弁護士法人 中央総合法律事務所
CHUO SOGO LAW OFFICE, P. C.

GDPR について

令和 5 年 10 月 24 日
弁護士　新澤　純
niizawa_j@clo.gr.jp

第１　はじめに

EU データ保護一般規則（General Data Protection Regulation (EU) 2016/679。以下、「GDPR」といいます。）が 2018 年 5 月 25 日に施行されてから 5 年が経過しました。最近では、2022 年 11 月、NTT データのスペイン子会社であった Everis（エヴェリス）が、過失により個人データを漏えいさせたとして、スペインの監督当局から 6 万 4000 ユーロ（約 1000 万円相当。1 ユーロ 158 円換算。）の制裁金を科されたとの報道があり、日系企業に関連するはじめての GDPR 事案として注目を集めました。

もっとも、日本の改正個人情報保護法、米国カリフォルニア州のプライバシー法（CCPA/CPRA）、中国の個人情報保護法など、現在データ保護法制は世界各国で立法の動きが見られ、日本企業としても、何から手を付けてよいか分からない、あるいは制裁金リスクがそれほど高くないので、既存のウェブサービス利用規約やプライバシーポリシーのままで問題ないだろうと考えておられる方も多いかと思います。

そこで、本稿では、EU における統一的なデータ保護法令である GDPR に焦点を当てて、具体的に、日本企業が講じるべき措置について説明させて頂きます。①日本企業が GDPR の適用範囲に含まれるか否か、②プライバシーポリシーをどのように策定・修正すれば、GDPR を遵守したことになるのか、③代理人・DPO 選任の要否、④越境移転規制の枠組み、⑤世界各国の他のデータ保護法制との関係性（GDPR 対応を行えば、それで十分か）の順に説明させて頂きます。

第２　GDPR の概要

１　GDPR の役割

GDPR は、2018 年 5 月 25 日に施行され、各 EU 加盟国の個別の立法行為を要することなく、また、各 EU 加盟国の国内法に優先して、EU 全域に直接的な法的拘束力を生じさせる、EU における統一的なデータ保護法令です。

本稿において、「EU」という用語には、便宜上、EU 加盟国（27 カ国）に加え、欧州経済領域（EEA）の一部であるアイスランド、ノルウェー、リヒテンシュタインを含むものとします。また、英国については、EU を離脱したものの、GDPR と同等のデータ保護法令（英国 GDPR）を定めており、GDPR と英国 GDPR を総称して、「GDPR」と呼ぶこととします。EU 域内、英国域内を総称して、「EU 域内」と呼ぶこととします。

２　GDPR の適用範囲

（１）個人データの定義

GDPR で保護される「個人データ（personal data）」とは、識別され、又は識別され得る自然人（GDPR では、この自然人のことを、「データ主体（data subject）」と呼んでいます。）に関する一切の情報をいいます。

識別され得る自然人とは、氏名、識別番号、位置データ、オンライン識別子（IP アドレスや Cookie[1]等）のような識別子を参照することによって、又は、当該自然人固有の要素（身体的、生理的、遺伝的、精神的、経済的、文化的又は社会的な同一性を示す要素）を参照することによって、直接又は間接に、識別され得る者をいいます（GDPR 第 4 条第 1 項）。

（２）地理的適用範囲

GDPR の地理的適用範囲は、以下のとおりです（GDPR 第 3 条）。

域内適用： 管理者又は処理者が EU 域内に拠点を有し、EU 域内の拠点の活動の過程において（EU 域内外で）個人データの処理を行う場合 域外適用： 管理者又は処理者が EU 域内に拠点を有しない場合でも、データ処理が、 (i)　EU 域内のデータ主体に対する物品又はサービスの提供に関連して行われる場合（ターゲティング基準） (ii)　EU 域内のデータ主体の行動をモニタリングする目的で行われる場合（モニタリング基準）

「管理者（controller）」とは、個人データの処理の目的及び手段を決定する者をいい（分かりやすく言えば、個人情報取扱事業者）、「処理者（processor）」とは、管理者の代わりに個人データを処理する者をいいます（分かりやすく言えば、委託先）。法人格や営利性の有無は問われません（GDPR 第 4 条第 7 項、第 8 項）。

ターゲティング基準については、EU 域内に所在する自然人を意図的にターゲットとした物品又はサービスの提供のみが対象となります。「物品又はサービスの提供」に該当するか否かのポイントは、管理者・処理者へのアクセスの可能性、使用言語、決済通貨、ウェブサイト等での記載内容などの要素により判断されるとされています（GDPR 前文第 23 項）。

モニタリング基準については、「モニタリング」とは、EU 域内のデータ主体の物理

[1] 日本の改正個人情報保護法（2022 年 4 月 1 日施行）では、Cookie は「個人関連情報」に位置付けられることになりましたが、Cookie 単体では個人情報に含まれないとされている点に注意が必要です。Cookie の法的取扱いにつき、弊所橿渕弁護士による法律コラムをご覧ください。https://www.clo.jp/column/3541/

的な行動に限らず、オンライン上での行動を元に嗜好や傾向を分析し、EU 域内のデータ主体をオンライン上で追跡することをいいます（GDPR 前文第 24 項）。例えば、行動ターゲティング広告、マーケティング目的での位置情報の提供、Cookie を用いたオンライントラッキング、パーソナライズ化された食事、オンライン健康診断サービスなどのトラッキング技術は、「モニタリング」を構成するものと考えられます[2]。

日本企業も、英語、ドイツ語などの言語に対応し、ポンドやユーロで決済可能なウェブサイトを作り、EU 域内の自然人を意図的にターゲットとして、EC やオンラインサービスを提供する場合（EU 域内のデータ主体に対する物品又はサービスの提供）、その他、モニタリングに該当する場合には、GDPR の域外適用を受けると整理して、GDPR 遵守のための措置を講じておくことが望ましいものと考えられます。

3　GDPR の適用を受ける場合に日本企業が講じるべき措置

（1）プライバシーポリシーの策定

GDPR において、管理者がデータ主体から個人データを取得する際に、データ主体に通知しなければならないとされている項目は、以下の一覧表[3]のとおりです。管理者がデータ主体から直接取得する場合が GDPR 第 13 条で、第三者から間接的に取得する場合が GDPR 第 14 条で、情報提供義務の内容が若干異なります。これら通知を個別にデータ主体に行うのは煩雑であるため、実務上、プライバシーポリシーに盛り込んで、ウェブサイト上で公開することが一般的です。

	提供すべき情報の項目	管理者の情報提供義務の概要	GDPR第13条の根拠	GDPR第14条の根拠	日本型プライバシーポリシーにおける記載の有無	対応難易度
1	管理者及び代理人の身元・連絡先	管理者及び代理人の身元及び連絡先の情報（所属・住所・電子メールアドレス・電話番号）をデータ主体に提供する。	1項(a)	1項(a)	◎	low
2	DPOの連絡先	DPO（データ保護責任者）について連絡先の情報をデータ主体に提供する。	1項(b)	1項(b)	×	high
3	データ処理の目的・法的根拠	個人データの処理の目的及び法的根拠（例：同意、契約の履行、法的義務の遵守、正当な利益etc）を特定し、その情報をデータ主体に提供する。	1項(c)	1項(c)	△	middle
4	データ処理の「正当な利益」	前項で「正当な利益」が処理の法的根拠となっている場合、管理者又は第三者が追求する正当な利益についての情報をデータ主体に提供する。	1項(d)	2項(b)	×	middle
5	データの類型	関係する個人データの類型情報をデータ主体に提供する。	—	1項(d)	×	middle
6	データの受領者	個人データの受領者が存在する場合、受領者の情報（会社名）又は受領者の類型（種別・セクター・所在地等）をデータ主体に提供する。	1項(e)	1項(e)	△ 共同利用で会社名を記載している事例有	middle
7	越境移転	越境移転を行う場合、当該事実、当該国の十分性認定の有無、保護措置、個人データの複製物を取得するための方法、どこで個人データが利用可能とされているかについての情報をデータ主体に提供する。	1項(f)	1項(f)	△	middle
8	保有期間	保有期間又は保有期間を決定するための基準に関する情報をデータ主体に提供する。	2項(a)	2項(a)	△	middle
9	データ主体の権利	データ主体の権利の内容（開示請求権、訂正権、削除権、データ処理を制限する権利、データポータビリティ権、データ処理に異議を唱える権利）の情報をデータ主体に提供する。	2項(b)	2項(c)	△ データポータビリティ権に対応している事業者がほぼ無	high
10	同意の撤回権	本人の同意に基づき個人データを取扱う場合、いつでも同意を撤回する権利があること、及びその方法についての情報をデータ主体に提供する。	2項(c)	2項(d)	×	high
11	監督機関にする異議申立権	監督機関に異議を申し立てる権利があることをデータ主体に提供する。	2項(d)	2項(e)	×	low
12	データ提供が法令・契約上の要件であるか等	・個人データの提供が法令・契約上の要件であるか、又は契約を締結する際に必要な要件であるかの情報、並びに、 ・個人データの提供義務をデータ主体が負うか、及び個人データの提供をしない場合に生じうる結果についての情報 をデータ主体に提供する。	2項(e)	—	×	low
13	データの取得元	個人データを取得した情報源、及び一般人がアクセスできるデータから収集したか否かに関する情報をデータ主体に提供する。	—	2項(f)	△	middle
14	自動化された意思決定の存在等	自動化された意思決定（AIによるデータ処理等）を事業者が行う場合、自動処理を行うこと、自動処理のロジック、自動処理のデータ主体にとっての重要性、及び生じうる結果に関する情報をデータ主体に提供する。	2項(f)	2項(g)	×	low

[2] 森大樹他著「GDPR の最新実務動向 [第 1 回] GDPR の執行状況および非欧州企業への GDPR の域外適用の概観」NBL1240 号（2023.4.15）37 頁

[3] 出典：「日本型プライバシーポリシーを GDPR 対応させるために足りない要素一覧表」クラウドサイン社 HP（ https://www.cloudsign.jp/media/20181025-privacypolicy-euvsjapan/ ）より引用。

（２）既存のプライバシーポリシーとの関係性

様式の問題ですが、日本の個人情報保護法に対応した既存のプライバシーポリシーに加えて、GDPR 対応、米国対応、中国対応など、世界各国対応のプライバシーポリシーをどのように策定するかという問題があります。この点、1 つのプライバシーポリシーに集約するグローバル型と、事業を展開する国や地域ごとに個別の規定を特則的に設ける個別型のパターンがあります。

その上で、GDPR 対応のプライバシーポリシーとして、一覧表の 14 項目を英語等で記載していくことになります。一覧表の日本型プライバシーポリシーにおける記載の有無の欄で、殆どが×または△となっていることからも分かる通り、GDPR は日本の個人情報保護法よりも厳格な規制であるため、既存のプライバシーポリシーでカバーできる部分は殆どありません。

したがって、会社の事業活動の性質や、データ主体から取得するデータの類型を洗い出した上で、一つ一つ分析・検討していく必要があります。

４　データ処理の法的根拠

GDPR では、個人データの処理は、以下の少なくとも 1 つの法的根拠が適用される場合においてのみ、適法であるとされています（GDPR 第 6 条）。

これは、GDPR における法定の通知事項ですが、筆者が、日本企業や外国企業の GDPR 対応の英文プライバシーポリシーを 100 社ほど確認したところ、法的根拠について、会社の事業活動の性質・内容や、取得するデータの類型に即して、会社独自の文言で記載しているところもあれば、管理者の正当な利益として、「ensure business continuity（事業の継続性を確保する）」とするなど、どこの会社にも当てはまるような定型的な文言しか記載していないようなところまで、様々でした。

IT、フィンテック、金融、メーカー、小売販売、運輸、観光など事業活動の性質・内容に応じて、データ処理の法的根拠は異なると考えられますので、できる限り事業内容に沿った法的根拠を記載しておくことが望ましいと考えられます。

（１）データ主体による同意

GDPR における有効な同意とは、「自由に与えられ、特定され、事前に説明を受けた上での、不明瞭ではない、データ主体の意思表示を意味し、それによって、データ主体が、その陳述又は明確な積極的行為により、自身に関連する個人データの処理の同意を表明するものを意味する」と定義されています（GDPR 第 4 条第 11 号、第 7 条）。日本法とは同意が必要とされる場面や同意の要件が異なり、要件自体も GDPR の方が厳格であるため、日本法の感覚で、「同意を取得しておけば安全」と安易に考

えるべきではありません[4]。

（２）データ主体との契約の履行

データ主体が当事者となっている契約の履行のために当該処理が必要な場合、又は契約締結前のデータ主体の要求に応じて手続をとるために当該処理が必要な場合。

ex. 個人がオンラインショップで商品を購入して、商品の配達のために個人データを処理する場合。

（３）法的義務の遵守

管理者の法的義務を遵守するために処理が必要な場合。ここでいう法的義務とは、EU 法又は EU 加盟国法上の法的義務のことをいい、日本法やそれ以外の法令は含まれません。

（４）データ主体又は他の自然人の重大な利益の保護

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必要な場合。

ex. 自然災害又は人的災害等の人道上の緊急事態の場合、感染症の拡大の監視のために必要な場合（GDPR 前文第 46 項）。

（５）公共の利益又は公的権限の行使

公共の利益又は管理者の公的権限行使のために行われる業務遂行において処理が必要な場合。

ex. 公衆衛生や社会保障のような医療目的のために個人データを取得することが必要な場合（GDRP 前文第 45 項）

（６）管理者又は第三者の正当な利益

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。「正当な利益（legitimate interest）」は、幅広い企業の事業活動をカバーし得る有用な法的根拠であり、実務上も広く活用されています。もっとも、事業活動に関連していればどのような場合でも正当な利益によって処理が許容されるというわけではなく、データ主体の権利・自由と事業者の利益との比較衡量を行うことが必要であるとされています[5]。

５　データ主体の権利

GDPR では、データ主体は、以下の権利を有するものとされています。

（１）開示請求権（GDPR 第 15 条）

管理者が自己に関する個人データの処理を行っているかの確認、及び処理を行っている場合、当該個人データ及び一定の関連情報の開示を受ける権利

（２）訂正権（GDPR 第 16 条）

---

[4] 岡田淳他著『実務担当者のための欧州データコンプライアンス―GDPR から e プライバシー規則まで』（商事法務、2019 年 4 月 15 日）（以下、「岡田」といいます。）34 頁

[5] 岡田 35 頁

自己に関する不正確・不完全な個人データにつき、訂正を受ける権利

（３）削除権（GDPR 第 17 条）

自己に関する個人データの削除を受ける権利

（４）データ処理を制限する権利（GDPR 第 18 条）

自己に関する個人データの処理に制限を加える権利

（５）データポータビリティ権（GDPR 第 20 条）

自己に関する個人データを、一般的な機械で読み取り可能な形式で自ら受領し、または他の管理者に移転させる権利

（６）データ処理に異議を唱える権利（GDPR 第 21 条）

自己に関する個人データの処理に異議を唱える権利

（７）自動化された意思決定を受けない権利（GDPR 第 22 条）

自動化された意思決定（AI によるデータ処理等）の対象から除外される権利

６　代理人・DPO の選任の要否

（１）代理人

代理人とは、データ主体や監督当局が域外適用の対象となる事業者とコンタクトを取る必要がある場合に、窓口としての役割を果たす人物をいいます。

EU 域内に拠点を持たず、GDPR の域外適用を受ける管理者・処理者は、原則、代理人の選任が義務付けられます（GDPR 第 27 条）。

ただし、以下に該当する場合には、例外的に選任義務が免除されます。

① **データ処理が、(i) 一時的なものであり、かつ、(ii) 特別な種類の個人データ（GDPR 第 9 条第 1 項）、又は有罪判決及び犯罪行為と関連する個人データ（GDPR 第 10 条）の大規模なデータ処理を含まず、かつ、(iii) 処理の性質、過程、範囲及び目的を考慮に入れた上で、自然人の権利及び自由に対するリスクが生じる可能性が低い場合**。

② 公的機関又は団体の場合。

データ処理が一時的であり、かつ、自然人の権利及び自由に対するリスクが生じる可能性が低いことが明らかである場合は極めて例外的であると考えられますので、実務上は、代理人の選任を前提として、効率やコストの観点から、誰を代理人として選任するかを検討することが現実的であると考えられます。

代理人は、データ主体が所在する EU 域内に置く必要があります。実務上、代理人には、EU 域内の法律事務所やコンサルタント等が選任されることが多いです。代理人は、DPO とは異なり、資格要件は定められておらず、監督当局への届出も必要とはされていません。

代理人の選任を怠った場合、最大 1000 万ユーロ又は前年度の年間世界売上高の 2%のいずれか高額である方を上限とする制裁金が科されます（GDPR 第 83 条第 4 項）。

代理人選任義務違反の執行事例としては、2021 年 5 月、カナダ企業である LocateFamily.com が、オランダのデータ保護機関から、EU 域内の代理人を選任していなかったとして、52 万 5,000 ユーロ（約 8300 万円相当。1 ユーロ 158 円換算。）の制裁金を科されたというものがあります[6]。

（2）DPO

データ保護責任者（Data Protection Officer。以下、「DPO」といいます。）とは、管理者から独立した立場で、個人データの処理を監視し、GDPR の遵守を指導・監督する役割を果たす人物をいいます（GDPR 第 37 条～第 39 条）。

以下のいずれかに該当する場合には、管理者・処理者は、DPO を選任する義務を負います。

① データ処理が公的機関又は団体によって行われる場合

② **管理者又は処理者の中心的業務が、性質、範囲及び／又は目的に照らして、データ主体の定期的かつ体系的なモニタリングを要する大規模なデータ処理によって構成されている場合。**

③ 管理者又は処理者の中心的業務が、特別な種類の個人データ（GDPR 第 9 条第 1 項）、並びに有罪判決及び犯罪行為と関連する個人データ（GDPR 第 10 条）の大規模な処理によって構成されている場合。

④ EU 法又は加盟国法に基づき要求されている場合。

上記のうち、日本企業が最も問題となり得る類型は、②であると考えられます。EU データ保護指令の第 29 条作業部会が公表している DPO に関するガイドラインによれば、類型②の各要件について、次のような説明がなされています。

「中心的業務」：管理者又は処理者の目的を達成するための主要な業務。但し、これに該当しない業務でも、当該個人データの処理が管理者又は処理者の業務の切り離せない部分を形成している場合には、当該業務も含む。

ex. 民間警備会社による民間ショッピングセンターや公共の場の監視、病院による患者の健康データの管理（病院の中心的業務である医療の提供と切り離せない業務）

「大規模」：大規模に当たるか否かは、(i) データ主体の数、(ii) データの量・種類、(iii) 処理の期間・永続性、(iv) 処理の地理的範囲等の要素を考慮して判断する。

ex. 大規模に当たる例は、公共交通機関のシステムを利用した個人の乗降履歴の処理、保険会社又は銀行によって行われる通常業務における顧客情報の処理、検索エンジンによって行われる行動ターゲティング広告のための個人データの処理。

[6] 森大樹他著「GDPR の最新実務動向 [第 4 回] 日本企業における DPO・代理人の選任」NBL1249 号（2023.9.1）（以下、「森」といいます。）75 頁

「定期的かつ体系的なモニタリング[7]」：定期的とは、(i) 現在継続し又は一定期間内に一定の間隔で発生する、(ii) 定期的に繰り返される、又は (iii) 常時又は周期的に発生するものをいう。体系的とは、(i) システムに従って行われる、(ii) あらかじめ決められた、組織的に、又は方法論に基づき行われる、(iii) データ収集のための一般的な計画の一環として行われる、又は (iv) 戦略の一環として行われるものをいう。

ex. インターネット上でのトラッキング（モバイルアプリ等による位置情報の追跡を含む）、リスク評価目的（信用評価や保険料算定、マネーロンダリング検知等）のプロファイリング・スコアリング、行動ターゲティング広告、ウェアラブルデバイスによる健康情報等のモニタリング。

一般的に、企業が顧客向けに行うデータ処理は、中心的業務と切り離せないものとして「中心的業務」に当たるとされ（従業員向けの給与支払管理や、社内の IT サポート業務などは、補助的な業務に過ぎないと位置付けることはできると思います）、また、従業員個人がオフラインでデータ処理をするのではなく、企業が管理者としてオンラインで行う場合には、「大規模」に当たるとされる場合が多いと考えられます。

したがって、DPO の選任義務を負うか否かは、「定期的かつ体系的なモニタリング」に当たるか否かがポイントとなり、該当例を踏まえて、その可能性がある場合には、実務上は、DPO の選任・維持にかかるコストと、違反の場合に科される制裁金のリスクとを勘案した上で、当該企業としての対応を決定すべきであると考えられます。

DPO は、DPO ガイドラインで、監督当局及びデータ主体が容易にアクセスできる必要があるとされていますが、代理人とは異なり、EU 域内に置かなければならないという制限はなく、独立性があれば、日本国内の社内・社外に置くことも可能です。もっとも、それでもやはり、実務上は、DPO についても、代理人と同様、EU 域内の法律事務所やコンサルタント等が選任されることが多いと考えられます。

DPO は、代理人とは異なり、資格要件が定められており、専門家としての資質、特にデータ保護法及びプラクティスの専門知識、並びに GDPR 第 39 条の業務を遂行する能力に基づいて選任されなければなりません（GDPR 第 37 条第 5 項）。また、DPO に関しては、監督当局に、DPO の連絡先を届け出ることが必要とされています。

DPO の選任を怠った場合、最大 1000 万ユーロ又は前年度の年間世界売上高の 2% のいずれか高額である方を上限とする制裁金が科されます（GDPR 第 83 条第 4 項）。

DPO 選任義務違反の執行事例としては、2019 年 12 月、Facebook が、DPO を務める個人の変更を監督当局に適切に届け出なかったとして、ドイツ・ハンブルクの監督当局から、5 万 1,000 ユーロ（約 800 万円相当。1 ユーロ 158 円換算。）の制裁金を科

[7] 第 2、2、(2)GDPR の地理的適用範囲の箇所で述べた通り、「モニタリング」とは、EU 域内のデータ主体の物理的な行動に限らず、オンライン上での行動を元に嗜好や傾向を分析し、EU 域内のデータ主体をオンライン上で追跡することをいいます（GDPR 前文第 24 項）。

されたというものがあります。

また、2020 年 4 月、ある通信会社の DPO が、部門責任者であると同時に、監査・リスク・コンプライアンス部門の責任者でもあったところ、部門責任者として自分が出した決定を、データ保護遵守の観点から自ら監視するという関係にあり、独立性が損なわれる状況を作り出していたとして、ベルギーの監督当局から、5 万ユーロ（約 790 万円相当。1 ユーロ 158 円換算。）の制裁金を科されたという事例もあります[8]。

7　越境移転規制の枠組み

（1）越境移転規制

越境移転規制とは、個人データの EU 域内[9]から域外（第三国及び国際機関）への移転（transfer）、また、そこからの再移転（onward transfer）は、GDPR 第 45 条、第 46 条、第 49 条のいずれかの要件を満たさない限り、違法であるというルールをいいます（GDPR 第 44 条）。

日本企業が GDPR の域外適用を受ける場合、日本企業は、EU 域内のデータ主体に対する物品又はサービスの提供に関連して、EU 域内から域外への個人データの移転を受けることになるため、この越境移転規制に服することになります。

（2）十分性認定

もっとも、2019 年 1 月 23 日、欧州委員会は、日本に対して、GDPR 第 45 条に基づく十分性認定を行いました。十分性認定とは、欧州委員会が、移転先の個人データの保護のレベルを検証・評価した結果、特定の第三国・地域・国際機関等が、個人データについて十分な水準の保護を確保していると決定することをいいます[10]。

これにより、EU 域内から日本への個人データの越境移転については、適法であると整理されることになりました。

（3）補完的ルール

日本の個人情報保護法委員会は、GDPR と日本の個人情報保護法の相違点に照らし、EU 域内から十分性認定により越境移転を受けた個人データについて高い水準の保護を確保するために、補完的ルール[11]を策定し、十分性認定と同日に施行しました。

---

[8] 森 74 頁。筆者によれば、「なお、上記制裁金の金額は小さく思えるが、欧州の規制当局は、警告の趣旨で低額の制裁金を科した後、同様のデータ保護規則違反に対してはるかに高額な制裁金を科すことが一般的であることに留意する必要がある。」とのことです。

[9] 冒頭で述べた通り、「EU 域内」という用語が、厳密には、EU＋EEA の一部であるアイスランド、ノルウェー、リヒテンシュタイン＋英国という意味で、EU よりも広い領域を指すことにご注意ください。

[10] 個人情報保護委員会の HP によれば、2022 年 1 月末時点で、十分性認定を受けている国は、アルゼンチン、イスラエル、ウルグアイ、英国、カナダ、韓国、スイス、日本、ニュージーランド、その他小規模な地域を含む、14 の国・地域のみです。https://www.ppc.go.jp/enforcement/infoprovision/EU/

[11] 個人情報保護委員会「個人情報の保護に関する法律に係る EU 及び英国域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール」（2019 年 1 月、2023 年 3 月一部改正）。
https://www.ppc.go.jp/personalinfo/legal/

1点注目すべきは、補完的ルールに関するパブリックコメントの結果が公表されており、それによれば、EU域内から十分性認定により移転された個人データについて、日本からさらに第三国に再移転（onward transfer）する場合には、日本の個人情報保護法第24条（補完的ルール(4)）に従って移転を行えばよく、日本企業と第三国の企業間で、SCC（Standard Contractual Clauses、標準契約条項）を締結する等の追加措置が求められているわけではないとされている点です（パブリックコメント 132 番）[12][13]。

８　世界の他のデータ保護法制との関係性

冒頭で述べたとおり、米国カリフォルニア州のプライバシー法、中国の個人情報保護法、ブラジルの個人情報保護法など、現在データ保護法制は世界各国で立法の動きが見られ、何から手を付けるべきかという問題があります。この点、監督当局による執行事例やデータ主体からの訴訟リスク等を評価して、リスクの高い法域の対応から優先に進めるというリスク・ベースド・アプローチを行うことが重要です。

GDPR は相当程度厳格な規制であると言われていますが、それでもやはり、米国カリフォルニア州のプライバシー法（CCPA/CPRA）、中国の個人情報保護法、ブラジルの個人情報保護法は、それぞれ異なっており、GDPR 準拠のプライバシーポリシーを策定すればそれで十分というわけにはいきません。リスク・ベースド・アプローチに基づき、優先度が低いと考えられる法域についても、執行リスクが認められる場合には、ノーマークとするわけではなく、多少なりとも対応を行うことで、基本的には重大なリスクは抱えていないという状態を作っておくことが重要であると考えられます[14]。

第３　おわりに

弊所では、GDPR 対応・CCPA/CPRA 対応のプライバシーポリシーの策定や修正、データ処理の法的根拠の個別具体的な検討、代理人・DPO の選任の要否の検討、バイオメトリック（生体）情報や健康関連情報などのヘルスケア領域の個人データの処理など、クライアントの皆様のニーズに応じた法的助言を行っておりますので、ご相談・ご不明点等ございましたら、ご遠慮なく当職（新澤）までご連絡頂ければと存じます。

ここまでお読み頂きありがとうございました。今回のメールマガジンが皆様のご理解の一助になれば幸いです。本記事に関してご質問事項等ございましたら、冒頭の当職（新澤）のメールアドレスまでご連絡ください。

---

[12] パブコメ https://public-comment.e-gov.go.jp/servlet/Public?CLASSNAME=PCM1040&id=240000050&Mode=1
[13] 岡田 206 頁も同趣旨。
[14] 田中浩之著「第 3 回海外個人情報保護規制への対応 2022　GDPR、中国個人情報保護法、CPRA 等の法改正動向と実務のトレンド」BUSINESS LAWYERS https://www.businesslawyers.jp/articles/1109

以上

当事務所では、主として名刺交換をさせていただいた方を対象とし、有用な法律情報等をお知らせすべく定期的にメールマガジンを発行させていただいております。また、バックナンバーはこちらに掲載しておりますので、あわせてご覧ください。
本稿は一般的な情報を提供するもので、リーガルアドバイスを目的とするものではございません。本稿記載の見解は執筆担当者の個人的見解であり、当事務所の見解ではありません。個別の案件については当該案件の個別の状況に応じ、弁護士の適切なアドバイスを求めていただく必要がございます。お問い合わせ等ございましたら、執筆担当者までご遠慮なくご連絡くださいますよう、お願いいたします。

【配信停止・お問い合わせについて】
今後、本メールマガジンの配信又は配信停止をご希望の方、メールアドレスの変更その他お問い合わせがございましたら、大変お手数ではございますが、下記メールアドレスまでご連絡ください。
（clo_mlstop@clo.gr.jp）