西村あさひ法律事務所

EU-U.S. Data Privacy Framework に対する十分性認定のドラフトの公表(前編)

ヨーロッパ / 個人情報保護・データ保護規制ニューズレター　2022 年 12 月 23 日

執筆者:
E-mail 石川 智也　E-mail 菅 悠人
E-mail 佐々木 将也

2022 年 12 月 13 日、欧州委員会は、米国連邦商務省(DoC)が設定しようとしている EU-U.S. Data Privacy Framework に定められた個人データの保護に関する諸原則(DPF 原則)に準拠した個人データの処理を行う米国の事業者への個人データの移転に関する十分性認定のドラフト [1]を公表した [2]。上記ドラフトは、同年 10 月 7 日に公表された米国大統領令 14086(Executive Order 14086)[3]及びその関連規則を受けたものである。十分性認定のドラフトが採択され、正式に決定された暁には、DPF に参加する米国事業者に対して他に特段の保護措置等を実施することなく GDPR の適用を受ける個人データを移転できるようになる。正式決定は 2023 年の夏前となる見込みと報じられている。

本連載では、欧州委員会の十分性認定のドラフトの概要とその実務上の影響について、2 回に分けて紹介する。前編の本稿では、十分性認定のドラフトに至る背景(**1.**)と、DPF の核心部分である DPF 原則に対する評価(**2.**)を解説する。

本連載の目次

1. 背景
2. DPF 原則に対する評価　(以上、前編)
3. 米国大統領令 14086 に対する評価
4. 実務へのインパクトと今後の対応

1. 背景

GDPR 上、EEA 域外に個人データを移転するための要件の 1 つとして、移転先の国が個人データの保護について十分な保護水準を確保していること(十分性認定を受けていること)が挙げられている(GDPR 45 条 1 項)。従来、米国への個人データの移転は EU-U.S. Privacy Shield(以下「Privacy Shield」)という十分性認定の枠組みの 1 つに基づき行われていたが、2020 年 7 月、Schrems II 判決 [4]により上記枠組みが無効とされたため、欧州委員会と米国との間では新たな十分性認定の枠組み構築に向けた作業が開始されることとなり、今回の EU-U.S. Data Privacy Framework(以下「DPF」)につながった。

2022 年 10 月 7 日、米国の信号諜報活動に対する保護措置を強化する大統領令 Executive Order 14086(以下「EO14086」)(及びその授権を受けた司法省規則)が公表された [5]。これは、Schrems II 判決が問題視した 2 点、すなわち、米国

---

1 https://commission.europa.eu/system/files/2022-12/Draft%20adequacy%20decision%20on%20EU-US%20Data%20Privacy%20Framework_0.pdf 参照。

2 欧州委員会の公表は、https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7631 参照。欧州委員会による Q&A は、https://ec.europa.eu/commission/presscorner/detail/en/qanda_22_7632 参照。

3 https://www.whitehouse.gov/briefing-room/presidential-actions/2022/10/07/executive-order-on-enhancing-safeguards-for-united-states-signals-intelligence-activities/参照。

4 弊所ヨーロッパニューズレター2020 年 7 月 29 日号 https://www.nishimura.com/ja/newsletters/europe_200729.html 参照。

5 EO14086 第 3 項では、2 段階の救済メカニズムの第 2 段階としてデータ保護審査裁判所(DPRC)を設置するための規則の制定を司法長官に授権している。これを受け、2022 年 10 月 7 日、メリック・ガーランド司法長官は、DPRC を設置する新規則に署名した。司法省のコメントについては、https://www.justice.gov/opcl/redress-data-protection-review-court 参照。

© Nishimura & Asahi 2022

政府の監視プログラムに対する必要性及び比例性の制限の欠如と、違法監視に対する救済措置の不十分さに対処することを目的としたものであった。

今回の欧州委員会による十分性認定のドラフト(以下「十分性認定ドラフト」)の公表は、上記の流れの中で、米国側による、米国へ移転された個人データの扱いに係る保護を強化するための取組みを受けて、欧州委員会としてこれを評価し、米国への個人データの移転に新たな十分性認定を付与するための大きな一歩といえる。十分性認定ドラフトは、今後、欧州データ保護会議(EDPB)、閣僚理事会及び欧州議会による検討と意見表明等の手続を経て正式決定へと向かうことが見込まれている。

2. DPF 原則に対する評価

十分性認定ドラフトは、215 項に亘る前文と、全 4 条の本文、そして、DPF の概要等について記した 7 つの Annex からなる。

前提として、DPF に参加するためには、米国の事業者が DPF 原則に準拠した個人データの処理を行う旨の自己認証を行い、かかる自己認証をまとめた書面を米国連邦商務省(以下「DoC」)に提出することとなる。DoC は、自己認証に関する完全な書面の提出がなされたことを確認した場合には、DPF リストに当該提出者の名前を追加することとされており、当該リストに掲載された米国の事業者に対しては十分性認定に基づく個人データの移転が可能となる。自己認証とリスト掲載により十分性認定の対象を限定するという方式は、Privacy Shield 時代の方式を踏襲しており、かつ、下記で詳述する DPF 原則の主要な部分は、細部を除けば、Privacy Shield 時代に定められていた原則(EU-U.S. Privacy Shield Framework Principles)[6]の内容と基本的に共通している。このため、Privacy Shield 時代に既に自己認証を行っていた米国の事業者は、今般の DPF への参加も容易なはずであり、かかる事業者が今般の新たな十分性認定の枠組みに参加するに際して追加的な負担が生じないように考慮されている。

(1) DPF 原則

DPF 原則は、個人データの処理に関して一定の義務を規定しているところ、十分性認定ドラフト前文では、その内容について以下のような分析がなされている。DPF 原則は、端的にいえば、GDPR の基準及びルールのエッセンスをまとめたものである。上記のとおり、この DPF 原則の内容は、Privacy Shield 時代に定められていた原則と基本的に共通したものとなっている。

① **目的制限とオプトアウトの選択肢(Purpose limitation and choice)**：DPF 原則の中の Data Integrity and Purpose Limitation Principle は、GDPR 5 条 1 項 b 号と同様、データが当初収集された目的又は事後に承認された目的と適合しない態様でのデータ処理を禁止している(前文パラ 14)。また、同じく DPF 原則の中の Choice Principle により、事業者は、取得済みの個人データを新たな目的のために使用し又は第三者に開示するためには、データ主体にオプトアウトの機会を提供しなければならない(前文パラ 15)。

② **特別なカテゴリーの個人データの処理(Processing of special categories of personal data)**：DPF 原則の中の Choice Principle により、センシティブ情報(sensitive information)の処理に対しては特定の保護措置が適用される(前文パラ 17)。具体的には、DPF 原則に準拠して個人データを処理する事業者は、センシティブ情報を当初収集された目的又は事後に承認された目的以外の目的で処理する場合又はセンシティブ情報を第三者に開示する場合には、データ主体から事前の積極的明示的同意(affirmative express consent)を取得しなければならない(前文パラ 18)。

③ **データの正確性、最小化及びセキュリティ(Data accuracy, minimisation and security)**：DPF 原則の中の Data Integrity and Purpose Limitation Principle により、データ処理は処理目的に関連性のある範囲に限定され、データは予定された処理のために正確、完全かつ最新のものであることが確保されなければならない(前文パラ 21)。また、Choice Principle により、データは当初収集された目的又は事後に承認された目的に資する限度でのみ、個人データとして保持され得る。そして、DPF 原則の中の Security Principle は、GDPR32 条同様、処理のリスク及びデータの性質を考慮に入れた上で、適切な技術上及び組織上の措置を講ずる義務を規定している(前文パラ 24)。

④ **透明性(Transparency)**：DPF 原則の中の Notice Principle により、DPF 原則に準拠して個人データを処理する事業者は、GDPR 上の透明性要件同様、データ主体に対して、(i)DPF への参加の事実、(ii)収集されるデータの種類、(iii)処理の

6 https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg 参照。

© Nishimura & Asahi 2022

目的、(iv)個人データの開示対象となる可能性のある第三者の種類及び身元情報、(v)データ主体の権利、(vi)事業者の連絡先、(vii)利用可能な救済措置について、明確かつ目立つ言語により事前に通知しなければならない(前文パラ 26 及び 27)。また、DPF を反映したプライバシーポリシーを公開すると同時に、DoC のウェブサイト、DPF に参加する事業者のリスト(DPF List)及び代替的な紛争解決事業者のウェブサイトへのリンクをそれぞれ提供しなければならない(前文パラ 28、第 1 条)。

⑤ **データ主体の権利(Individuals rights)**:データ主体は、DPF 原則の中の Access Principle により、データに対するアクセス権、処理に対して異議を申し立てる権利及びデータを訂正又は消去させる権利を有する(前文パラ 30)。

⑥ **再移転の制限(Restrictions on onward transfer)**:DPF 原則の中の Accountability for Onward Transfer Principle により、DPF 原則に準拠して個人データを処理する事業者は、当該事業者から更に第三者に対して個人データを再移転すること(onward transfer)に対して一定の制限が課されている。具体的には、再移転は、(i)限定されかつ特定された目的のために、(ii)DPF 原則に準拠して個人データを処理する事業者と第三者との間の契約に基づいて、(iii)当該第三者が DPF Principles と同等の水準の保護を提供する場合にのみ、許容される(前文パラ 38)。

⑦ **アカウンタビリティ(Accountability)**:DPF 原則の中の Recource, Enforcement and Liability Principle により、DPF 原則に準拠して個人データを処理する事業者は、DPF 遵守の確保のための効果的な措置を実施し、かつ、プライバシーポリシーの記載を含め、DPF 遵守の確保を検証する措置を講じなければならない(前文パラ 45)。

(2) 管理、監視及び執行

DPF は DoC によって管理・モニタリングされ、DPF の不遵守に対する監視及び執行については、DoC、連邦取引委員会(以下「FTC」)又は連邦運輸省(以下「DoT」)によって実行される(前文パラ 47)。モニタリングの方法については、DoC は、無作為の抜き打ち調査(spot checks)を含め、複数のメカニズムにより DPF の遵守の状況を監視するものとされている(前文パラ 53)。

DPF 原則に準拠して個人データを処理する事業者は、FTC 又は DoT による管轄に服する(前文パラ 59)。FTC は、DPF 原則の不遵守について調査権限を有し、執行の一環として、行政又は連邦裁判所による差止めや民事上の損害賠償請求等を求めることができる。DoT は、航空会社によるプライバシー関連の実務について専属的な管轄を有している(前文パラ 63)。

(3) 救済手段

Recource, Enforcement and Liability Principle により、DPF 原則に準拠して個人データを処理する事業者は、EU のデータ主体のために、効果的な独立の救済手段を用意する必要があるが、同時に、データ主体は、拘束力のある仲裁を利用する権利をも有するとされている(前文パラ 67)。具体的には、EU のデータ主体は、DPF 原則に準拠して個人データを処理する事業者、無償の独立紛争解決機関、EU のデータ保護監督当局又は DoC に対して異議申立てをすることができるほか、EU のデータ保護監督当局及び DoC を通じて FTC に対して異議申立てを回付することができ、さらに、これらの手段が奏功しない場合には、EU-U.S. DPF パネルによる拘束力のある仲裁を発動させることができる(前文パラ 68~80)。

なお、これらの救済手段は(仲裁の発動を含め)、米国法の下での司法上の救済を排除するものではない(前文パラ 85)。

*　　*　　*

連載後編では、十分性認定ドラフトによる EO14086 に対する評価(**3.**)及び実務へのインパクトと今後の対応(**4.**)について解説する。

© Nishimura & Asahi 2022

当事務所では、クライアントの皆様のビジネスニーズに即応すべく、弁護士等が各分野で時宜にかなったトピックを解説したニューズレターを執筆し、随時発行しております。N&A ニューズレター購読をご希望の方は N&A ニューズレター　配信申込・変更フォームよりお手続きをお願いいたします。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。

本ニューズレターはリーガルアドバイスを目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、日本法または現地法弁護士の適切なアドバイスを求めていただく必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所　広報室　E-mail

© Nishimura & Asahi 2022