ジェトロは、GDPRに詳しいウィルマーヘイル法律事務所ブリュッセルオフィスの杉本武重弁護士（日本国、ブリュッセル（準会員）、米国ニューヨーク州）に委託し、本レポートを作成した。本レポートは、欧州ビジネスに取り組む中小企業の実務担当者の利用を念頭に、専門的な政策解説・法解釈は避け、実務事例をベースとした「Q&A形式」とした。前半の「概要編」でGDPRの意義・全体構造など概要を示し、「Q&A基礎編」でGDPRの基本を概説、後半の「Q&A応用編」では、顧客関連の対応を中心とする「社外」と、EEA進出企業の従業員関連の対応を中心とする「社内」の具体的な実務に焦点を当て、問題と対策を概説した。

JETRO

目　次

Ⅰ. 概要編

欧州連合（EU）の「一般データ保護規則（General Data Protection Regulation：GDPR）」（2016/679）[1]は、EU レベルのデータ保護法（日本でいうところの個人情報保護法に相当する）であり、2018 年 5 月 25 日から適用が開始される。

GDPR は、個人データの処理、および個人データを欧州経済領域（European Economic Area：EEA[2]）から第三国に移転するために満たすべき法的要件を規定している。

GDPR は「EU 基本権憲章」という EU 法体系の根幹をなす法において保障されている、**個人データの保護に対する権利という基本的人権の保護を目的とした法律**である。GDPR は、基本的人権という「EU 基本権憲章」上の重要な価値を保障するため、違反に対して厳しい行政罰を定めている。

GDPR は、EEA 域内でビジネスを行い、個人データを取得する中小・零細企業を含む日本企業や日本の公的機関に対しても、幅広く適用される。そして、GDPR の規定の建付けは、企業や公的機関が GDPR へのコンプライアンス対応を怠れば、原則として GDPR 違反となりやすい形となっている。

従って、日本企業や日本の公的機関は、今、GDPR に注目し、GDPR へのコンプライアンス対応の要否について検討し、必要な場合には、速やかに具体的な対応を行うことが、将来における GDPR 違反に基づく巨額の制裁金の賦課という事態を避けるために重要である。

このように書くと大袈裟に思われる方も多いかもしれない。しかしながら、EEA 域内においてビジネスを行う日本企業が 2000 年代に EU 競争法違反、特にカルテル規制違反に基づき欧州委員会競争総局によって巨額の制裁金を課せられる事案が相次いで報道されたことを忘れてはならない。

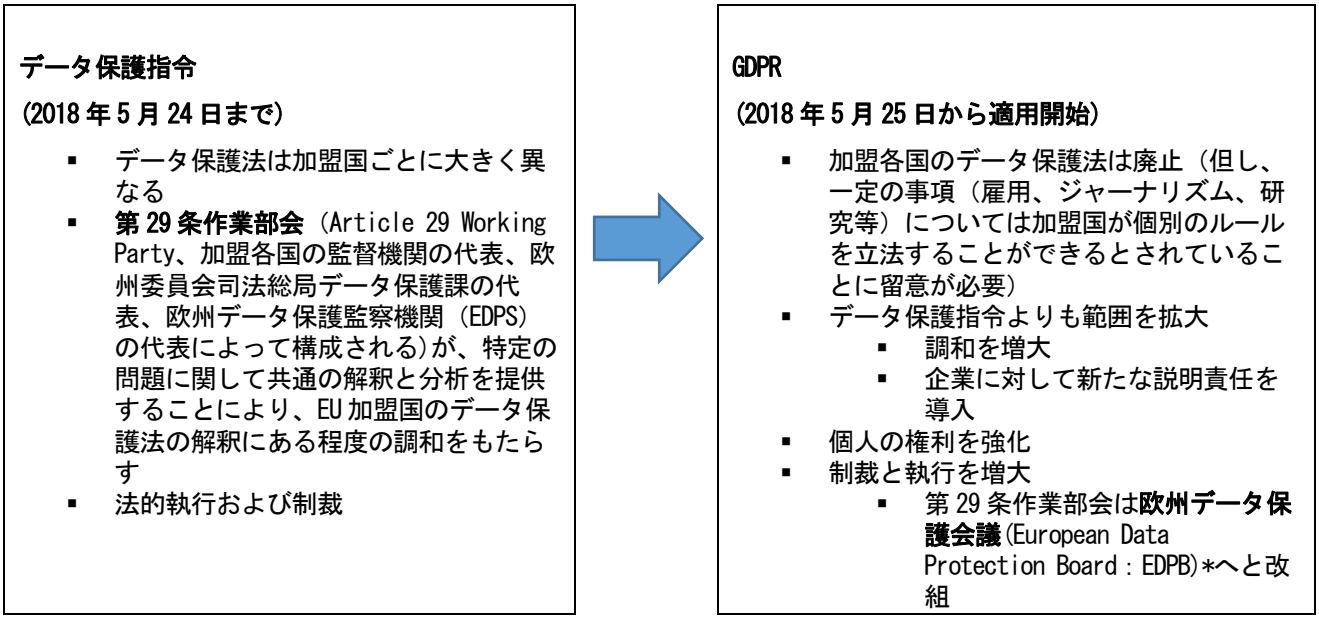
GDPR の制裁金制度は、EU 競争法の制裁金制度を基本としている。EU 競争法のカルテル規制の執行における成功体験があるからこそ、GDPR は EU 競争法の制度を踏襲するのである。

また、GDPR 対応においてはきめ細やかな対応が必要になる。GDPR の先行法令である 1995 年の EU「データ保護指令」（95/46/EC）[3]に基づき立法された 31 の EEA 加盟国のデータ保護法と監督機関の下で、各々の加盟国でデータ保護法の実務は独自の変容を遂げてきている。GDPR 施行後も、各々の加盟国の監督機関の特殊性を踏まえた対応を行うことが、GDPR の執行リスクを低く抑えるためには必要である。

2018 年 5 月 25 日の GDPR の適用開始に伴い、先行法令のデータ保護指令は廃止される。また、加盟各国のデータ保護法を廃止し、EU レベルでの規制の調和や、制裁・執行の強化が図られる。主な変更点は図 1 に示すとおり。

[1] http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32016R0679
[2] EU 加盟国 28 カ国およびアイスランドとリヒテンシュタイン、ノルウェー
[3] http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31995L0046

図 1：データ保護指令から GDPR への主な変更点[4]



*：EDPB については「Q7 GDPR を所管する当局とは何ですか？EU と EU 加盟国には各々どのような権限がありますか？」を参照

1. GDPR の適用対象

(1) GDPR を一言で説明すると？＝「個人データ」の「処理」と「移転」に関する法

GDPR は、EEA 域内で取得した「個人データ」を「処理」し、EEA 域外の第三国に「移転」するために満たすべき法的要件を規定している。これらの概念の説明と例を表 1 に示す。

表 1：基礎的な概念の説明と例

概念	説明	例
個人データ	識別された、または識別され得る自然人（「データ主体」）に関するすべての情報	▪ 自然人の氏名 ▪ 識別番号 ▪ 所在地データ ▪ メールアドレス ▪ オンライン識別子(IP アドレス、クッキー識別子) ▪ 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因

[4] なお、本レポートは可能な限り読者の GDPR へのコンプライアンス対応に資するように作成されているが、本レポートを御利用頂くにあたっては、本レポートの校了時点（2016 年 11 月 14 日）において、GDPR の解釈や制度運用について、欧州委員会や上記のように監督機関の代表者等によって構成される第 29 条作業部会からいまだに何らのガイドラインも公表されていない点に留意が必要である。現時点では、GDPR を執行する立場となる監督機関の担当者でさえも、GDPR の解釈や制度運用について活発な議論を繰り広げており、いまだその議論は結論を見ない。2016 年 12 月から順次第 29 条作業部会等が GDPR に関するガイドラインを公表する予定となっており、読者におかれては、本レポートの内容と併せて、これらのガイドラインの内容を注視されたい。

処理	自動的な手段であるか否かに関わらず、個人データ、または個人データの集合に対して行われる、あらゆる単一の作業、または一連の作業	▪ クレジットカード情報の保存 ▪ メールアドレスの収集 ▪ 顧客の連絡先詳細の変更 ▪ 顧客の氏名の開示 ▪ 上司の従業員業務評価の閲覧 ▪ データ主体のオンライン識別子の削除 ▪ 全従業員の氏名や社内での職務、事業所の住所、写真を含むリストの作成
移転	GDPR に定義なし。あえて定義すれば、EEA 域外の第三国の第三者に対して個人データを閲覧可能にするためのあらゆる行為	▪ 個人データを含んだ電子形式の文書を電子メールで EEA 域外に送付することは「移転」に該当する

(2) 保護対象となる「個人データ」の範囲

GDPR の保護対象となる「個人データ」とは、EEA 域内に所在する個人（国籍や居住地などを問わない）の個人データをいう。短期出張や短期旅行で EEA 域内に所在する日本人の個人データや、日本企業から EEA 域内に出向した従業員の情報（元は日本から EEA 域内に移転した情報）も、処理および第三国への移転の制限を受ける個人データに含まれる。また、日本から EEA 域内に一旦、個人データが送付されると、EU の基準に沿って EEA 域内において処理されなければならない。さらに、当該個人データを日本へ移転する場合、EU の基準を遵守しなければならない。

EEA 域内の監督機関（「Q7 GDPR を所管する当局とは何ですか？EU と EU 加盟国には各々どのような権限がありますか？」を参照）は、EEA 域外の第三国に所在する「管理者」が EEA 域内の「処理者」へ個人データを送り、その後、元の EEA 域外の国に当該個人データ(特に、非 EEA 市民のデータである場合)を再度輸出する場合については、GDPR を適用する必要性が低いと考えている。

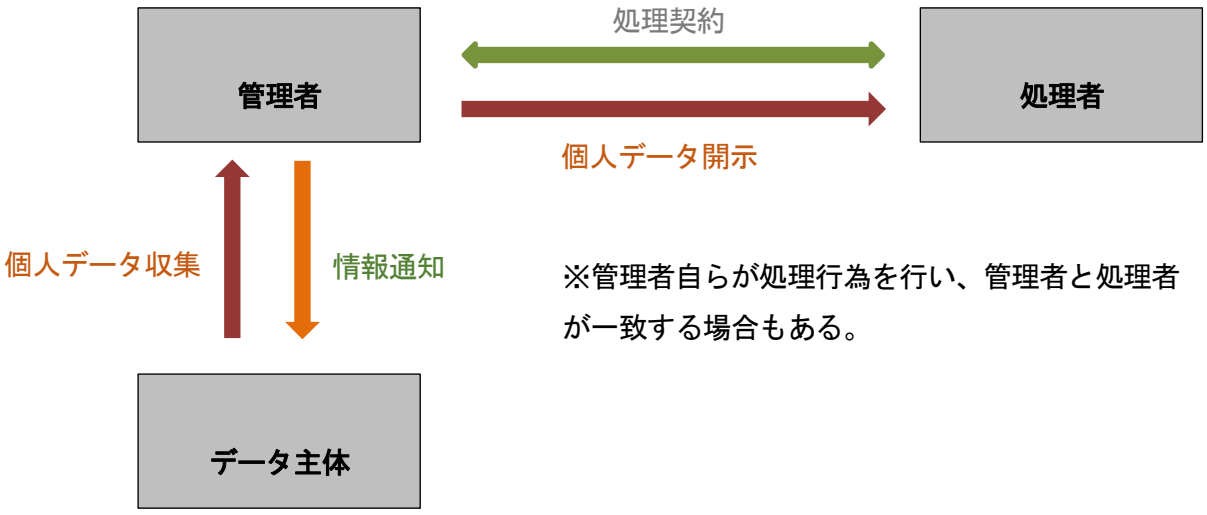
なお、「データ主体」、「管理者」および「処理者」の説明と例は表 2 に示すとおり。

表 2：「データ主体」、「管理者」および「処理者」の説明と例

概念	説明	例
データ主体	個人データが関連する当該個人。	ABC 社は自社従業員の個人データを処理している。この個人データが関連する ABC 社の従業員個人がデータ主体である。
管理者(第 4 条(7))	単独または共同で個人データの処理の目的と手段を決定する。管理者は、個人データの処理の適法性と GDPR 違反に対する責任を負う。	ABC 社は自社従業員の個人データを処理している。雇用者としての義務を遂行するために処理を行っているため、管理者に相当する。
処理者(第 4 条(8))	管理者を代理して、個人データの処理を行う自然人または法人。	ABC 社は他社のマーケティングツールの管理のための個人データの処理を専門業としている。この機能において ABC は処理者であり、管理者を代理して処理を行う。

また、「データ主体」、「管理者」および「処理者」の関係を図2に示す。

図2：「データ主体」、「管理者」および「処理者」の関係



(3) GDPRの適用範囲(第2条および第3条)

GDPRは、管理者、または処理者がEEA域外で設立されたものである場合であっても、以下のいずれかの場合には適用される。

- EEAのデータ主体に対して商品またはサービスを提供する場合
- EEAのデータ主体の行動を監視する場合

例えば、日本本社のウェブサイトでEEA所在者に対して商品・サービス(鉄道切符、航空券、パッケージ旅行など)を販売する企業は、本社に対してGDPRが直接、適用され得ることに注意が必要である。

EEAで取得した個人データ（顧客情報、取引先情報、従業員の人事情報、潜在顧客の情報、現地従業員の採用に当たって収集する履歴書など）を処理する場合、企業は当該個人データを確実に適法に処理すべきである。

(4) 「拠点」と「主たる拠点」

GDPRは、提供対象となる「拠点」と「主たる拠点」を表3のとおりに定義している。

表 3：「拠点」と「主たる拠点」の定義

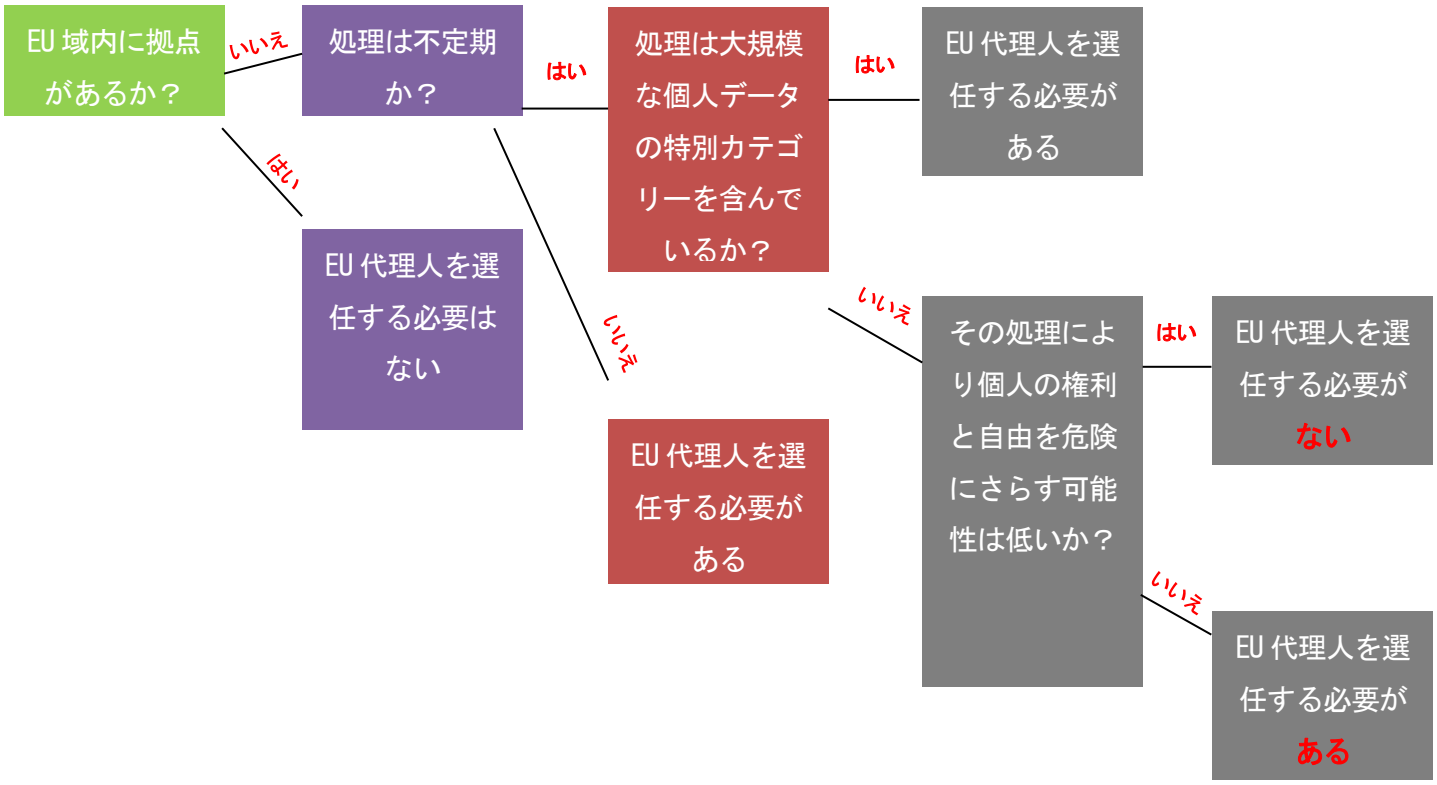
概念	説明	例
拠点（前文第 22 項および第 36 項）	固定的な体制を通じて、実効的かつ現実に活動を実施する場合、拠点とみなされる。 「固定的な体制」の法的形態は、拠点であるか否かの判断要素とはならない。支店でも子会社（駐在員 1 名だけ）でも拠点に該当する。	• 日本企業 A がロンドンに子会社を持つ場合、この子会社は拠点とみなされる。 • 日本企業 B がベルリンに支店を持つ場合、この支店は拠点とみなされる。 • 日本企業 C は、EEA 域内に支店も子会社も持たない。しかし、業務を遂行するのに必要な機器を備えた事務所を持つ駐在員がルクセンブルクにいる。
主たる拠点（第 4 条(16)、前文第 36 項）	EEA 域内に複数の拠点がある場合、「管理者の主たる拠点」は、EEA 域内にある統括管理部門の所在地となる。ただし、個人データのデータ処理の目的および手段に関する意思決定が EEA 域内にある管理者の別の拠点でなされ、かつ後者の拠点がかかる意思決定をする権限をもっている場合は、その拠点が「主たる拠点」となる。 また、「処理者の主たる拠点」は、EEA 域内にある統括管理部門の所在地か、統括管理部門が EEA 域内に存在しない場合は、EEA 域内にある処理者の拠点は、GDPR が定める特定の義務が処理者に適用される限りにおいて、主たる処理業務が行われる場所となる。	• 企業 A は管理者である。EEA 域内にある複数の拠点のうち、ベルリンに統括管理部門を設立している。このベルリンの拠点が「主たる拠点」となる。 • 企業 B は管理者である。EEA 域内にある複数の拠点のうち、統括管理部門はベルリンに所在しているが、ロンドンの拠点が処理を担当している。このロンドン拠点が「主たる拠点」となる。 • 企業 C は処理者である。EEA 域内の統括管理部門の場所を識別することができないが、会社はデータの大部分をロンドンで処理している。ロンドン拠点が「主たる拠点」となる。

2. 個人データの処理・移転に関する義務・法的要件

(1) EU 代理人を選任する義務(第 27 条)

EU 域内に拠点を持たない企業は、代理人を選任しなければならない可能性がある。その場合、EU 代理人を、個人データが処理されるデータ主体が居住する加盟国の中のひとつに設置する(第 27 条(3))。代理人は、管理者・処理者に加えて、または、管理者・処理者の代わりに GDPR の遵守に関する一切の問題に取り組むために、管理者・処理者により委任される(第 27 条(4))。EU 代理人の選任の必要性の有無を図 3 にまとめる。

図 3：EU 代理人選任の必要性の有無



(2) 個人データの処理の法的要件のまとめ

表 4：個人データの処理の法的要件

概要	内容
説明責任 (第 5 条(2))	**説明責任**:管理者は適切な個人データ保護指針の採択、およびその実行を含め、処理行為が**適法な個人データ処理の要件**をはじめとする GDPR の要件を確実に遵守し、かつそれを実証できなければならない。
遵守実証の対策の実施(第 24-30; 37-39 条)	説明責任を果たすための遵守実証の対策の実施として必要な事項は上記以外に以下のようなものがある。 **内部記録**:管理者および処理者は、個人データの処理行為の内部記録を保持しなければならない。 **データ保護責任者（Data Protection Officer：DPO）の選任（義務がある場合)*** **設計によるまたは初期設定によるデータ保護**:管理者は、処理システムの設計、および当該システムの運用において、データ主体の権利を保護し、GDPR を確実に遵守するために、適切な技術的および組織的な措置を実行しなければならない。また、個人データは、処理の目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない。 **影響評価および事前相談**:新技術の使用や処理の性質、対象、目的などに鑑みて、自然人の権利と自由が脅かされる高いリスクが予想される場合はデータ保護影響評価を実施し、当該影響評価の結果、管理者がリスクを軽減する対策を採らなければ処理が自然人の権利や自由に高いリスクを生じさせる可能性がある場合は、当該処理の前に監督機関と事前相談を行う。
個人データのセキュリティに関する義務 (第 4 条(12)、第 32-36 条)	**個人データのセキュリティ要件**:適切なセキュリティ措置の実施 **個人データの侵害通知**:個人データの不慮または不法な破壊、喪失、改ざん、無断開示・アクセスに繋がる保護安全性の侵害は、一定の場合に監督機関およびデータ主体に通知しなければならない。
データ主体の権利の尊重(第 12～22 条)	**データ主体の権利**:管理者は次のデータ主体の権利を尊重しその行使を円滑にする必要がある。情報権、アクセス権、訂正権、削除権（忘れられる権利）、制限権、データポータビリティの権利、異議権、および自動的な個人の意思決定に関する権利
情報権(第 13 条、第 14 条)	管理者はデータ主体から個人データを収集する場合、個人データ入手時に、データ主体に一定の情報を提供しなければならない。
アクセス権(第 15 条)	管理者はデータ主体から処理が行われている個人データへのアクセスの請求があればそのコピーを提供しなければならない。
訂正の権利 (第 16 条)	不正確な自己の個人データに関する訂正を管理者に求める権利を有する。
削除権(第 17 条(1))	一定の場合、データ主体は自分に関する個人データの削除を遅滞なく管理者から得る権利を有する。

制限権(第 18 条)	データ主体は管理者に対して一定の場合に個人データ処理を制限する権利を有する。
データポータビリティの権利(第 20 条)	データ主体は自分に係わる個人データを、構造化され、一般的に使用され、機械によって読み取り可能な形式で受け取る権利を有する。
異議権(第 21 条)	データ主体は管理者または第三者によって追求される適法な利益の目的のための処理の必要性に基づく自己の個人データの処理に異議を唱える権利を有する。
自動化された個人の判断に関する権利(第 22 条)	データ主体は、自分に対する法的影響を生じ得るような、プロファイリングを含む自動処理のみに基づいた判断の対象にならない権利を有する(例、人が介入しないオンライン上での借入申込やインターネットでの採用活動–前文第 71 項)。

＊：Q19「企業内での責任者の任命など、組織体制面ではどのような対応が必要ですか？」を参照

(3) 適法な個人データ処理の要件

個人データを処理するに当たり、管理者は下記 6 原則を遵守する義務を負っている。これに加えて、管理者はその遵守を証明できなければならない（説明責任の原則）。その原則を表 5 にまとめる。

表 5：個人データの処理における原則

No	原則	内容（GDPR 第 5 条第 1 項）
1	適法性、公平性および透明性の原則	個人データは、適法、公平かつ透明性のある手段で処理されなければならない。
2	目的の限定の原則	個人データは、識別された、明確かつ適法な目的のために収集されるものでなければならず、これらと相容れない方法で更なる処理を行ってはならない。
3	個人データの最小化の原則	個人データは、処理を行う目的の必要性に照らして、適切であり、関連性があり、最小限に限られていなければならない。
4	正確性の原則	個人データは、正確であり、必要な場合には最新に保たれなければならない。不正確な個人データが確実に、遅滞なく消去または訂正されるように、あらゆる合理的な手段が講じられなければならない。
5	保管の制限の原則	個人データは、当該個人データの処理の目的に必要な範囲を超えて、データ主体の識別が可能な状態で保管してはならない。
6	完全性および機密性の原則	個人データは、当該個人データの適切なセキュリティを確保する方法で取り扱われなければならない。当該方法は、無権限の、または違法な処理に対する保護および偶発的な滅失、破壊、または損壊に対する保護も含むものとし、個人データの適切なセキュリティが確保される形で処理されなければならない。

また、管理者または処理者は、GDPR 第 6 条第 1 項が定める項目（表 6）のいずれかに該当しない場合には、個人データの処理を適法に行うことができない。すなわち、管理者または処理者は、表 6 の適法な処理の要件を満たした場合にのみ、処理を行うことが許される。

表 6：個人データの適法な処理の要件

	適法な処理の要件（GDPR 第 6 条第 1 項）
(a)	データ主体が 1 つ以上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与えた場合
(b)	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、または契約の締結前のデータ主体の求めに応じて手続きを履践するために処理が必要な場合
(c)	管理者が従うべき法的義務を遵守するために処理が必要な場合
(d)	データ主体、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
(e)	公共の利益、また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処理が必要な場合
(f)	管理者また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、特に子どもがデータ主体である場合の個人データの保護を求める基本的権利および自由が、当該利益に優先する場合を除く

これらの項目のうち、実務上、特に重要なものは、（a）の個人データ処理に関してデータ主体が同意を与えた場合といえる。「データ主体の同意」とは、自由に与えられた、特定的で、情報提供を受けた上で、かつ曖昧でないデータ主体の意思表示であることを意味する。その意思は、当該データ主体が、宣言または明らかな積極的行為によって、自己に関わる個人データの処理に合意して表すものとされている。

（a）以外の項目は、データ主体から直接同意を取得することができない場合、またはデータ主体から「同意」の定義や条件を満たす意思表示を得られない場合に、処理の適法性を基礎付けるために検討する必要がある。（a）と（b）から（f）の項目は並列の関係にあり、特に優劣関係がある訳ではないが、実務上は、データ主体から直接同意を取得できるケースでは、先ず、同意の取得を試みるのが通常であることから、このような順序で説明をしている。

(b)では契約の当事者として、「データ主体」本人が規定されていることに注意が必要である。そのため、データ主体の雇用者が契約当事者である契約の履行のために処理が必要な場合であっても、(b)の項目には該当しない。

（c）の法的義務は、EU 法または EU 加盟国法上のものを意味し、日本法や米国法などのその他の国・地域の法律に基づく義務はそれに該当しない。

（f）の管理者また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は、データ主体の個人データの保護を求める基本的権利および自由と、管理者または第三者による処理によって追及される正当な利益との比較考量を行い、後者が前者を上回る場合に、（f）の項目に該当することになる。この比較考量のテストの方法については、先行法令のデータ保護指令に基づいて設立された第 29 条作業部会の「データ保護指令第 7 条における個人データ管理者の正当な利益の

考えに関する 2014 年 4 月 9 日付意見書」[5]に詳しい説明があり、GDPR の解釈においても引き続き参考になる。実際のところ、企業が行う個人データの処理の多くは（f）の項目に基づいて処理の適法性が認められることとなるため、当該項目の重要性は高い。

なお、特別カテゴリーの個人データ（人種もしくは民族的素性、政治的思想、宗教的もしくは哲学的信条、または労働組合員資格に関する個人データ、および遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータ）は原則として処理が禁止されており、例外的に適用除外事由が定められている。

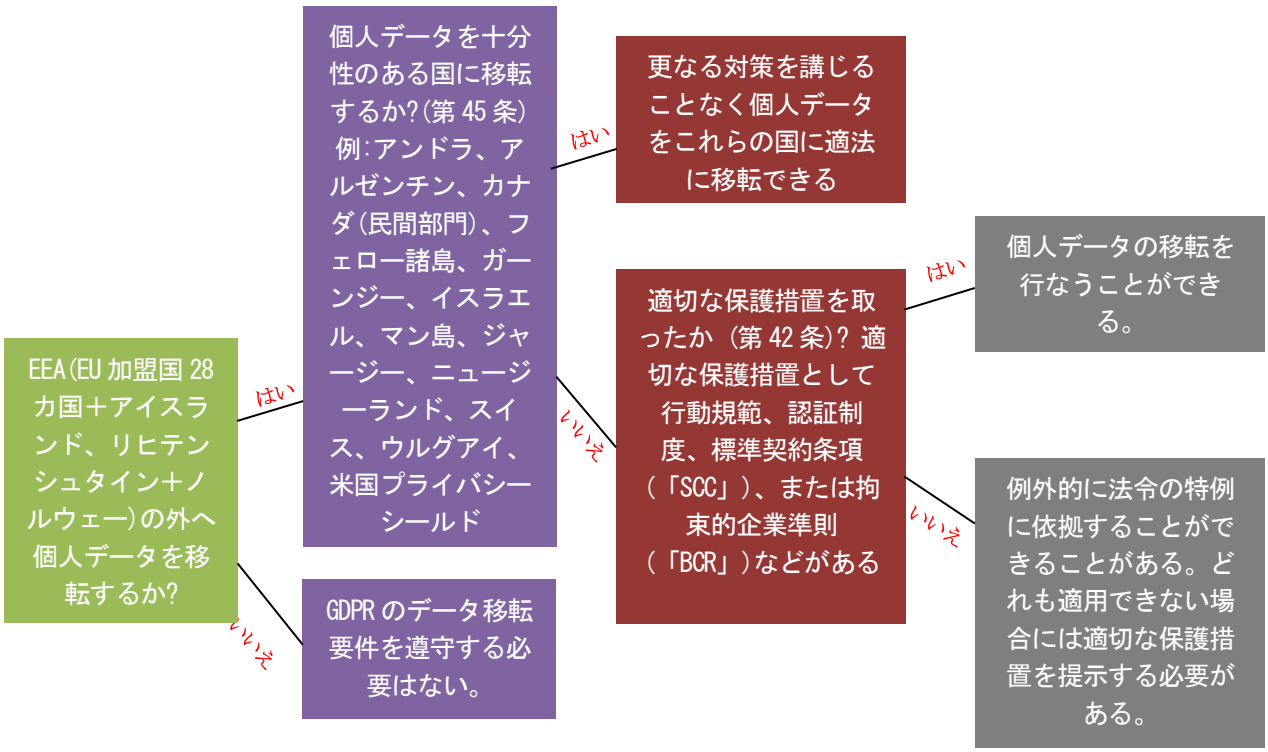
特に、上記（a）との対比では、特別カテゴリーの個人データに関しては適用除外事由に該当するにはデータ主体の明示的な同意が要求されており、また、上記（f）のような比較考量のテストは適用除外事由には含まれていない。これは特別カテゴリーの個人データに関して、通常の個人データに比べて適法な処理が認められる範囲が狭く規定されており、手厚く保護されていることを意味する。

[5] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf

3. 個人データの移転の法的要件

EEA 域外への個人データの移転は原則として違法である。移転先の国・地域に「十分性」（法整備などに基づき、十分に個人データ保護を講じていること）が認められた場合、または適切な保護措置を取った場合などには、例外的に適法となる。現状では、日本企業はデータ移転の複雑さと頻度を考慮し、標準契約条項（Standard Contractual Clauses: SCC）、または拘束的企業準則（Binding Corporate Rules: BCR）によって、データ移転規制を遵守することが望ましいと考えられる（SCC と BCR については Q24「『名刺』記載の個人データ」を参照）。移転に関する法的要件を図 4 にまとめる。

図 4：個人データの移転の法的要件



4. 制裁金

(1) GDPR に違反した場合の制裁－巨額の制裁金

GDPR 違反の場合の制裁金の上限額には、次の 2 とおりの類型がある[6]。

- 1,000 万ユーロ、または、企業の場合には前会計年度の全世界年間売上高の 2%のいずれか高い方
- 2,000 万ユーロ、または、企業の場合には前会計年度の全世界年間売上高の 4%のいずれか高い方

例えば、公的機関の場合、通常は売上高に該当するものがないため、1,000 万ユーロ以下か 2,000 万ユーロ以下という 2 つの類型の制裁金制度ということになる。また、例えば、前会計年度の全世界年間売上高が 100 億円の企業グループの場合、売上高の 4%は 4 億円だが、2,000 万ユーロ（約 22 億 6,000 万円。1 ユーロ＝113 円として換算）の方が「高い方」に当たるため、制裁金の上限額は 20 億円を超えるレベルになる。GDPR の制裁金の額が、企業経営や公的機関の運営を揺るがし兼ねない規模であることが分かる。

(2) GDPR 義務違反の類型と制裁金の上限額

上記の 2 とおりの制裁金の上限額は、各々表 7 にまとめる義務違反に適用される。

表 7：義務違反の類型と適用される制裁金の上限額

制裁金の上限額の基準	義務違反の類型
企業の全世界年間売上高の 2%、または、1,000 万ユーロのいずれか高い方（第 83 条(4)）	• 16 歳未満の子どもに対する直接的な情報社会サービスの提供に関する個人データの処理には、子に対する保護責任を持つ者による同意または許可が必要という条件に従わなかった場合（第 8 条） • GDPR 要件を満たすために適切な技術的・組織的な対策を実施しなかった、またはそのような措置を実施しない処理者を利用した場合（第 25 条、第 28 条） • EU 代理人を選任する義務を怠った場合（第 27 条） • 責任に基づいて処理行為の記録を保持しない場合（第 30 条） • 監督機関に協力しない場合（第 31 条） • リスクに対する適切なセキュリティレベルを保証する適切な技術的・組織的な対策を実施しなかった場合（第 32 条） • セキュリティ違反を監督機関に通知する義務を怠った場合（第 33 条）、データ主体に通知しなかった場合（第 34 条） • 影響評価を行なわなかった場合（第 35 条） • 影響評価によってリスクが示されていたにも関わらず、処理の前に監督機関に助言を求めなかった場合（第 36 条） • データ保護責任者（DPO）*を選任しなかった場合、または、その職や役務を尊重しなかった場合（第 37～39 条）

[6] なお、GDPR 違反の場合の監督機関による執行としては、行政制裁金の賦課のみならず、開示や監査といった調査、作為または不作為に関する遵守命令、処理の禁止、データ主体に周知させる命令、認証の撤回、および警告があり、常に行政制裁金が課せられるわけではない。

企業の全世界年間売上高の4%、または、2,000万ユーロのいずれか高い方(第83条(5))	• 個人データの処理に関する原則を遵守しなかった場合(第5条) • 適法に個人データを処理しなかった場合(第6条) • 同意の条件を遵守しなかった場合(第7条) • 特別カテゴリーの個人データ処理の条件を遵守しなかった場合(第9条) • データ主体の権利およびその行使の手順を尊重しなかった場合(第12-22条) • 個人データの移転の条件に従わなかった場合(第44-49条) • 監督機関の命令に従わなかった場合(第58条(1)および(2))

＊:Q19「企業内での責任者の任命など、組織体制面では、どのような対応が必要ですか？」を参照

＜定義・対象＞

- **Q1:GDPR が適用される個人データとは、どのようなデータを指しますか？**

GDPR において「**個人データ**」とは、識別された、または識別され得る自然人に関するすべての情報であると定義されています。識別された、または識別され得る自然人は「**データ主体**」と定義されます。「識別され得る自然人」とは、当該自然人の氏名、識別番号、所在地データ、オンライン識別子、または身体的・生理的・遺伝子的・精神的・経済的・文化的・社会的固有性などの中から、上記の識別因子のいずれかひとつ以上によって、直接または間接的に識別される個人のことをいいます。個人データの例は以下のとおりです。

- 自然人の氏名
- 識別番号
- 所在地データ
- メールアドレス
- オンライン識別子(IP アドレス/クッキー識別子)
- 身体的、生理学的、遺伝子的、精神的、経済的、文化的、社会的固有性に関する要因

ある自然人が識別され得るかどうかを判断するには、管理者やそれ以外の者が個人を直接または間接的に識別するために**合理的に使用可能なすべての手段を考慮する必要**があります。また、手段が、個人を識別するために合理的に使用可能であることを確認するためには、費用と時間のような**識別に必要な一切の客観的要因**および**処理の時点で利用可能な技術や技術的進歩**を考慮する必要があります。

個人の識別につながり得る情報かどうかという基準に照らして個人データに該当するか否かを判断することになります。

- **Q2:GDPR は誰に、どのような場合に適用されますか？**

GDPR は、個人データを処理するため、および個人データを EEA から第三国に移転するために満たすべき法的要件を規定しています。すなわち、GDPR が適用されるのは「処理」と「移転」の二つの場合です。

「処理」について

GDPR は、全体または一部が自動的な手段による個人データの**処理**、および、ファイリング・システム（機能的または地理的に集結、分散、あるいは拡散されているかに関わらず、特定の基準に基づいてアクセスできる、構造化された個人データの集合）の一部である、もしくはファイリング・システムの一部にすることが意図された個人データの自動的な手段以外の処理に適用されます。

「処理」とは、自動的な手段であるか否かに関わらず、個人データまたは個人データの集合に対して行われる、あらゆる単独の**作業**または一連の作業をいいます。この「作業」は、取得、記録、編集、構造化、保存、修正または変更、復旧、参照、利用、送信による開示、周知またはその他周知を可能にすること、整列または結合、制限、消去または破壊することをいいます。

より具体的には、クレジットカード情報の保存、メールアドレスの収集、顧客の連絡先詳細の変更、顧客の氏名の開示、上司の従業員業務評価の閲覧、データ主体のオンライン上の識別子の削除、および全従業員の氏名、社内での職務、事業所の住所および写真を含むリストの作成も「処理」に該当します。

GDPR は、管理者が、個人データの処理に関係する諸原則を遵守することに責任を負い、かつ当該諸原則の遵守を実証することを義務付けています。すなわち、企業や団体の側に GDPR を遵守していることを証明することが義務付けられているのであり、この証明ができなければ、GDPR 違反が認定されやすいということです。

「移転」について

「個人データ」の「移転」の概念は、先行法令であるデータ保護指令および GDPR のいずれにも定義されていません。例えば、個人データを含んだ電子形式の文書を電子メールで EEA 域外に送付することは「移転」に該当します。EEA 域外への個人データの移転は原則として違法です。ただし、移転先の国・地域に十分性決定（移転先の国・地域で、法整備などに基づき、十分に個人データ保護を講じているとの認定）が既に行われている場合、または適切な保護措置を取った場合などに、例外的に適法となります。また、特例として例外的に適法になるケースも定められています。

- **Q3:GDPR が適用される地域はどこですか？**

GDPR は、処理が行われる場所が EEA 域内か EEA 域外どうかに関わらず、EEA 域内の管理者または処理者の**拠点**の活動に関連してなされる個人データの処理に適用されます。「拠点」とは、

「固定的な体制を通じて、実効的かつ現実に活動を実施する場合」を意味しています。固定的な体制の法的形態は判断要素とはなりません。拠点とは、支店、子会社または、その業務を遂行するために必要なすべての機器を備えた事務所をもつ個人も含まれます。

- **Q4:GDPR は中小・零細企業、公的機関、地方自治体、非営利団体にも適用されますか？**

GDPR は中小・零細企業、公的機関、地方自治体、非営利団体にも適用されます[7]。

公共の安全への脅威に対する保護および防止を含む、犯罪の防止、捜査、探知、起訴、または刑事罰を科すために所轄官庁が行う個人データの処理には GDPR は適用されませんが、所轄官庁による上記処理以外の個人データの処理には GDPR が適用されます。例えば、ある EEA 加盟国の警察署の職員が容疑者の個人データの入ったファイルを地下鉄の中に置き忘れて紛失した場合、個人データの処理に当たって GDPR が適用されます。

また、GDPR は外交および防衛政策を担う EEA の公的機関、ならびに EU の公的機関ではない EEA 域内に所在する日本国の在外公館（日本国大使館など）による個人データの処理は GDPR の適用を受けません。

- **Q5:EEA 域内に現地法人を置いていない場合も、GDPR の適用対象になりますか？**

そのとおりです。（i）EEA 域内のデータ主体に対して商品やサービスを提供する場合、および（ii）EEA 域内のデータ主体が EEA 域内で行う行動への監視に関連する処理には GDPR が適用されます。

- **Q6:企業の現地従業員の個人データも、GDPR の適用対象になりますか？**

[7] なお、個人データの処理行為の記録保持義務について 250 名未満を雇用している「企業」や組織については当該義務を免除する規定（第 30 条(5)）があります。しかしながら、「企業」の判断基準が文言どおり企業単体の規模で見るべきか、企業の最終親会社を頂点とする企業グループ全体での規模を基準として見るべきなのかは判然とせず、欧州委員会または第 29 条作業部会によるガイドラインにおいて解釈が明確にされることが望まれます。
仮に、「企業」を文言どおりに解すれば、多くの日本企業の EEA 域内の子会社は個人データの処理行為の記録保持義務を負わないことになりますが、この場合にも、EEA 域内の個人データについての管理者が 250 名以上を雇用する EEA 域外の法人とされる場合もあり得るため、EEA 域内の法人の規模が小さい場合でも、必ずしも EEA 域内の法人における個人データの処理行為の記録保持義務が免除されることにはならない点に留意が必要です。
また、「組織」については、例えば、ある公的機関のパリ駐在員事務所が 250 名未満を雇用している場合であっても、当該公的機関が全体で 250 名以上を雇用している場合には、個人データの処理行為の記録保持義務が免除されることにはなりません。

そのとおりです。GDPR は、個人の国籍や居住地に関係なく EEA 所在者の個人データの処理を適用対象としています。企業内の現地従業員は基本的に EEA 所在者であり、当該現地従業員の個人データの処理には GDPR が適用されます。但し、雇用関係の個人データの処理については、加盟国が個別の国内法等のルールを策定できることに注意が必要です。

- **Q7:GDPR を所管する当局とは何ですか？EU と EU 加盟国には各々どのような権限がありますか？**

各 EEA 加盟国は、GDPR の適用を監視する責任のある独立した国家機関を 1 カ所以上設置する必要があります。当該機関は「監督機関」と呼ばれます。監督機関の権限は以下のとおりです。

- 調査権限：監督機関は、管理者や処理者に対して必要な情報の提供を命じ、調査の遂行や認証の審査を行うことができる。
- 是正権限：監督機関は、データ主体の要請の遵守を命じ、処理の限定を課し、データフローの停止を命じ、厳しい制裁金を課すことができる。
- 管理者または処理者は、監督機関と協力する義務がある。

GDPR は、欧州委員会競争総局が執行機関を務める EU 競争法とは異なり、EU レベルでの執行機関を持ちません。

これに対し、EU レベルにおいて、各加盟国の監督機関の代表、欧州データ保護監察機関（European Data Protection Supervisor: **EDPS**）の代表から構成される「欧州データ保護会議」（European Data Protection Board：**EDPB**）が、諮問機関および上級委員会の役目を務めます。EDPB は、諮問機関として、監督機関が以下を行おうとする場合に、意見を提供するものとされています。

- 個人データ保護の影響評価のための要件の対象となる処理業務のリストを採用する場合
- 数カ国の加盟国での処理活動に関連する行動規範を承認する場合
- 標準契約条項（SCC）を決定する場合
- 契約条項を承認する場合
- 拘束的企業準則（BCR）を承認する場合

（SSC および BCR については Q24「『名刺』記載の個人データ」を参照のこと）

EDPB は上級委員会として以下の場合に拘束力を持つ決定をするものとされています。

- 監督機関間で草案に関する意見の相違がある場合
- 監督機関間で管轄に関する意見の相違がある場合

- 監督機関が、義務であるにも関わらず、EDPB に意見を求めない場合、または意見に従わない場合

- **Q8:複数の EEA 加盟国で事業を行っている場合、あるいは EEA 域内に拠点が存在しない場合、どの当局が所管（手続きの窓口）となりますか？**

各監督機関は、原則として、GDPR に従って当該監督機関に対して割り当てられた業務の遂行、および当該監督機関に付与された権限の行使に関して当該監督機関の加盟国の領域において管轄権を有するものとされます。

また、主たる拠点、または、管理者もしくは処理者の単一の拠点の監督機関は、当該管理者または処理者によって実行される、EEA 域内の国境を越える個人データの処理に関する主要監督機関としての活動の管轄権を有するものとされます。

従って、複数の EEA 加盟国で処理を行っている場合は、原則として主たる拠点の監督機関が管轄権を有することになります。ただし、各監督機関は、対象事項が監督機関の加盟国内にある拠点にだけ関係しているか、または、対象事項が実質的に監督機関の加盟国内に所在するデータ主体だけに影響を及ぼしている場合は例外的に、監督機関への苦情申立て、または GDPR に対する違反が発生した場合に管轄権を有することになります。

ここで、「主たる拠点の監督機関」は、国境を越えた処理における主要監督機関としての役割を果たす唯一の窓口となります。主たる拠点の監督機関は、管理者および処理者いずれの場合でも、原則として EEA 域内の統括拠点が所在する場所の監督機関をいいます。ただし、これは、管理者については、個人データの処理の目的および手段の決定が EEA 域内の管理者の統括拠点で行なわれておらず、統括拠点が実施決定に権限を持っていない場合に限り、この決定が行われる拠点が主たる拠点になると考えられます。また、処理者については、処理者が EEA 域内の統括拠点を持たない場合には、処理者に対して GDPR が定める特定の義務が適用される限りにおいて、処理者の拠点の活動に関連する主な処理業務が行われている EEA 域内の処理者の拠点をいいます。

EEA 域内に拠点が存在しない場合には、主要監督機関はなく、処理を行う個人データを提供した、データ主体が所在する場所や苦情申立てがなされた監督機関が窓口ということになるものと思われますが、この点や上記の点については、2016 年末までに第 29 条作業部会がガイドラインを出すものとされているため、当該ガイドラインを参照することが望ましいと考えられます。

- **Q9:企業としての GDPR への対応について、GDPR の適用の日程や今後の予定はどうなっていますか？**

GDPR は、2018 年 5 月 25 日付けで適用開始される予定です。しかし、GDPR を遵守するには時間が掛かるため（例：従業員の教育、適切な保護措置の実施、情報通知のドラフト、データ移転方法の検討など）、早めに対応を行うことが望ましいと考えられます。

フランスでは、GDPR の施行に先立って、デジタルリパブリック法案というフランスのデータ保護法を GDPR の内容に近づける改正法案が 2016 年 10 月 6 日に可決されました。この改正法案の内容として注目すべき点は、フランスの個人データ保護監督機関が課すことのできる制裁金の上限額が 300 万ユーロ（約 3 億 3,900 万円。1 ユーロ＝113 円として換算）に引き上げられている点です。加盟国によっては、このように 2018 年 5 月に先立って監督機関の権限を強化している点に注意が必要です。

- **Q10:そもそも、GDPR のような規制が必要となった理由と目的を教えてください？**

EU においては個人データの処理に関連する自然人の保護は EU 基本権憲章という EU 法体系の根幹をなす法によって基本的人権とされています。この基本的人権を保護することがデータ保護法の目的です。技術の急速な発展とグローバル化は、この基本的人権の保護に新しい課題をもたらしました。そのため、この基本的人権をより強固に保護するために EEA 域内での新たな個人データ保護の枠組みが必要となり、GDPR のような規制が必要とされたものと考えられます。

＜個人データの移転＞

- **Q11:EEA 域内から域外に個人データを移転する場合、GDPR が適用されるとのことですが、どのような行為が個人データの移転に該当しますか？**

Q2 の回答にあるとおり、個人データの「移転」の概念は、データ保護指令および GDPR のいずれにも定義されていません。例えば、個人データを含んだ電子形式の文書を電子メールで EEA 域外に送付することは「移転」に該当します。EEA 域外への個人データの移転は原則として違法です。移転先の国・地域に十分性決定（移転先の国・地域で、法整備などに基づき、十分に個人データ保護を講じていると認定すること）が既に行われている場合、または適切な保護措置を取ったなどの場合に、例外的に適法となります。また、特例として例外的に適法になるケースも定められています。

- **Q12:個人データの移転は、個人データが通過するサーバの設置場所にも関係ありますか？**

関係があります。例えば、フランスの拠点の従業員がドイツの拠点の別の従業員に対し、個人データを含む電子メールを送信する場合、そのメールが日本本社のメールサーバを経由して届く場合（フランス→日本→ドイツ）、EEA 域外への個人データの移転が行われたと考えられ、GDPR 上の個人データの移転を適法化するための対策を採る必要が出てきます。

- **Q13:クラウドなどのオンライン・サービスは、GDPR では、どのように扱われますか？**

クラウドなどのオンライン・サービスを利用する場合、管理者が個人データをクラウド・サービスのプロバイダー（処理者）の保有するクラウド・サーバに預けるという形になります。管理者は処理者との間で書面での処理契約を締結する必要があります。また、処理者が EEA 域外に所在する場合、管理者（個人データの輸出者）は EEA 域外に所在するクラウド・サービスのプロバイダー（個人データの輸入者・処理者）に対して EEA 域内で取得した個人データを移転させることになるため、欧州委員会決定 2010/87/EC[8]が定める標準契約条項（SCC、詳細は Q24「『名刺』記載の個人データ」を参照のこと）を締結する必要があります。

＜罰則＞

- **Q14:GDPR に違反した場合、罰則などはありますか？**

「I. 概要編」にもあるとおり、GDPR 違反の場合の制裁金の上限額には次の 2 とおりの類型があります。なお、GDPR 違反の場合の監督機関による執行としては、行政制裁金の賦課のみならず、開示や監査といった調査、作為または不作為に関する遵守命令、処理の禁止、データ主体に周知させる命令、認証の撤回、および警告があり、GDPR 違反の場合に常に行政制裁金が課せられるわけではありません。

  - 1,000 万ユーロ以下または、企業の場合には前会計年度の全世界年間売上高の 2%以下のいずれか高い方
  - 2,000 万ユーロ以下または、企業の場合には前会計年度の全世界年間売上高の 4%以下のいずれか高い方

例えば、公的機関の場合には、通常は売上高に該当するものがないため、1,000 万ユーロ以下か 2,000 万ユーロ以下という 2 つの類型の制裁金制度ということになります。また、例えば、前会計年度の全世界年間売上高が 100 億円の企業グループの場合、全世界年間売上高の 4%は 4 億円ですが、2,000 万ユーロ（約 22 億 6,000 万円。1 ユーロ＝113 円として換算）の方が「高い方」に当たる

[8] http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32010D0087

ため、制裁金の上限額は 20 億円を超えるレベルになります。GDPR の制裁金の額が、企業の経営を揺るがし兼ねない規模の大きさであることが分かります。

- **Q15:GDPR 違反に対する制裁金の金額はどのように算定されますか？**

制裁金の金額についての判断を行うに当たって、監督機関は確実に、制裁金が相応の金額であり、抑止力を有するようにする必要があります。そのため、監督機関は以下の基準を考慮しなければなりません。

a) 問題となる処理の性質、範囲、または目的、影響を受けるデータ主体の数、およびデータ主体が被った損害のレベルを考慮した、違反の性質、重大さおよび期間
b) 違反の故意性または過失性
c) データ主体が被った損害を緩和するために管理者または処理者が講じた措置
d) GDPR 第 25 条（設計によるまたは初期設定によるデータ保護）および第 32 条（処理のセキュリティ）に基づき実行された技術的および組織的対策を考慮した、管理者または処理者の責任の程度
e) 管理者または処理者による関連する過去の違反
f) 違反を是正し、違反によって生じ得る悪影響を緩和するための、監督機関との協力の程度
g) 違反によって影響のある個人データの種類
h) 監督機関が違反を知ることになった経緯、特に、管理者または処理者が監督機関に違反を通知していたかどうか、通知していた場合、どの程度通知を行ったか
i) GDPR 第 58 条第 2 項（監督機関の是正権限）に定める方策が、過去に管理者または処理者に対して同じ係争に関して命じられていた場合、当該方策への遵守
j) 承認を受けた行動規範、または承認を受けた認証手続きへの遵守
k) 違反によって直接または間接に、獲得した金銭的利益、被らずに済んだ損害などの事案に応じたその他の加重、または軽減事由

＜対策＞

- **Q16:GDPR への基本的な対策として、実務上、何に留意すべきでしょうか？**

GDPR への基本的な対策として重要なのは、「データ・マッピング」と GDPR と現状のコンプライアンスの状況に関するギャップ分析と言えるでしょう。GDPR への対応の主なステップと内容は、表 8 のとおりです。

表 8：GDPR への対応の主なステップと内容

ステップ	内容
対応状況の把握	▪ データ・マッピング - 企業グループの本社、子会社、支店などにおいて処理される EEA で取得した個人データの処理の目的、種類(特別カテゴリーの個人データの有無)および量と内容を、各々の本社、子会社、支店などに質問票を送付・回収すること、またはフォローアップのインタビューを行うことで把握する。 ▪ 法令、ガイドラインなどにおける要求事項の洗い出し ▪ 資料調査やインタビューによる評価の実施 ▪ 評価結果の整理
ギャップ分析	▪ 要求事項と対応状況を把握した結果を比較 ▪ 要求事項との相違を識別し、優先順位付けをする
対応方針の策定	▪ 現在の対応状況を踏まえて対応方針を検討 ▪ 実施に要するコストなどを考慮し、対応方針を策定
対応策の実施	▪ 適切な手続き、管理体制、技術面での対応策の実施

先ず、企業グループ内で EEA 域内に所在する個人の個人データをどのような目的で処理するのかをデータ・マッピングにより明確化し、網羅的な対策を取る土台作りを行うことが必要です。また、GDPR から導き出される要求事項に照らして、企業グループ内の個人データ保護コンプライアンスの対応状況がどこまで進んでいるかを評価し、その評価結果について優先順位をつけることで、どのような順番で GDPR 対応を進めるべきなのかが明確化されます。その上で、優先順位と実際の実施に要するコストを考慮した上で、対応方針を策定することになります。GDPR の企業に対する適用開始日（2018 年 5 月 25 日）より前に、すべての対応策が実施できることが望ましいですが、難しければ、優先順位の高いものだけでも、この日までに対応策を実施しておくことが肝要です。

- **Q17:個人データの EEA 域外への移転には、当該個人からの同意が必要とのことですが、具体的にどのような形式で取得すれば良いでしょうか？**

GDPR では、同意には二つの種類があり、「個人データの処理の適法性の根拠としての同意」、そして「個人データの EEA 域外への移転を適法化するための同意」です。後者は、前者の要件をすべて満たした上で、さらに「十分性決定および適切な保護措置がないことによって、当該移転によってデータ主体に対して生じ得るリスクについて情報提供を受けた後、データ主体がその提案された移転に明示的に同意」することが必要とされています。

先ず、前者の要件（個人データの処理の適法性の根拠としての同意）について説明します。

「データ主体の同意」とは、「データ主体が、宣言または明らかな積極的行為によって、自己に関するの個人データの処理に合意して表す、自由意思による、特定的で、情報提供に基づく、曖昧でない意思表示」を意味します。

個人データの処理の適法性の根拠となる同意を取得する際には、上記の「データ主体の同意」に該当するかどうか、特に、表 9 で示した同意の条件を満たしているかのチェックが重要です。GDPR 違反を含んだあらゆる宣言は拘束力がないものとされているためです。沈黙や、予めチェックマークが記入されているボックス、不作為では同意をしたものとみなすことはできません。

表 9：データ主体の同意の条件

	同意の条件（GDPR 第 7 条）
1	処理が同意に基づく場合、管理者は、個人データ主体が自己の個人データの処理に対して同意しているということを証明できるようにしなければならない。
2	個人データ主体の同意が他の案件にも関係する書面において与えられている場合、その同意の要求は、明瞭かつ平易な文言を用い、理解しやすくかつ容易にアクセスし得る形で、その他の案件と明らかに区別できる方法によって明示されなければならない。
3	データ主体は、同意を与える以前に以下の事項が通知されていなければならない。同意の撤回は、その付与と同程度に容易なものでなければならない。 ▪ データ主体は、いつでも同意を撤回する権利があること。 ▪ 同意の撤回は、撤回前の同意に基づく処理の適法性に影響を与えない。
4	同意が自由意思によりなされているかについて判断する際、サービス約款を含む契約の履行が、当該契約の履行に必要のない個人データの処理に対する同意を条件としているか否かについて、最大限の考慮が払われなければならない。

データ主体から個人データを収集する場合、管理者は、データ主体に以下の情報を提供しなければなりません。ただし、データ主体が既に当該情報を有している場合を除きます。

- 管理者と（該当する場合には）代理人および／またはデータ保護責任者（DPO、Q19「企業内での責任者の任命など、組織体制面ではとして、どのような対応が必要ですか？」を参照）の身元および連絡先詳細
- 処理の目的および法的根拠
- 処理の法的根拠としての管理者または第三者が追求する正当な利益
- 個人データの受取人または受取人の種類
- 管理者の EEA 域外の第三国または国際組織への個人データの移転の意思、および十分性決定の有無、または（該当する場合には）適切な保護措置への言及や当該コピーの入手方法、または入手先
- 個人データの保管期間、期間の決定ができない場合には決定の基準
- 監督機関に苦情を申し立てる権利を含めた、データ主体の権利
- 同意をいつでも撤回することができる権利
- プロファイリング（自然人の個人的な側面を評価するため、または、自然人の職務業績や経済状態、健康状態、個人的な嗜好、関心、信頼性、行動、所在、移動などを分析したり、評価したりするために個人データを利用する、あらゆる形式の個人データの自動

的な処理）および処理に利用するロジックに関する有意な情報や、データ主体に対する処理の意義や想定上の結果を含む、自動化判断（automated decision-making）の有無

- 個人データの提供が、法律上または契約上の義務、または契約を締結するのに必要な要件であるか否か、およびデータ主体に個人データの提供の義務があるか否か、ならびに、当該データ提供の不履行により起こり得る結果

次に、後者（「十分性決定および適切な保護措置がないことによって、当該移転によってデータ主体に対して生じ得るリスクについて情報提供を受けた後、データ主体がその提案された移転に明示的に示す同意」）の要件についてですが、明示的な同意があったといえるためには、個人データを EEA 域外へ移転させることを説明した上で、この移転に対し同意するかどうかを「はい」または「いいえ」で回答させることが典型的な形となります。これについては、チェック欄を設けて、「このチェック欄にチェックを入れた場合には、当該個人データの日本への移転について明示的に同意したものとみなします」としてチェックをさせるといった形が考えられます。

同意の証明については、第 29 条作業部会が 2017 年中にガイドラインを公表することを示唆しているため、当該ガイドラインの公表の動向についても注意することが必要です。

- **特定の状況における特例 (第 49 条)**

個人データの移転のための同意は、以下（表 10）のとおり、特定の状況における特例の一例です。また、必要性に基づいて移転が認められる場合もあります。

表 10：特定の状況における特例の例

データ主体による同意（第 49 条(1)(a)）	▪ 十分性の判断または保護措置が不在の場合、データ主体が明示的に同意すれば移転を行うことができる
必要性に基づいて移転が認められる場合（第 49 条(1)(b)-(f)）	▪ データ主体と管理者の間の契約の履行のため、またはデータ主体の要請により講じる契約前の措置の実施のため ▪ 管理者とその他の個人との間で、データ主体の利益のために交わされる契約の締結または履行のため ▪ 公共の利益の重大な事由があるため ▪ 法的主張の立証、行使または抗弁のため ▪ データ主体が身体的または法的な理由で同意できない場合に、データ主体またはその他の個人の重要な利益を保護するため

データ主体による同意は制約の大きい特例

EEA 域内のデータ保護監督機関は、従業員が有効な同意を行えるか、特に、当該同意が「任意の」ものといえるかどうかについて非常に懐疑的な立場を取っています。

少なくとも、従業員の個人データについては、同意により移転を行うことには一定のリスク(従業員からの苦情申立を監督機関が受けた場合に、監督機関が調査を行うリスクなど)があると考えられています。

データ主体の同意のみの対応とする場合の留意点については、以下の事項を踏まえ、リスクがあると判断した場合にはSCCを利用することが望ましいと考えられます。

- データ主体がいつでも同意を撤回できる
- 文書中の個人データに関するすべてのデータ主体が同意する必要があるため、事実上、同意の取得が不可能な場合が多くあり、十分な移転規制の遵守が困難(例：自社の努力では同意取得が困難なデータ主体の個人データが文書中に多く含まれている場合)
- 第29条作業部会によれば、繰り返し行なわれ、大量で、かつ構造的であると認められる可能性がある個人データの移転は、可能であればSCCやBCR（Q24「『名刺』記載の個人データ」を参照）のような適切な保護措置の下で行なわれるべきである

特定の状況での従属的特例(第49条(1)後段)

特定の状況での従属的特例は、要件が限定的であり、ガイドラインなどで当該従属的特例の使用例が示されることが望ましいと考えられます。

また、第49条(1)(a)-(g)が定める特例が適用できない場合であっても、下記1)および2)の条件を満たす場合、EEA域外の第三国へ個人データを移転することができます。この場合、管理者は、当該個人データの移転に関する監督機関に対する通知、および、データ主体に対する、移転と当該移転を行わなければならない、やむにやまれぬ正当な利益に関する通知を行わなければなりません。

1) 移転が以下のすべての条件を満たすこと
    - 移転が繰り返し行われないこと
    - 限定された数のデータ主体のみに関わること
    - データ主体の利益または権利および自由が優越することのない、管理者が追求する、やむにやまれぬ正当な利益の目的のために、移転が必要であること
2) 管理者が個人データの移転を取り巻くすべての状況を評価し、この評価に基づき、個人データの保護に関してふさわしい保護措置を提供すること

- **Q18:インターネット取引など、ホームページ経由で、EEA域内の個人データを域外に移転する場合、具体的にどのように当該個人から同意を取得すれば良いでしょうか？**

個人データの処理には、データ主体の不明瞭でない同意が必要となりますが、同意に依拠して個人データを移転するためには「十分性決定および適切な保護措置がないことによって、当該移転によってデータ主体に対して生じ得るリスクについて情報提供を受けた後、データ主体がその提案された移転に明示的に同意」することが必要です。

個人データの移転への同意は明示的である必要があるため、企業はデータ主体が同意を黙示的に表示する行為には依拠することができません。そのため、ホームページ（インターネット取引）経由でデータ主体から有効な同意を得るための適切な方法は、データ主体から同意を得る旨のチェック欄および「本欄にチェックマークを入れることで、あなたの個人データを EEA 域外に移転することに同意するものとします。この同意によって、欧州委員会が個人データ保護の十分性決定を行っていない国へ、標準契約条項などの保護措置なしに当該データが移転されることを意味します。当社においては送信先の国に関わらず、個人データを保護致します」といった文言を含める必要があります。データ主体は、ボックスにチェックマークを入れ、EEA 域外に自分の個人データが移転されることに同意することになります。

ここで留意すべきことは、個人データの移転の根拠として使われる同意には、個人データの処理に使われる同意と同じ要件が充足される必要があることです。また、移転が大量に繰り返される場合には、第 29 条作業部会が同意に依拠することを抑制することを薦めていることにも留意が必要です。

- **Q19:企業内での責任者の任命など、組織体制面ではどのような対応が必要ですか？**

以下の場合には、データ保護責任者（Data Protection Officer：DPO）を選任する必要があります。

- 処理が公的機関または公的団体によって行われる場合（司法機関としての裁判所の行為を除く）
- 管理者または処理者の中心的業務が、その性質、適用範囲および／または目的によって、大規模にデータ主体の定期的かつ系統的な監視を必要とする処理作業である場合
- 管理者または処理者の中心的業務が、特別カテゴリーの個人データ（人種もしくは民族的素性、政治的思想、宗教的もしくは哲学的信条、または労働組合員資格に関する個人データ、および遺伝データ、自然人の一意な識別を目的とした生体データ、健康に関するデータまたは自然人の性生活もしくは性的指向に関するデータ）ならびに有罪判決および犯罪に関する個人データを大規模に処理する場合
- EU 法または加盟国の国内法で DPO の選任が義務付けられている場合
    - ドイツの連邦データ保護法（本レポート校了時点：2016 年 11 月 14 日）では、10 名以上の従業員が個人データの自動処理（パソコンによる個人データの処理）を行っている場合、または 20 名以上の正社員が個人データ処理を行っている場合に DPO の選任義務があるため、現在は非常に広範囲のドイツに所在する企業に DPO の選任義務がある（例えば、多くの日本企業がデュッセルドルフに拠点を有する

と思われるが、デュッセルドルフの事業所の個人データの処理の状況を確認することなどが、ドイツにおける DPO の選任義務の有無を確認する上で必要と考えられる）

- 今後、同法における DPO の選任義務の要件は多少絞り込まれると予想されるが、依然として多くの企業が DPO の選任義務を負うことになると考えられる

GDPR における、DPO の規定は概ね表 11 にまとめるとおり（第 37～39 条）。

表 11：DPO の主な規定

DPO の任務 （第 39 条）	▪ 少なくとも第 39 条第 1 項に列挙された任務、例えば、GDPR と、その他の EU および加盟国の条項に基づく義務について、管理者・処理者および個人データを処理する従業員に対して、情報と助言を提供すること、管理者・処理者の個人データ保護指針の遵守を監視することなど行う
DPO の選任 （第 37 条）	▪ 専門家としての質、特にデータ保護法およびその実務の専門知識、ならびに任務を遂行する技量に基づいて選任されるものとし、管理者または処理者の従業員、または、業務委託契約に基づいて任務を遂行するものでも良い
DPO の地位 （第 38 条）	▪ 管理者・処理者は、DPO が個人データの保護に関する一切の事柄について適切、適時に取り組めるように保証する ▪ 管理者・処理者は、DPO が任務の遂行に関する指示を一切受けないようにしなければならず、DPO は、当該任務の遂行について管理者・処理者から解雇または処罰を課されない ▪ DPO は、管理者または処理者の最高経営レベルに直接報告を行う ▪ DPO は、その他の任務や義務も遂行できるが、管理者・処理者は、そのような任務や義務が利益相反にならないことを保証しなければならない

また、管理者または処理者は、DPO を選任した場合、DPO の連絡先詳細を公表し監督機関に通知する必要があります。なお、第 29 条作業部会は、DPO について 2016 年末までにガイドラインを発表する予定です。

- **Q20:企業内の「個人データ保護責任者（DPO）の所属（常駐勤務地）は日本本社でも良いでしょうか？選任された DPO は、どの所管当局に届け出る必要がありますか？**

企業グループは、DPO が各拠点から容易にアクセスできる限りにおいて、EEA 域外に勤務する DPO を選任することができると考えられます。従って、DPO が日本本社に常駐する場合にも、EEA 域内にある当該企業グループの拠点から容易にアクセスができる限り、GDPR の観点からは問題がないと考えられます。ただし、この点の結論は、GDPR の文言上、明確に記載されている訳ではないため、前述の DPO について 2016 年末までに第 29 条作業部会が策定するガイドラインを参照することが望ましいと考えられます。

- **Q21:個人データで本人が識別されることが問題ならば、「社員番号」や「顧客番号」など記号・暗号などを活用し、匿名化する対応は可能ですか？**

GDPR が定める要件を満たすのであれば、「匿名化」は有効な対応になると考えられますが、第29 条作業部会は匿名化技術に関する意見書の中で、匿名化が認められる場合を狭く解するという立場を表明しており、GDPR においても匿名化の要件は満たすのが容易ではないことに注意が必要です。質問のように「社員番号」「顧客番号」を使った記号化・暗号化は不可逆的な特定の防止ではなく、「匿名化」したものと評価されない恐れがあるものと考えられます。

「匿名化」とは不可逆的に識別を防止するものです。匿名化されたデータである「匿名化データ」は、個人の識別につながり得る情報ではなく「個人データ」に該当しないため、GDPR の適用を受けません。

これに対し、「仮名化」とは、識別されたまたは識別可能な自然人に属さないことを保証するために、追加情報は別途に保管され、技術的および組織的対策の対象になっている限り、当該追加情報なしには個人データが特定のデータ主体に属するものと判断できないように個人データを処理することをいいます。通常、仮名化データは、不可逆的に識別が防止されたものではなく、依然として「個人データ」に該当します。

個人データを暗号化した場合、通常、暗号化されたデータは、暗号を解く鍵なしでは、個人の識別につながり得ない情報となりますが、暗号を解く鍵が存在する限りにおいて、個人の識別が不可逆的に防止された訳ではないため、「匿名化データ」には該当しません。その結果、暗号化されたデータは、依然として「個人データ」に該当するため、暗号化されたデータの処理および移転についてはGDPR が適用されることになります。

これに対して、当該暗号を解く鍵が廃棄されていている場合には、当該暗号化されたデータは不可逆的に個人の識別につながり得ない情報であり、「匿名化データ」に該当し、「個人データ」には該当しません。もっとも、この場合、企業においても、この暗号化されたデータが誰に関するものか分からなくなるため、このデータを活用することができるのかどうかという問題が出てくるものと考えられます。

- **Q22:信頼関係に基づく個人データの移転**

当社（日本国内法人）は、EEA 域内の顧客から「挨拶状」や「クリスマスカード」を貰った場合、それらに記載された個人データ（住所・氏名・メールアドレス）を日本側で営業目的のためもあって管理しています。相手方の要望もあり、商品カタログなどを記載住所に送付することもありますが、相手方の要望なのだから、GDPR の観点でも問題ないと考えていますが、いかがでしょうか？
【個人データ取得の経緯：挨拶状・クリスマスカードなどのレター】

問題ありません。貴社が EEA 域内の顧客から「挨拶状」や「クリスマスカード」を受領する場合、取引関係に基づいて EEA 所在者の個人データを取得することになりますが、取得したデータを貴社において営業目的のために管理するという処理行為については、相手方の要望から当該 EEA 域内の顧客による同意しているものと考えることが可能と考えられます。また、当該 EEA 域内の顧客が貴社に対して商品カタログなどを記載住所に送付することを要望した場合、貴社が当該個人データを使用して商品カタログなどを当該顧客に送付するという処理行為に対して、当該顧客は同意をしているものと考えられます。従って、当該処理行為については GDPR の観点からは問題がありません。

- **Q23:「インターネット取引」での個人データの移転**

当社（日本国内法人）は国内で旅館を営業しており、インターネット経由で個人データ（住所・氏名・クレジットカード番号など）を登録して貰い、取引管理しています。利用者には EEA 域内の方々も含まれます。特に宿泊者が旅館に個人データを提出するのは当たり前との認識で、インターネット・サイト上で「（個人データの EEA 域外への移転について）同意を取得するプロセス」は入れていませんが、GDPR の観点で問題はありますか？
【個人データ取得の経緯：ホームページ（インターネット取引）】

問題がある可能性があります。貴社が、EEA 域内所在者向けにインターネット上で、EU 言語（英語、フランス語など）で旅館への宿泊に当たってのサービスという商品・サービスを提供している場合には、日本国内で旅館を営業しているだけであっても、GDPR の適用が問題となる可能性があります。その場合、EEA 所在者がインターネット経由で個人データ（住所・氏名・クレジットカード番号など）を貴社に対して登録し、貴社が当該個人データを取得することは、EEA の個人データの直接取得、即ち EEA の個人データの処理に当たり GDPR を遵守する必要が出てくるものと考えられます。

この場合、適法な処理の要件が問題となりますが、貴社と宿泊者の間では宿泊サービスに関する契約が締結されるのが通常と考えられ、「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、または、契約締結前にデータ主体の求めに応じて手続きを履践するために処理が必要な場合」に該当するものとして、上記個人データの直接取得については処理の適法性が満たされるものと考えられます。

なお、貴社は、処理の適法性が問題ないとしても、その他の GDPR 上の義務、例えば、**個人データ侵害**の場合における監督機関に対する 72 時間以内の通知義務など、EEA 所在者の個人データを処理することから発生する諸々の義務の遵守を行うように、対応を行うことが望ましいものと考えます。

- 個人データの侵害の監督機関への通知

個人データの侵害とは、移転、保存またはその他の取り扱いがなされた個人データに対する偶発的な、または違法な破壊や滅失、変更、許可されていない開示、アクセスをもたらすセキュリティ侵害のことをいいます。個人データの侵害の例としては、サイバー攻撃により自社サーバに保管された EEA 所在者の個人データが漏洩した場合などが考えられます。

管理者は、個人データの侵害が発生した場合、自然人の権利および自由に対してリスクが生じ得る侵害を、不当な遅滞なく、可能であれば侵害を認識してから 72 時間以内に監督機関に通知しなければなりません（処理者は、個人データの侵害を認識した後、不当な遅滞なしに管理者に通知しなければなりません）。また、監督機関への通知が 72 時間以内になされない場合には、遅滞に関する理由も通知しなければなりません。当該通知には、少なくとも以下の事項を含めなければなりません（表 12）。当該通知義務に違反した場合、1,000 万ユーロまたは前会計年度の全世界年間売上高の 2%のいずれか高い方を上限額とする制裁金が課される可能性があります。

表 12：個人データの侵害の監督機関への通知において含めなければならない内容

	GDPR 第 33 条第 1 項の通知に最低限含めなければならない事項（同条第 3 項）
(a)	個人データの侵害の性質に関する記述、可能であれば、関連するデータ主体の種類と概数。関連する個人データの記録の種類と概数を含む。
(b)	DPO の氏名および連絡先の詳細、または、さらなる情報が入手できるその他の連絡先
(c)	個人データの侵害の結果、生じ得る結果に関する記述
(d)	個人データの侵害に対処するために、管理者によって取られている対策、または取られることが予定されている対策の記述。必要に応じて、個人データ侵害により起こり得る悪影響を軽減するための対策を含む。

他方で、通知と同時に情報（上の GDPR 第 33 条第 3 項各号記載の事項に該当する情報を意味すると解されますが、文言上は必ずしも明らかではありません）を提供することが不可能である場合、情報はさらなる遅滞なしに段階的に提供されても良いとされています。

- データ主体への個人データの侵害の通知

管理者は、個人データの侵害が自然人の権利および自由に対して高いリスクを引き起こし得る場合、不当な遅滞なしにデータ主体に個人データの侵害について通知しなければなりません。当該通知義務に違反した場合、1,000 万ユーロまたは前会計年度の全世界年間売上高の 2%のいずれか高い方を上限額とする制裁金が課される可能性があります。管理者は、次のいずれかの状況に合致する場合には、上記通知を行う必要はありません（表 13）。

表 13：データ主体への通知が不要となる場合

	GDRR 第 34 条第 1 項のデータ主体への通知が不要となる場合（同条第 3 項）
(a)	**管理者が、暗号化のように個人データへのアクセスを許可されていないあらゆる人に対して、個人データが判読できないようにするといった対策を始めとする、適切な技術的および組織的保護対策を、個人データの侵害によって影響を受ける個人データに適用している場合**
(b)	**管理者が、自然人の権利および自由に対する高いリスクが具体化し得ないことを確実にする事後的措置を取った場合**
(c)	**過度な労力を要する場合。この場合、代わりとして、データ主体が等しく効果的手法で通知されるように、公的な通信またはそれに類似する対策を取らなければならない**

個人データの侵害の監督機関への通知について、通知義務違反の場合に制裁金が課せられるという制度は、GDPR が初めて導入するものではありません。代表的なものとしては、すでに英国やオランダが導入しており、英国では豊富な執行事例があります。従って、GDPR の施行を待たずに対策を採ることが重要です。

また、侵害を認識してから 72 時間以内に監督機関へ通知するという義務は、平時から準備がなされていなければ、時間内での対応は難しいのが実情ではないかと考えられます。個人データの侵害の監督機関への通知義務への対応をきっかけとして貴社内で個人データのセキュリティ対策を改めて評価し直し、有事の場合に迅速に動けるように準備をしておくことが肝心と考えます。

- 処理のセキュリティ

管理者および処理者は、リスクに見合ったセキュリティレベルを確保するために、到達水準と実施コスト、処理の性質、範囲、文脈、目的、ならびにデータ主体の権利と自由に対するさまざまな可能性と重大性のリスクを考慮し、「適切な技術的および組織的対策」を実施しなければなりません。「適切な技術的および組織的対策」には、必要に応じて、(a)個人データの仮名化および暗号化、(b)処理システムおよびサービスの継続中の機密性、完全性、可用性および復旧を確保する能力、(c)物理的または技術的事故の際、個人データの可用性とそのアクセスを迅速に復旧する能力、(d)処理の安全を確保するための技術的および組織的対策の効果を定期的に審査し評価するプロセスを含みます。

管理者または処理者によって実施された「適切な技術的および組織的対策」は、監督機関が制裁金を課すか否かの決定および個別案件における制裁金額の決定において考慮すべき事項の１つ、すなわち、管理者または処理者の責任の程度を決する上で考慮すべき事項として規定されています。「適切な技術的および組織的対策」の策定の前提として必要となるセキュリティレベルの適切さの評価に当たっては、特に偶発的または違法な破壊、滅失、変更、ならびに伝達、保管、およびその他の方法での処理がなされた個人データの無許可の開示またはアクセスの観点から、処理に伴うリスクを考慮しなければならない、とされています。事前にセキュリティレベルの評価を行った上で、技術的および組織的対策を立案することが重要であるといえます。

- **Q24:「名刺」記載の個人データ**

当社（日本国内法人）は毎年、EEA 域内で開催される世界的な見本市に出展し、海外市場開拓に力を入れています。出展時に来場者から膨大な名刺を入手しますが、顧客候補企業の担当者には、日本本社から「営業のための新商品紹介」の電子メールなどの連絡を行っています。名刺交換時に「（個人データの EEA 域外への移転について）同意を取得するプロセス」を入れるのも非常識な印象です。そもそも、名刺交換（メールアドレスを明記）という行為自体で、電子メールでの情報のやり取りに同意したという解釈が成立するのではないでしょうか？今後もメールでの営業を行うためには GDPR の観点でどのような点に注意が必要でしょう？

【個人データ取得の経緯：名刺交換】

名刺交換という行為自体から、「営業の新商品紹介」の電子メールで情報の連絡を行うという処理行為に同意したという解釈は成立する余地がありますが、同意の範囲については拡張的に解釈しないように留意が必要です。また、個人データの EEA 域外への移転についての同意は「十分性の決定および適切な保護措置がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意」することが要件となりますので、名刺交換という行為自体から明示的な同意を導くことはできません。

例えば、見本市来訪に対する御礼や、当該見本市に出展していたものと関連する新商品を紹介する連絡については、名刺交換を行ったデータ主体としても、そうした連絡が行われることを予見可能であるといえますので、その範囲の個人データ処理を行うことについて、データ主体による同意があったと考えることは GDPR の観点からは問題ないものと考えます。なお、企業によっては、上記の予見可能性を確実なものとするために、自社の名刺中に「名刺交換をさせて頂いた方には、当社より当社の商品やサービスに関する御案内を差し上げることがございます」といった記載を行うといった工夫をしている事例もあります。

これに対して、EEA 域内で開催された見本市で取得した名刺中の個人データを EEA 域外へ移転させることは、名刺交換行為自体から明示的な同意を導くことができません。従って、貴社（データ輸出者：データ管理者）と日本本社（データ輸入者：データ管理者）との間で標準契約条項

（Standard Contractual Clause: SCC）（EC Decision 2004/915/EC）を締結することにより、これらの個人データを移転させることが望ましいと考えます。また、当該データ移転は、拘束的企業準則（Binding Corporate Rules: BCR）の承認を取得することにより行うことも可能です。

- **SCC の基礎知識**

SCC とは、欧州委員会によって決定された契約書の雛形であり、当事者間でこの雛形を使ってデータ移転契約を締結することで適切な保護措置を提供し、適法なデータ移転を行うものです。現時点で利用可能な SCC は「管理者-管理者 SCC」が 2 種、「管理者-処理者 SCC」が 1 種の計 3 種あります。

SCC は、単に署名をしさえすれば、後は保管しておけば良いという性質のものではなく、SCC 中のデータ輸出者とデータ輸入者の義務を各々履行できる体制を整えることが肝要です。当該義務の違反は制裁金の対象となります。

表 14：SCC の種別

輸出者	輸入者	状況	現在の SCC のセット
管理者	管理者	個人データが EEA 域内の管理者から EEA 域外の管理者へ移転される場合	2 セットの SCC がある ▪ **2001 年 SCC**(EC Decision 2001/497/EC) ▪ **2004 年 SCC**(EC Decision 2004/915/EC)
管理者	処理者	個人データが EEA 域内の管理者から EEA 域外の処理者へ移転される場合	▪ **2010 年 SCC**(EC Decision 2010/87/EC)
処理者	復処理者[9]	個人データが、先ず EEA 域内で管理者から処理者へ移転され、その後、その処理者から EEA 域外にいる復処理者へ移転される場合	第 29 条作業部会は 2014 年 3 月、**「処理者-復処理者 SCC」案**を提案した(WP214)。しかし、欧州委員会はこれをまだ承認していない。

複数当事者間のデータ移転の方法にはさまざまなアプローチが考えられますが、以下の方法が一般的です。

方法 1:データ移転ごとに SCC を締結する

方法 2:基本契約書においてすべての輸出者、輸入者が単一の SCC に署名する

方法 3:すべての輸出者、輸入者各々の代理で包括証書に署名

日本企業の EEA 域内の統括拠点の法務部門では、方法 1 で対応していた企業がある程度の数あったようです。最近では、方法 2 または方法 3 を使って包括的な対応を行う体制に移行しようとしている企業が増えている印象があります。

[9] 処理者から委任を受けて処理者の指示の範囲内で処理者を代理して個人データを処理する者

- **加盟国ごとに異なる SCC によるデータ移転の条件等**

現行の指令の下では SCC の使用は EEA 加盟各国にて条件が異なるため、異なる条件への対応が必要です。

特に、SCC の監督機関への事前通知や監督機関からの事前承認取得を行うに当たり、企業として個人データ処理の登録を特定の法域で行っていない場合、当該法域の監督機関への当該登録作業やデータ処理の適法性の確認が必要となる場合があります。

相当数の加盟国においては監督機関に SCC を事前通知しなくてはなりません。他の相当数の加盟国においては SCC を使用したデータ移転について事前承認取得が必要とされている事前承認の取得には時間とコストが掛かります。

GDPR の下では、SCC によるデータ移転について事前承認は不要になると規定されています。しかし、データ保護影響評価が必要となる処理業務のリスト中に、EEA 域外への SCC によるデータ移転が列挙された場合、データ保護影響評価を実施した結果、監督機関への事前相談が必要となる可能性が残っていると考えられます。データ保護影響評価に関する第 29 条作業部会のガイドラインが 2017 年初めには出るといわれており、そこでどのような内容が規定されるかを確認することが望ましいと考えられます。

また、現行の指令の下における加盟各国の監督機関への個人データ処理の登録義務は、GDPR の下では、管理者および処理者の個人データの処理行為の記録の保持義務に置き換えられることになると説明されることがありますが、これについても第 29 条作業部会のガイドライン等の監督機関による公的な文書で明言されるまでは、当該説明が確実に正しいと言い切ることは難しいものと考えられます。

従って、GDPR の適用開始を待てば SCC によるデータ移転をより簡潔に行うことができるかは、第 29 条作業部会や欧州委員会によるガイドラインの策定・公表がない現段階では、不透明さが残っており、GDPR の適用開始に先立って指令の下での SCC によるデータ移転の対応を行うことが、より慎重な対応であると考えられます[10]。

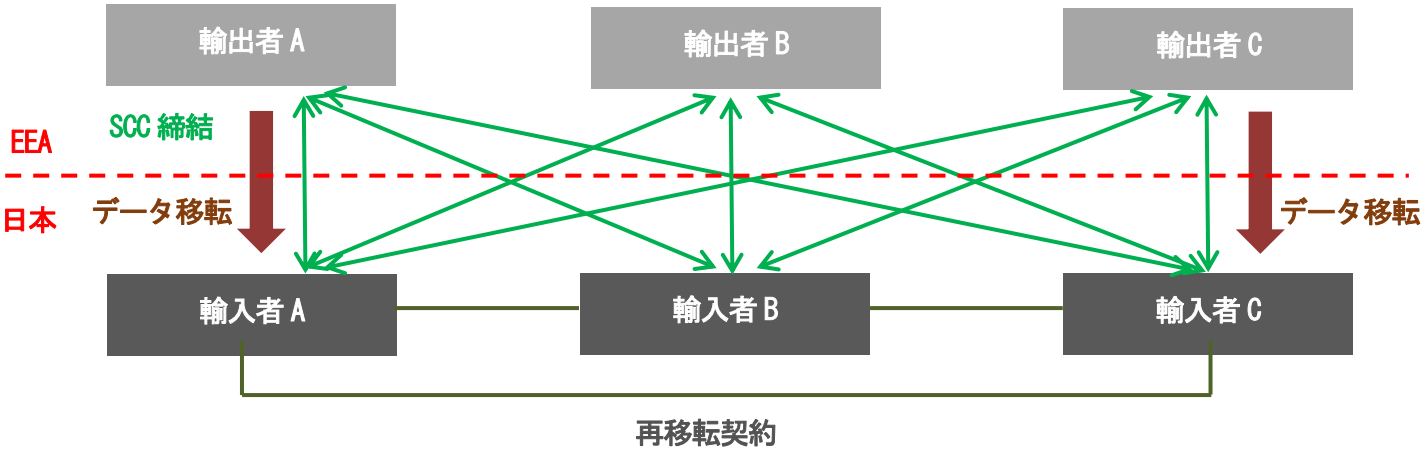
また、加盟国法において他の法的要件があるか否か、例えば、雇用関係のデータに関する義務(ワークスカウンシルとの強制的協議など)については事前に確認することが望ましいといえます。

[10] ここに記載した理由により、本レポートでは、現行の指令の下での SCC 対応について解説を行っています。また、GDPR の下では、現行の指令の下での SCC は欧州委員会決定によって修正、差し替えまたは廃止されるまで有効とされています（GDPR 第 46 条(5)）。

SCC による複数当事者間のデータ移転方法 1：データ移転ごとに SCC を締結する

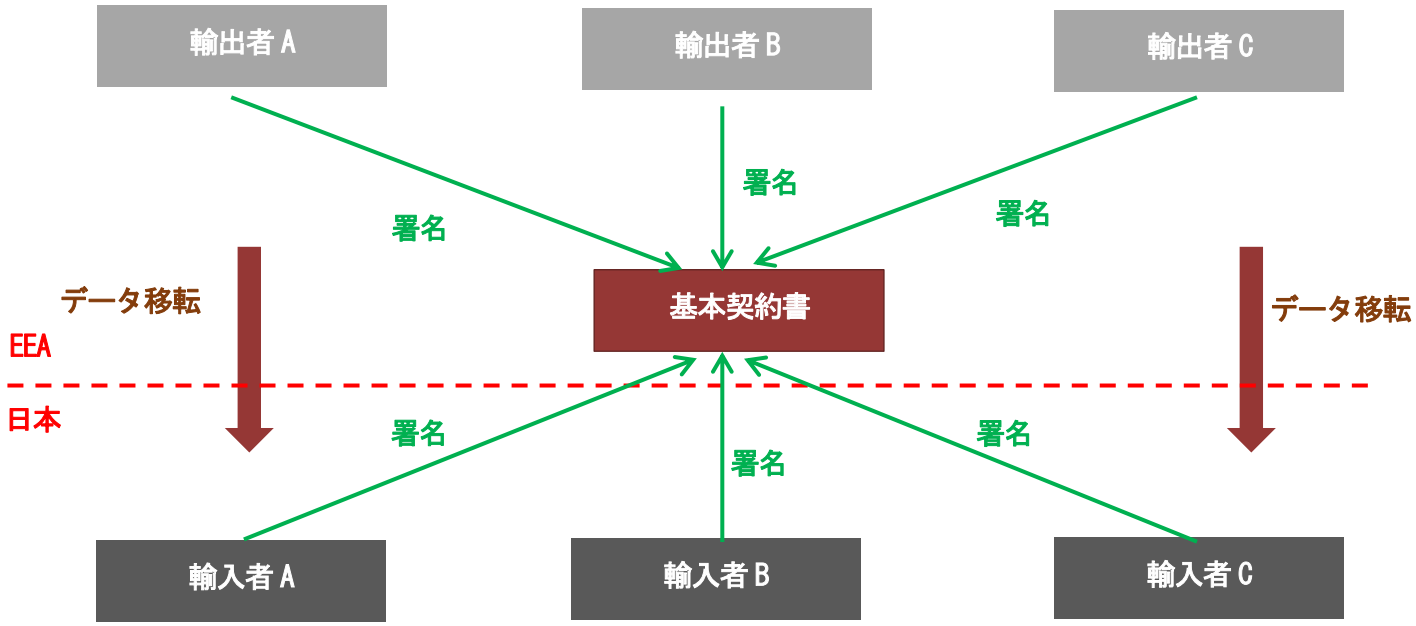
方法 1 は契約当事者に変更がある場合に柔軟性がなく数多くの SCC を締結しなければならないことから方法 2 または方法 3 を使う企業の数が増えている印象があります。

図 5：データ移転ごとの SCC の締結



SCC による複数当事者間のデータ移転方法 2：基本契約書においてすべての輸出者、輸入者が単一の SCC に署名する

図 6：基本契約書においてすべての輸出者、輸入者が単一の SCC に署名

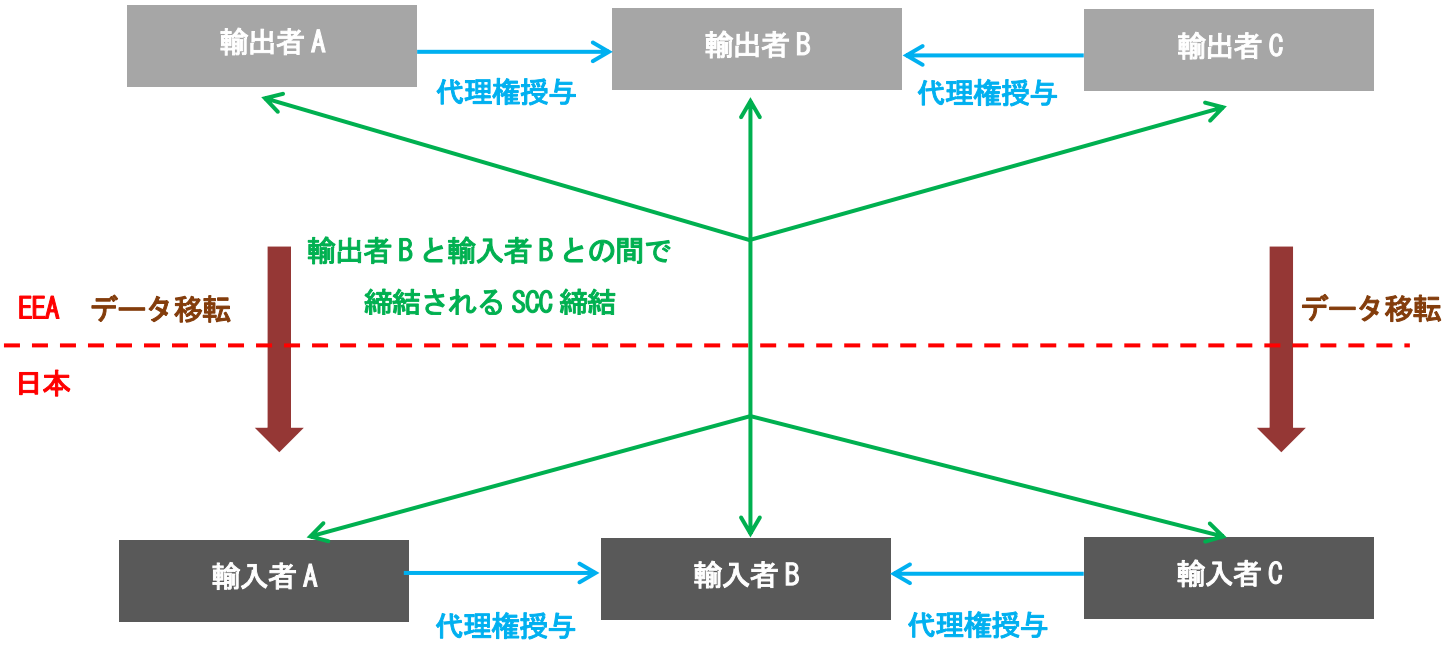


EEA からデータを送る者を輸出者、EEA からデータを受け取る者を輸入者とするのが簡便

SCC による複数当事者間のデータ移転方法 3：すべての輸出者、輸入者各々の代理で包括証書に署名

輸出者が企業グループ外である場合には、契約締結の代理権を授与することに抵抗のある企業もあるようです。

図 7：すべての輸出者、輸入者各々の代理で包括証明書に署名



- **BCR は企業グループ内でのデータ移転のみ適法化するが、最も安全な手段**

BCR(Binding Corporate Rules。拘束的企業準則)は監督機関による承認が必要なため、承認取得までに比較的長い期間と多額の費用が掛かるものの、最も安全な手段です。また、直近では、承認取得に掛かる期間は短縮されてきています。

BCR は、事業体グループまたは共同経済活動に従事する事業体グループ内で、一カ国または複数の第三国における管理者または処理者に対して個人データの移転または一連の個人データの移転のため加盟国の領域上にある管理者、または処理者によって遵守される個人データ保護方針を指します。監督機関によって承認された BCR に企業が従っている限りにおいて、全世界において企業グループ内での適法で自由なデータ移転が可能となります[11]。EEA 域内の企業グループ内の拠点から EEA 域外の企業グループ外へのデータ移転は SCC を締結するのが一般的です。

監督機関による BCR の審査開始から終了までには平均で約 18 カ月掛かると言われていますが、これは BCR 本文のドラフトの準備に時間が掛かっていた訳ではありません。監督機関の要請に応じて、企業グループ内部でのデータ移転に関する数多くの文書の作成と英訳を行うことに時間を要します。BCR 本文自体以外の、会社提出資料は、一から作成する必要があるものが通常あり、量も多く、企業ごとに異なるため、その準備には長い時間が掛かるのが通常です。

2016 年 11 月 14 日現在、ドイツのデュッセルドルフを管轄するノルトライン＝ヴェストファーレン州の監督機関の BCR 審査の担当者は、BCR の合理的なファースト・ドラフト提出から 1 年以内での BCR 審査終了に自信を見せています。同州の BCR 審査の担当者は、英語が堪能であるため、英語によるコミュニケーションが可能です。他にも、英国の DPA（Data Protection Authority）である Information Commissioner's Office の BCR 審査の責任者やオランダの DPA の審査の担当者も同様に、BCR の合理的なファースト・ドラフトの提出から 1 年以内での審査終了ができると明言しています。ただし、これは監督機関からのコメントや追加の文書提出の要求があったことにタイムリーに対応ができるなど、さまざまな条件を前提にしたスケジュールであることに留意することが必要と考えられます。

監督機関による BCR 審査を通じて、監督機関からの質問またはコメントの形で、自社のコンプライアンス上の問題について指摘を受けることで、監督機関による執行を受けずに、事前に問題を解決する機会があります。これにより GDPR の執行リスクを減らすことにつながるものと考えられます。

[11] 厳密には、現行指令の下では、EEA 内の 21 の国（オーストリア、ベルギー、ブルガリア、キプロス、チェコ共和国、エストニア、フランス、ドイツ、アイスランド、アイルランド、イタリア、ラトビア、リヒテンシュタイン、ルクセンブルグ、マルタ、オランダ、ノルウェー、スロバキア、スロベニア、スペインおよび英国）が BCR の相互認証手続（Mutual Recognition Procedure）に加盟しており、これらの国の監督機関のいずれかを主要監督機関として承認を受けた BCR の取得企業グループ内では、上記 21 の国々から EEA 域外への個人データ移転を BCR によって適法に行うことができることになります。BCR の取得企業が、上記 21 の国々以外の EEA 加盟国から EEA 域外への個人データ移転を当該 BCR によって行う場合、当該 EEA 加盟国の監督機関から個別に当該 BCR の審査を受け承認を受ける必要があります。GDPR 適用開始後は、相互認証手続への加盟の有無にかかわらず EEA 域内のどの国からの個人データ移転も BCR 取得企業グループ内では BCR に基づいて適法に行うことができることになります。

2016年11月14日時点で、筆者が知る限りで、2社の日本企業が監督機関へのBCR申請を終えており、うち1社がプレスリリースを行っています[12]。これ以外にも2016年中にBCR申請を行うことを検討している日本企業が何社かあるようです。今後は日本企業の中でもBCRによりデータ移転を行う企業の数は増えるものと考えられます。

- **Q25:「メールマガジン」配信登録のあった個人データ**

当社（日本国内法人）は、インターネット上で登録のあったメールアドレスに不定期ながら、メールマガジンを配信しています。この登録者にはEEA域内の個人も若干含まれています。GDPRの観点での問題を避けるためには、どのような対応が必要でしょうか？

【個人データ取得の経緯：メールマガジン配信登録】

企業は、データ主体の同意を既に得ているのか、またはこれから得るのかを確実にする必要があります。どちらの場合においても、データ主体は、同意を撤回し、メールマガジンを受け取らないようにするなどの権利について通知される必要があります。

- **Q26:「アンケート調査の回答」記載の個人データ**

当団体（日本国内法人）は公的機関で、例年、世界の在外日系企業に対してビジネス関係のインターネット・アンケート調査を実施しています。アンケート結果は個々の回答を集計して公表します。ただし、アンケート回答企業の属性を把握するため、企業名や業種、所在地などと共に回答者個人の氏名・メールアドレス・電話番号などの個人データも登録してもらっています。どのような文言をアンケート画面に挿入すれば、個人データのEEA域外移転について、当該個人からの同意を取得したことになるのでしょうか？

【個人データ取得の経緯：アンケート調査への回答登録】

個人データのEEA域外への移転についての同意は「十分性の決定および適切な保護措置がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意」することが要件となりますので、「明示的な同意」があったことを確実にできるような文言を考案する必要があります。ご質問頂いたケースでは、例えば、以下のような文言をアンケート画面に挿入すれば、個人データのEEA域外移転について当該個人からの同意を取得したと主張できるものと考えますが、同意取得のためのフォームについては、ケースバイケースで、どのような文言が適切かを検討することが明示的な同意の要件を満たす上で重要ですので、次の同意の文言をそのまま使用しないように、十分に注意が必要です。

[12] http://www.iij.ad.jp/news/pressrelease/2016/1026.html

EEA 加盟国内、すなわち、EU 加盟国、アイスランド、リヒテンシュタイン、ノルウェーのいずれかに在住の方は、以下をご確認下さい。

- 本調査で取得される個人データは世界の在外日系企業に対してビジネス関係のインターネット・アンケート調査に係わる用途のみに使用します。
- 個人データは日本に転送され、当団体の日本国内のサーバに保存されます。日本は、欧州委員会からデータ保護の十分性の決定を受けていませんが、当団体は回答者の個人データを適切に管理します。
- 回答者は、自らの個人データへのアクセス、不正確な個人データの修正、個人データの正確性の検証中のデータ加工の制限を当団体に要求できます。本調査の担当部署の連絡先は〇〇〇〇です。なお、当団体の個人データの取り扱いに不満がある場合には、EEA 加盟国の監督機関に苦情申し立てをすることができます。

個人データの使用および移転に関する上記に同意される場合は、以下の□にチェックしていただけますようお願いいたします。なお、回答者はこの同意をいつでも撤回する権利があり、この同意の撤回は、撤回前のデータ処理やデータ移転の適法性に影響を与えるものではありません。

□上記に同意する。

- Q27:「契約書」記載の個人データ

当社（日本国内法人）商品の取り扱いを望む EEA 域内の販売代理店と契約に基づき長らく取引を続けています。契約書には相手方の代表者の住所・氏名・銀行口座番号などの個人データも含まれています。契約に記載された情報も GDPR の観点での個人データに該当するのでしょうか？
【個人データ取得の経緯：契約書】

御理解のとおりです。相手方の代表者の住所、氏名または銀行口座は個人の識別につながり得る情報であるため「個人データ」に該当すると考えられます。契約に記載された「個人データ」との関係で問題となるのは EEA 域内の販売代理店が当該「個人データ」を取得しこれを EEA 域外である日本へ契約書を送付することにより「移転」することになるためです。

EEA 域内の販売代理店の代表者は、契約書を日本へ送付することにより自らの「個人データ」が日本へ「移転」することを認識することになり、当該代表者による明示的な同意があるといえます。この明示的な同意に基づき適法なデータ移転を行うことになるものと考えます。

同意以外の特例（必要性による特例）の例として「データ主体と管理者の間の契約の履行のため、またはデータ主体の要請により講じる契約前の措置の実施のため」という要件がありますが、これはデータ主体の代表者（データ主体）との間では貴社が契約関係に立つ訳ではありませんので、使用することができません。また、「管理者とその他の個人との間でデータ主体の利益のために交わされる契約の締結または履行のため」という同意以外の特例（必要性による特例）が移転のため

に認められていますが、これもデータ主体の代表者（データ主体）は契約当事者ではないため、使用することができません。

- **Q28:日本にあるサーバへの個人データ移転**

当社（日系企業の EEA 域内子会社）は専門コンサルタントの現地法人で、EEA 域内の顧客向けにビジネス・セミナーを開催しています。セミナー受講希望者には、インターネット上の登録画面で、氏名・所属・役職・メールアドレス・事前質問などの個人データを記入してもらい、受講票を電子メールで送付するなどの手続きを行っています。ただし、この手続きは日本にあるサーバを経由して行われています。このような場合でも、GDPR の観点での問題になり得るのでしょうか？問題にならないためには、どのような対策が必要でしょうか？
【個人データ取得の経緯：セミナー申込登録】

GDPR の観点で問題になり得ます。氏名・所属・役職・メールアドレスなど、個人の識別につながり得る情報である「個人データ」を貴社が取得し、これが日本にあるサーバを経由して行われることで貴社が EEA 域外である日本へ「個人データ」を「移転」させていることになります。

問題とならないための対策としては、貴社が上記「個人データ」を取得する時点、つまり、セミナー受講希望者にインターネット上の登録画面で「個人データ」を入力しセミナーの受講申込を完了させる時点で、セミナー受講希望者から「個人データ」の処理と EEA 域外である日本への移転について明示的な同意を取得しておくことが考えられます。具体的には、移転のための明示的な同意を取得するためのフォームを、セミナーの受講申込を行う前提として記入させることが考えられます。

- Q29:企業内の人事情報の取り扱い

当社（日系企業の EEA 域内子会社）は販売法人ですが、新たに現地採用の従業員を雇用することになりました。幹部候補レベルの人材なので、履歴書を日本本社に送付して、給与水準などの協議に入るつもりですが、GDPR の観点で問題あるでしょうか？
【個人データ取得の経緯：採用時の履歴書】

採用応募者や従業員の履歴書は個人の識別につながり得る情報が含まれており、「個人データ」に該当します。これを日本に送ることは「個人データ」の「移転」に該当するため、適切な保護措置を提供するか、法令上の特例として明示的な同意を取得する必要があります。

- Q30:企業内の従業員（個人）が作成した提案・企画書の取り扱い

当社（日系企業の EEA 域内子会社）は生産法人ですが、グループ全体で毎年、生産ラインの効率化などについて優秀な提案を行った現地従業員個人を表彰する制度があります。この関係で、生産ラインに従事する従業員全員の提案を氏名と共に管理し、日本本社とも共有しています。社内の管理目的のための活動で、一般公開される訳ではないので、GDPR の観点でも問題ないと考えていますが、いかがでしょうか？
【個人データ取得の経緯：業務上の改善提案書】

従業員の氏名や提案は個人の識別につながり得る情報であるため「個人データ」に該当します。これらの「個人データ」を日本本社と共有する際には、個人データの移転が行われるため、GDPR との関係が問題となります。これらの「個人データ」が一般公開されるか否かは GDPR の適用の有無に影響を与えません。

- Q31:企業内の個人業績評価の取り扱い

当社（日系企業の EEA 域内子会社）は販売法人ですが、グループ全体で毎年、駐在員を含めて従業員全員の個人業績を上司が評価して、賞与に連動させる制度があります。各従業員は、社内イントラネット上に自己評価を登録し、上司が 1 次評価の上、これらを総合的に日本本社の役員が最終評価しています。このような場合でも、GDPR の観点での「（個人データの EEA 域外への移転について）同意を取得するプロセス」が必要なのでしょうか？
【個人データ取得の経緯：個人業績評価登録】

必要です。しかし、同意ではなく、SCC または BCR に依拠することが望ましいと考えます。

社内イントラネット上に従業員の自己評価という個人の識別につながり得る情報が登録されることで、貴社は「個人データ」を取得します。貴社の日本本社の役員が最終評価を行うに当たっては、貴社の（EEA 域内の）社内イントラネット上の「個人データ」に日本からアクセスして閲覧する必要があります。この閲覧に当たり「個人データ」の EEA 域外である日本への「移転」が行われます。

従業員の個人データについては、使用者と従業員の関係において従業員が使用者のデータ移転に対して同意する場合、同意の任意性に疑義があると監督機関が考えることが多いと言われています。従って、監督機関が同意の任意性の疑義を根拠としてどの程度の執行を行うかは、今後の GDPR 執行を見守らなければわかりませんので、疑義のある従業員による同意に基づくのではなく、SCC によってデータ移転を適法に行うことが望ましいものと考えます。

もっとも、任意性を担保できればデータ主体による明示的な同意によるデータ移転も適法なものとして認められます。同意に基づいてデータ移転を行う場合には、任意性の確保に留意しながら進めることが望ましいといえるでしょう。

- **Q32:日本のサーバで一括管理するメールシステムの取り扱い**

当社（日系企業の EEA 域内子会社）は現地法人ですが、当社従業員が利用するメールシステムは、セキュリティ対策もあり、日本に設置されているデータサーバで一括管理しています。サーバには EEA 域内で勤務する現地従業員のメールアドレスと氏名・所属・役職・内線番号が一括で登録されています。これらは企業側が支給する社内的なものですが、それでも GDPR の適用対象となるのでしょうか？
【個人データ取得の経緯：新規採用・異動など】

従業員の氏名、所属、役職名および内線番号は、いずれも個人の識別につながるか、あるいは個人の識別につながり得るものであるため、「個人データ」に該当します。現地従業員のメールアドレスと所属・役職・内線番号が企業側の支給するものであるという事実は、GDPR の適用の有無を決める上では無関係です。

これらの個人データを日本に設置されているデータサーバで管理しているということは、これに先立って貴社から貴社の親会社である日系企業に対し個人データの「移転」がなされたものと考えられます。Q31 の回答のとおり、従業員の個人データについては、使用者と従業員の関係において従業員が使用者のデータ移転に対して同意する場合、同意の任意性に疑義があると監督機関が考えることが多いと言われています。従って、監督機関が同意の任意性の疑義を根拠としてどの程度の執行を行うかは、今後の GDPR 執行を見守らなければわかりませんので、疑義のある従業員による同意に基づくのではなく、SCC によってデータ移転を適法に行うことが望ましいのは前述のとおりです。

- **Q33:企業内で過去に取得した個人データの取り扱い**

当社（日系企業の EEA 域内子会社）は現地法人で、EEA 域内で 20 年以上、操業を続けています。GDPR の社内での対応は概ね完了していますが、現地従業員の給与や業績、採用時に提出された履歴書など個人データを、念のため、日本本社の人事部門で保管・管理しています。これら過去に取得した個人データについても、GDPR の適用対象になるのでしょうか？また、この場合の「（個人データの EEA 域外への移転について）同意を取得するプロセス」としてはどのような対応が想定されるのでしょうか？また、この機会に退職者・死亡者などについての対応も検討すべきでしょうか？

【個人データ取得の経緯：過去からの情報蓄積】

過去に取得したものであっても、個人の識別につながり得る情報であれば、「個人データ」に該当し、GDPR の適用対象になります。

現地従業員の給与や業績、採用時に提出された履歴書など個人データの中、既に退職してしまった元現地従業員などの個人データについては、当該元現地従業員すべてから同意を取得するのは現実的ではありません。また、在職中の現地従業員すべてから同意を取得することにも幾つかの問題があります。

第一に、使用者が従業員から取得する同意については監督機関が任意性に疑いを持つ恐れがあること、第二に、在職中の現地従業員すべてから同意を取得することを網羅的に行うことは簡単ではない場合が多いこと、第三に、現地従業員から同意を取得したとしても同意はいつでも撤回可能であることなどです。

そこで、日系企業の EEA 域内子会社（データ輸出者：データ管理者）が日本本社（データ輸入者：データ管理者）との間で、SCC を締結し、データ主体である元現地従業員からの同意を取得せずに、適法に個人データを移転させることが現実的な対応として想定されます。

退職者についてはそのとおりですが、死亡者についてはそのような対応は不要です。死亡者の識別につながるデータおよび死亡者の識別につながり得るデータは、いずれも GDPR 上の「個人データ」には該当しないと考えられています。ただし、これは加盟国が死亡者の個人データの処理に関する規制を導入する可能性を完全に否定しさるものではないと考えられますので、注意が必要です。

- **Q34:日本以外の第三国への個人データの移転**

当社（日系企業の EEA 域内子会社）は現地法人で、現地従業員の給与計算、社会保障経費算定などの業務をインドのシェアード・サービス・センターに集約・委託しています。こうしたオペレーションは賃金水準との関係で決まるため、今後、インド以外の第三国に個人データの移転を検討する可能性もあります。対象国を絞らずに GDPR への対応を進めることはできないでしょうか？

対象国を絞らずにGDPRへの対応を進めることは基本的には得策ではありません。

第一に、同意によって EEA 域外への個人データ移転を行う場合、「十分性の決定および適切な保護措置がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報が提供された後、データ主体がその提案された移転に明示的に同意」することが必要とされます。

先ず、当初、日系企業の EEA 域内子会社から、インドのシェアード・サービス・センターへの個人データの移転を、同意によって行う場合、この同意によって適法化されるのは、EEA域内からインドへのデータ移転であって、インドからインド以外の第三国への個人データの移転については適法化されません。

今後、インド以外の第三国に個人データの移転を行う場合には、その時点で当該第三国が「十分性の決定を受けているかどうか、および適切な保護措置がないことによってデータ主体に関する当該移転から生じ得るリスクについての情報を提供」するというプロセスが必要となります。

次に、日系企業の EEA 域内子会社（データ輸出者・管理者）からインドのシェアード・サービス・センター（データ輸入者・処理者）への個人データの移転を SCC（EC Decision 2010/87/EC）を 2 社間で締結することにより行うことが考えられます。当該センターからインド以外の第三国へ移転させる場合には、また別途の対応が必要となります。

- **Q35:企業としての包括的対応の是非**

当社（日系企業の在 EEA 域内駐在員事務所）は、自分と派遣社員数名の事務所です。社内の GDPR への対応は責任者である自分だけで対応しています。このため、取り扱う個人データは限られるのですが、組織的・網羅的な対応ができず、EEA 域外への個人データの移転についての同意を取得するプロセスを忘れるリスクを感じています。例えば、採用時の「労働契約」や「就業規則」などに包括的な同意を取得する条項を挿入することで、対応はできないのでしょうか？

この対応は同意の要件を満たさない可能性があるので、お薦めいたしません。労働契約や就業規則とは別の文書により、個人データの EEA 域外への移転についてデータ主体からの明示的な同意を取得することが望ましいと考えます。

また、使用者が従業員から取得する個人データ移転への同意については任意性に疑義が生じる可能性があります。

従って、貴社の在 EEA 域内駐在員事務所と貴社本社との間で SCC を締結することによって対応することがより望ましいと考えられます。なお、別々の法人格をもたない二当事者の間での SCC の締結を認める監督機関が多くなっていると考えられますが、個別に確認しておくことが肝要と考えられます。

JETRO

レポートをご覧いただいた後、アンケート（所要時間：約１分）にご協力ください。
https://www.jetro.go.jp/form5/pub/ora2/20160084

「EU 一般データ保護規則（GDPR）」
に関わる実務ハンドブック（入門編）

作成者　日本貿易振興機構（ジェトロ）海外調査部 欧州ロシア CIS 課
〒107-6006　東京都港区赤坂 1-12-32
Tel.03-3582-5569

2016.11