【ＧＤＰＲ】Privacy Shield を無効とする欧州司法裁判所の決定に関するＦＡＱ

執筆者：渡邉雅之
＊ 本ニュースレターに関するご相談などがありましたら、下記にご連絡ください。
弁護士法人三宅法律事務所
弁護士渡邉雅之
TEL 03-5288-1021
FAX 03-5288-1025
Email m-watanabe@miyake.gr.jp

欧州連合司法裁判所は、2020 年７月 23 日、EU（EEA）から米国への個人データの越境移転を認める EU と米国間で締結された **Privacy Shield** を無効であるとの判決をいたしました。

本ニュースレターは、欧州データ保護委員会（EDPB）が公表する同判決に関するＦＡＱ[1]を翻訳したものです。

○Privacy Shield とは

米国とＥＵとの間では、2000 年に、ＥＵ域内から米国に移転される個人データについてプライバシーに関するセーフハーバー原則に適合していると米国商務省が認定した米国企業に対してのみ、その情報の移転を認める「セーフハーバー協定」が結ばれていました。

しかしながら、セーフハーバー協定は、2015 年 10 月６日に欧州司法裁判所が当該協定を無効と判断されました。

これは、元ＣＩＡのスノーデン氏が、ＣＩＡ等の米国の国家安全保障当局が Facebook などのＳＮＳから無差別・大量の個人情報を取得していると暴露をしたことを契機に、ＥＵ市民がＥＵ域内の Facebook の現地法人に対して提起した訴訟です。

この司法判断を受けて、米国とＥＵは、従前のセーフハーバー協定に代わる新たな枠組みとして、2016 年２月に Privacy Shield を締結しました（ＧＤＰＲの十分性決定の一種）。

2020 年７月 23 日の欧州司法裁判所の判決により、Privacy Shield も無効とされたため、EU（EEA）から米国への個人データへの移転は、本ＦＡＱの規定に従ってなされる必要があります。

---

[1] Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems
https://edpb.europa.eu/sites/edpb/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf

〇今回の欧州司法裁判所の判決の影響は？

今回の判決により、従前の「セーフハーバー協定」と同様に、Privacy Shield によって、EU 域内の管理者（Controller）や取扱者（Processor）は、EU（EEA）域内から米国に所在する者（法人・個人）に個人データを移転することは認められなくなりました。

ただし、米国企業と標準契約条項（Standard Contractual Clauses（「SCC」））の締結したり、米国企業が拘束的企業準則（Binding Corporate Rules（BCR））を採用している場合は、当該米国企業に対して個人データを移転することは従前どおり認められます。

もっとも、EU 域内の企業（管理者・取扱者）と米国企業は、標準契約条項（SCC）や拘束的企業準則（BCR）により個人データを米国に移転することについて事前に評価し、その状況を考慮した評価結果と、実施できる補完的措置について検討することが求められます。

〇GDPR 第 49 条に基づく特例措置（適用除外）については認められるのか？

GDPR 第 49 条においては、①越境データ移転がデータ主体の同意に基づいている場合、②データ主体と管理者の間の契約の履行に必要な越境データ移転、③重要な公共の利益（EU または加盟国の法律で認められるもの）のために必要な個人データの越境データ移転に関しては、十分性の決定が認められていない国・地域の移転であって、標準契約条項（SCC）が締結されておらず、拘束的企業準則（BCR）が採用されていない場合であっても特例措置（適用除外）として認められるとされています。

ただし、欧州データ保護委員会（EDPB）はこれらの特例措置の適用は認められるものの、「不定期」の個人データの越境データ移転に限られ、「定期的（常態的）」な個人データの越境データ移転としては認められないとされています。

〇日本企業への影響は？

日本は、2019 年 1 月 23 日に欧州委員会から GDPR に基づき、日 EU 間で個人データ保護水準に関する十分性を認定を取得しています。

ただし、EU 域内から日本への個人データの移転に際しては、個人情報保護委員会の「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」[2]（「補完的ルール」）に基づく、個人情報保護法への上乗せ措置を遵守する必要があります。

日本企業が、米国を含む EU 域外の国・地域（十分性認定を受けている国・地域を除く）に拠点（現地法人・支店・駐在員事務所等）を有し、そこに個人データを移転する場合は、今回の判決に従い、当該拠点と標準契約条項（SCC）を締結して個人データを移転することが求められることになります。EU 域内から日本に一旦個人データが移転されれば、個人情報保護法+補完的ルールに基づく対応のみでよいという解釈もあり得ますが、EU 域内から必ずしも日本に移転されず、他の拠点に直接移転されるのであればこのような解釈にはリスクがあります。

---

[2] https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

【原文・翻訳】

Frequently Asked Questions on the judgment of the Court of Justice of the European Union in Case C-311/18 - Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems

欧州連合司法裁判所の C-311 / 18 事件の決定に関するよくある質問（FAQ）-データ保護委員会 v Facebook Ireland Ltd および Maximillian Schrems

Adopted on 23 July 2020

2020 年 7 月 23 日決定

This document aims at presenting answers to some frequently asked questions received by supervisory authorities (“SAs”) and will be developed and complemented along with further analysis, as the EDPB continues to examine and assess the judgment of the Court of Justice of the European Union (the “Court”).

The judgment C-311/18 can be found here, and the press release of the Court may be found here.

この文書は、監督当局（「SA」）が受け取ったいくつかのよくある質問（FAQ）への回答を提示することを目的としており、EDPB（欧州データ保護委員会）が欧州連合司法裁判所（「本裁判所」）の判決を引き続き調査および評価する際に、今後の分析とともに改訂および補完されます。

C-311 / 18 事件の判決はこちらをご覧ください。本裁判所のプレスリリースはこちらをご覧ください。

1) What did the Court rule in its judgment?

→ In its judgment, the Court examined the validity of the European Commission's Decision 2010/87/EC on Standard Contractual Clauses ("SCCs") and considered it is valid. Indeed, the validity of that decision is not called into question by the mere fact that the standard data protection clauses in that decision do not, given that they are contractual in nature, bind the authorities of the third country to which data may be transferred.

However, that validity, the Court added, depends on whether the 2010/87/EC Decision includes effective mechanisms that make it possible, in practice, to ensure compliance with the level of protection essentially equivalent to that guaranteed within the EU by the GDPR and that transfers of personal data pursuant to such clauses are suspended or prohibited in the event of the breach of such clauses or it being impossible to honour them. In that regard, the Court points out, in particular, that the 2010/87/EC Decision imposes an obligation on a data exporter and the recipient of the data (the "data importer") to verify, prior to any transfer, and taking into account the circumstances of the transfer, whether that level of protection is respected in the third country concerned, and that the 2010/87/EC Decision requires the data importer to inform the data exporter of any inability to comply with the standard data protection clauses, and where necessary with any supplementary measures to those offered by those clause, the data exporter then being, in turn, obliged to suspend the transfer of data and/or to terminate the contract with the data importer.

→ The Court also examined the validity of the Privacy Shield Decision (Decision 2016/1250 on the adequacy of the protection provided by the EU-U.S. Privacy Shield), as the transfers at stake in the context of the national dispute leading to the request for preliminary ruling took place between the EU and the United States ("U.S.").

The Court considered that the requirements of U.S. domestic law, and in particular certain programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes, result in limitations on the protection of personal data which are not circumscribed in a way that satisfies requirements that are essentially equivalent to those required under EU law **(footnote 1)** , and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities. As a consequence of such a degree of interference with the fundamental rights of persons whose data are transferred to that third country, the Court declared the Privacy Shield adequacy Decision invalid.

(footnote 1) The Court underlines that certain surveillance programmes enabling access by U.S. public authorities to personal data transferred from the EU to the U.S. for national security purposes do not provide for any limitations on the power conferred on the U.S.

authorities, or the existence of guarantees for potentially targeted non-US persons.

1）裁判所はその判決において何を決定しましたか？

→本裁判所は判決において、標準契約条項（「SCC」）に関する欧州委員会の 2010/87 / EC 決定の有効性について検討し、それが有効であると決定いたしました。事実、同決定の有効性は、同決定における標準的データ保護条項が、本質的に契約上のものであることを考えると、データが移転される可能性のある第三国の当局を拘束しないという単なる事実によって問題となることはありません。

ただし、本判決は、その有効性は 2010/87 / EC 決定において示されたとおり、実際に GDPR により EU 域内において保証されているレベルと本質的に同等の保護のレベルを確実に遵守され、かかる条項に違反した場合、またはそれらを遵守することが不可能である場合、かかる条項に基づく個人データの移転は一時停止または禁止される効果的なメカニズムが含まれているかどうかによります。

この点に関して、裁判所は特に、2010/87 / EC 決定は、データの輸出者とデータの受領者（「データの輸入者」）に、転送の前に検証し、 譲渡の状況、関係する第三国でそのレベルの保護が尊重されているかどうか検証する義務を課していると指摘しています。また、本裁判所は、2010/87 / EC 決定では、データ輸入者が標準のデータ保護条項に準拠できないことをデータ輸出者に通知する必要があること、および必要に応じて、同条項によって提供されている補完的措置がある場合、データ輸出者は、次に、データの移転を一時停止する、および/または、データ輸入者との契約を終了する義務があることを指摘しています。

→ 本裁判所は、中間判決の要請につながる国内紛争の状況で問題となっている移転が EU と米国（「米国」）の間で行われたため、Privacy Shield 決定（EU 及び米国間の Privacy Shield によって提供される保護の妥当性に関する 2016/1250 決定）の有効性についても検討しました。

本裁判所は、米国国内法の要件、特に米国の公的機関による、国家安全保障の目的で EU から米国に転送された個人データへのアクセスを可能にする特定のプログラムは、個人データの保護に制限をもたらしますが、EU 法**（脚注１）**で要求される要件と本質的に同等の要件を満たす方法で制限しておらず、また、同米国国内法は、裁判所に対して米国当局に対して訴訟を起こす権利をデータ主体に付与するものではない、と判断しています。データがその第三国に転送される個人の基本的権利に対するこのように一定程度妨害することから、裁判所は Privacy Shield による十分性決定は無効であると宣言しました。

（脚注１）本裁判所の決定は、国家安全保障の目的で EU から米国に移転された個人データへの米国公的機関によるアクセスを可能にする特定の監視プログラムは、米国当局に付与される権限にいかなる制限もしていないこと、また、潜在的に標的にされた非米国人

のための保証が存在しないことを強調しています。

2) Does the Court's judgment have implications on transfer tools other than the Privacy Shield?

→ In general, for third countries, the threshold set by the Court also applies to all appropriate safeguards under Article 46 GDPR used to transfer data from the EEA to any third country. U.S. law referred to by the Court (i.e., Section 702 FISA and EO 12333) applies to any transfer to the U.S. via electronic means that falls under the scope of this legislation, regardless of the transfer tool used for the transfer **(footnote 2).**

(footnote 2) Section 702 FISA applies to all "electronic communication service provider" (see the definition under 50 USC § 1881(b)(4)), while EO 12 333 organises electronic surveillance, which is defined as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a non electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction-finding equipment solely to determine the location of a transmitter" (3.4; b)).

2）本裁判所の判決は、Privacy Shield 以外の個人データの越境データ移転の方法にも影響しますか？

→一般的に、第三国の場合、本裁判所が設定した基準は、EEA から第三国への個人データの移転に適用される GDPR 第 46 条に基づく全ての適切な保護手段にも適用されます。本裁判所が言及する米国の法律（すなわち、外国情報監視法（FISA）第 702 条及び大統領令第 12333 号）は、電子的手段による米国への移転には、個人データの移転に使用される手段に関係なく、同法律の適用範囲に服します（脚注２）。

（脚注２）外国情報監視法（FISA）第 702 条はすべての「電子通信サービスプロバイダー」に適用され（50 USC§1881（b）（4）の定義を参照）、大統領令第 12333 号においては「電子的通信の当事者である個人の同意のない電子的手段による非公開通信の取得、又は非電子的通信の場合（ただし、送信機の位置を特定するためだけに無線方向探知機器を使用することは含まれない。）には通信の場所において目に見える形で存在する個人の同意のない電子的手段による非公開通信の取得」と定義されています。

3) Is there any grace period during which I can keep on transferring data to the U.S. without assessing my legal basis for the transfer?

→ No, the Court has invalidated the Privacy Shield Decision without maintaining its effects, because the U.S. law assessed by the Court does not provide an essentially equivalent level of protection to the EU. This assessment has to be taken into account for any transfer to the U.S.

3）移転の法的根拠について評価をせずに個人データを米国に移転し続けることができる猶予期間はありますか？

→いいえ。本裁判所が評価した米国の法律は本質的に同等のレベルの保護を EU に提供していないため、本裁判所は Privacy Shield 決定をその影響を維持することなく無効と判示しました。 この評価は、米国への個人データの移転の際に考慮する必要があります。

4) I was transferring data to a U.S. data importer adherent to the Privacy Shield, what should I do now?

→Transfers on the basis of this legal framework are illegal. Should you wish to keep on transferring data to the U.S., you would need to check whether you can do so under the conditions laid down below.

4)私（当社）は、Privacy Shield に準拠した米国のデータ輸入者に個人データを移転していましたが、どうすればよいですか？

→この法的枠組みに基づく個人データの米国への移転は違法です。米国への個人データの移転を継続する場合は、以下の条件で転送できるかどうかを確認する必要があります。

5) I am using SCCs with a data importer in the U.S., what should I do?

→The Court found that U.S. law (i.e., Section 702 FISA and EO 12333) does not ensure an essentially equivalent level of protection.

Whether or not you can transfer personal data on the basis of SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a caseby-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However, if you are intending to keep transferring data despite this conclusion, you must notify your competent SA **(footnote 3)**.

(footnote 3) See in particular recital 145 of the Court's judgment, and Clause 4(g) Commission decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) of Commission Decision 2004/915/EC.

5）私（当社）は、米国のデータ輸入者との間で標準契約条項（ SCCs）を締結していますが、どうすればよいでしょうか？

→本裁判所は、米国法（すなわち、外国情報監視法（FISA）第 702 条及び大統領令第 12333 号）は、GDPR と本質的に同等レベルの保護を保証していないと判示しています。

標準契約条項（SCC）に基づいて個人データを移転できるかどうかは、越境データ移転の状況を考慮した評価の結果と、実施できる補完的措置によって異なります。 越境データ移転を取り巻く状況をケースバイケースで分析した上で講じる標準契約条項（SCC）に基づく補完的措置においては、米国法が標準契約条項（SCC）による十分なレベルの保護を損なうことがないようにする必要があります。

越境データ移転の状況と可能な補完的措置を考慮して、適切な保護手段が確保されないという結論に達した場合、個人データの移転を一時停止または終了する必要があります。ただし、この結論にもかかわらず個人データを移転し続けるつもりである場合は、所管の監督当局（SA）に通知する必要があります。**（脚注３）**

（脚注３）特に、本裁判所の決定の前文第 145 項、委員会決定 2010/87/EU 号第 4(g)、および委員会決定 2001/497/EC 号第 5(a)および委員会決定 2004/915/EC 号の 2004 年の付属文書 II（c）をご参照ください。

6) I am using Binding Corporate Rules (“BCRs”) with an entity in the U.S., what should I do?

→ Given the judgment of the Court, which invalidated the Privacy Shield because of the degree of interference created by the law of the U.S. with the fundamental rights of persons whose data are transferred to that third country, and the fact that the Privacy Shield was also designed to bring guarantees to data transferred with other tools such as BCRs, the Court’s assessment applies as well in the context of BCRs, since U.S. law will also have primacy over this tool.

Whether or not you can transfer personal data on the basis of BCRs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. These supplementary measures along with BCRs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

If you come to the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, you are required to suspend or end the transfer of personal data. However if you are intending to keep transferring data despite this conclusion, you must notify your competent SA **(footnote 4)**.

(footnote 4) See in particular recital 145 of the Court’s judgment and Clause 4(g) of Commission Decision 2010/87/EU. See also Section 6.3 WP256 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/itemdetail.cfm?item_id=614109), and Section 6.3 WP257 rev.01 (Article 29 Working Party, Working Document setting up a table with the elements and principles to be found in Processor BCRs, endorsed by the EDPB, http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

6）私（当社）は、米国法人との間で拘束的企業準則（「BCRs」）を適用していますが、どうすればよいでしょうか？

→ 個人データが米国に移転される個人の基本的権利を米国法によって妨害していることにより Privacy Shield を無効にした本裁判所の判決、および、Privacy Shield は、拘束的企業準則（BCR）などの他の手段で移転された個人データに保証を提供するようにも設計されているという事実を前提とすると、米国法においても本手段を優先適用するため、裁判所の評価は拘束的企業準則（BCR）に関しても適用されます。

拘束的企業準則（BCR）に基づいて個人データを移転できるかどうかは、移転の状況を考慮した評価結果と、実施できる補完的措置によって異なります。越境データ 移転を取り巻く状況をケースバイケースで分析した後、拘束的企業準則（BCR）とともに、米国法によって、これらの補完的措置が保証する十分なレベルの保護に影響を与えないようにする必要があります。
個人データの越境データ移転の状況と可能な補完的措置を考慮して、十分な保護手段が確保されないという結論に達した場合、個人データの移転を一時停止または終了する必要があります。 ただし、この結論にもかかわらず個人データを転送し続けるつもりなら、所管の監督当局（SA）に通知する必要があります。**（脚注４）**

（脚注４） 特に、本裁判所の決定の前文 145 と委員会決定 2010/87/EU 号の第 4 条（g）を参照してください。 また、WP256 rev.01 の 6.3 条（欧州データ保護委員会（EDPB）によって承認された拘束的企業準則（BCR）に含まれる要素と原則をまとめた表を含む第 29 条作業部会の作業文書 http://ec.europa.eu/newsroom/article29/）、および 6.3 WP257 rev.01 の 6.3 条（第 29 条作業部会、欧州データ保護委員会（EDPB）によって承認された取扱者の拘束的企業準則（BCR）に含まれる要素と原則をまとめた表を含む作業文書、http：// ec .europa.eu / newsroom / article29 / item-detail.cfm？item_id = 614110）も参照のこと。

7) What about other transfer tools under Article 46 GDPR?

→ The EDPB will assess the consequences of the judgment on transfer tools other than SCCs and BCRs. The judgement clarifies that the standard for appropriate safeguards in Article 46 GDPR is that of “essential equivalence”.

As underlined by the Court, it should be noted that that Article 46 appears in Chapter V GDPR, and, accordingly, must be read in the light of Article 44 GDPR, which lays down that “all provisions in that chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by that regulation is not undermined”.

7)GDPR 第 46 条に規定されたその他の手段はどうでしょうか？

→欧州データ保護委員会（EDPB）は、標準契約条項（ SCC）および拘束的企業準則（BCR）以外の越境データ移転の手段に対する判断の結果を評価します。本判決は、GDPR 第 46 条に基づく十分なセーフガードの基準が「実質的に同等であること」の基準であることを明確にしています。

本裁判所が強調したように、第 46 条は、GDPR の第 V 章に記載されているため、「本章のすべての規定は、その規制によって保証されている自然人の保護レベルが損なわれないように適用されるものとする。」と規定している GDPR の第 44 条に照らして解釈する必要があることに留意する必要があります。

8) Can I rely on one of the derogations of Article 49 GDPR to transfer data to the U.S.?

→It is still possible to transfer data from the EEA to the U.S. on the basis of derogations foreseen in Article 49 GDPR provided the conditions set forth in this Article apply. The EDPB refers to its guidelines on this provision **(footnote 5)**.

(footnote 5) See EDPB Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018, https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf, p.3.

In particular, it should be recalled that when transfers are based on the consent of the data subject, it should be:

- explicit,
- specific for the particular data transfer or set of transfers (meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place even if this occurs after the collection of the data has been made), and
- informed, particularly as to the possible risks of the transfer (meaning the data subject should also informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented).

With regard to transfers necessary for the performance of a contract between the data subject and the controller, it should be borne in mind that personal data may only be transferred when the transfer is occasional. It would have to be established on a case-by-case basis whether data transfers would be determined as “occasional” or “non-occasional”. In any case, this derogation can only be relied upon when the transfer is objectively necessary for the performance of the contract.

In relation to transfers necessary for important reasons of public interest (which must be recognized in EU or Member States’ **(footnote 6)** law), the EDPB recalls that the essential requirement for the applicability of this derogation is the finding of an important public interest and not the nature of the organisation, and that although this derogation is not limited to data transfers that are “occasional”, this does not mean that data transfers on the basis of the important public interest derogation can take place on a large scale and in

a systematic manner. Rather, the general principle needs to be respected according to which the derogations as set out in Article 49 GDPR should not become “the rule” in practice, but need to be restricted to specific situations and each data exporter needs to ensure that the transfer meets the strict necessity test.

(footnote 6) References to “Member States” should be understood as references to “EEA Member States”.

8）個人データを米国に移転するために、GDPR 第 49 条に規定されている各適用除外のうちの 1 つに依拠することができますか？

→GDPR 第 46 条に規定されている条件が適用される場合、同条で予測される特例に基づいて、EEA から米国に個人データを移転することは引き続き可能です。欧州データ保護委員会（ EDPB）は本規定に関するガイドラインを参照します**（脚注５）**。

（脚注５）2018 年 5 月 25 日に採択された規則 2016/679（GDPR）に基づく第 49 条の特例措置に関する欧州データ保護委員会(EDPB)ガイドライン 2/2018 号を参照してください。https：//edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf、p.3 。

特に、越境データ移転がデータ主体の同意に基づいている場合は、以下のことに留意する必要がある。

- 明確であること
- 特定の越境データ移転または一連の越境データ移転に際して個別になされること（すなわち、個人データの収集が行われた後であっても、越境データ移転を実行する前に、データ輸出者が特定の同意を得る必要があります。）、および
- 特に越境データ移転の潜在的なリスクについて情報が与えられていること（すなわち、データ主体は、個人データについて十分な保護を提供せず、十分な安全管理措置が講じられていない国に移転されるという事実から生じる特定のリスクについても情報提供されるべきであるということです。）。

データ主体と管理者の間の契約の履行に必要な越境データ移転については、越境データ移転が不定期に行われる場合にのみ個人データを移転できることにご留意ください。 越境データ移転が「不定期」または「定期」になされているか否かは、ケースバイケースで判断する必要があります。 いずれの場合も、本適用除外の手段は、契約の履行のために客観的に個人データの移転が必要な場合にのみ依拠することができます。

重要な公共の利益（これはEUまたは加盟国（**脚注６**）の法律で認められるものでなければなりません。）のために必要な個人データの越境データ移転に関しては、この適用除外の適用のための実質的な要件は、当該組織の固有のものではなく、重要な公益に基づくものでなければならず、また、この適用除外は「不定期」に行われる越境データ移転に限定されないものの、重要な公共の利益の適用除外に基づく越境データ移転が大規模かつ体系的に行われることを意図するものではないと欧州データ保護委員会（EDPB）が解釈していることに留意する必要があります。むしろ、GDPR第49条に規定されている特例措置は、実際には「ルール」になるべきではなく、特定の状況に限定して適用する必要があり、各データ輸出者は、越境データ移転が厳密な必要性テストを満たすようにする必要があるという原則を尊重する必要があります。

（脚注６）「加盟国」とは、「EEA加盟国」のことである。

9) Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?

→ The Court has indicated that SCCs as a rule can still be used to transfer data to a third country, however the threshold set by the Court for transfers to the U.S. applies for any third country. The same goes for BCRs.

The Court highlighted that it is the responsibility of the data exporter and the data importer to assess whether the level of protection required by EU law is respected in the third country concerned in order to determine if the guarantees provided by the SCCs or the BCRs can be complied with in practice. If this is not the case, you should assess whether you can provide supplementary measures to ensure an essentially equivalent level of protection as provided in the EEA, and if the law of the third country will not impinge on these supplementary measures so as to prevent their effectiveness.

You can contact your data importer to verify the legislation of its country and collaborate for its assessment. Should you or the data importer in the third country determine that the data transferred pursuant to the SCCs or to the BCRs are not afforded a level of protection essentially equivalent to that guaranteed within the EEA, you should immediately suspend the transfers. In case you do not, you must notify your competent SA **(footnote 7)**.

(footnote 7) See in particular recital 145 of Court's judgment . In relation to SCCs, see Clause 4(g) Commission Decision 2010/87/EU, as well as Clause 5(a) Commission Decision 2001/497/EC and Annex Set II (c) Commission Decision 2004/915/EC. In relation to BCRs, see Section 6.3 WP256 rev.01 (endorsed by the EDPB), and Section 6.3 WP257 rev.01 (endorsed by the EDPB).

→ Although, as underlined by the Court, it is the primary responsibility of data exporters and data importers to assess themselves that the legislation of the third country of destination enables the data importer to comply with the standard data protection clauses or the BCRs, before transferring personal data to that third country, the SAs will also have a key role to play when enforcing the GDPR and when issuing further decisions on transfers to third countries. As invited by the Court, in order to avoid divergent decisions, they will thus further work within the EDPB in order to ensure consistency, in particular if transfers to third countries must be prohibited.

9）標準契約条項（SCC）または拘束的企業準則（BCR）を引き続き使用して、米国以外の別の国に個人データを移転できますか？

→本裁判所の決定は、原則として、標準契約条項（SCC）を第三国への個人データの転送に引き続き使用できることを示していますが、米国への移転について裁判所が設定した基準は、どの第三国への移転にも適用されます。 拘束的企業準則（BCR）についても同様です。

本裁判所は、標準契約条項（SCC）または拘束的企業準則（BCR）によって提供される保護措置を実際に遵守できるかどうかを判断するために、個人データが移転される第三国において、EU 法が求めている個人データの保護レベルが尊重されているかどうかを評価することは、データ輸出者およびデータ輸入者の責任であることを強調しています。

これが当てはまらない場合、EEA で提供されているものと実質的に同等のレベルの個人データの保護を確保するための補完的な対策を提供できるかどうか、および、第三国の法律がこれらの補完的措置に影響を与えず、それらの有効性を妨げないかどうかを評価する必要があります。

データ輸出者は、データ輸入者に連絡して、その国の法律を確認し、共同でその評価を行うことができます。データ輸出車または第三国のデータ輸入車が標準契約条項（SCC）または拘束的企業準則（BCR）に従って移転された個人データについて、EEA 内で保証されているレベルと実質的に同等のレベルの保護が提供されていないと判断した場合、直ちに個人データの移転を一時停止する必要があります。 そうしない場合は、所管の監督当局（SA）に通知する必要があります**（脚注７）**。

（脚注７）特に本裁判所の決定の前文 145 を参照してください。 標準契約条項（SCC）に関しては、委員会決定 2010/87 / EU の第４条(g)、および委員会決定 2001/497 / EC の第 5 条(a)および委員会決定 2004/915 / EC の附属書 II（c）を参照のこと。拘束的企業準則（BCR）に関しては、（欧州データ保護委員会（EDPB）によって承認された）WP256 rev.01 の 6.3 条、および（欧州データ保護委員会（EDPB）によって承認された）WP257 rev.01 の 6.3 条を参照してください。

→ 本裁判所の決定によって強調されているように、個人データを第三国に移転する前に、移転先の第三国の法制がデータ輸入者により標準データ保護条項または拘束的企業準則（BCR）を遵守することができるものか否かを評価するのは、第一義的にデータ輸出者及びデータ輸入者の責任ですが、監督当局（SA）は、GDPR を執行する場合、および、第三国への移転に関する更なる決定を行う場合においても重要な役割を担います。本裁判所によって判示されているとおり、矛盾した決定を回避するために、特に第三国への移転を禁止しなければならない場合、監督当局（SA）は欧州データ保護委員会（EDPB）においてさらに作業を進めるでしょう。

10) What kind of supplementary measures can I introduce if I am using SCCs or BCRs to transfer data to third countries?

→ The supplementary measures you could envisage where necessary would have to be provided on a case-by-case basis, taking into account all the circumstances of the transfer and following the assessment of the law of the third country, in order to check if it ensures an adequate level of protection.

The Court highlighted that it is the primary responsibility of the data exporter and the data importer to make this assessment, and to provide necessary supplementary measures. The EDPB is currently analysing the Court's judgment to determine the kind of supplementary measures that could be provided in addition to SCCs or BCRs, whether legal, technical or organisational measures, to transfer data to third countries where SCCs or BCRs will not provide the sufficient level of guarantees on their own.

The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance.

10）当社が標準的契約条項（SCC）または拘束的企業準則（BCR）を使用して個人データを第三国に転送する場合、どのような補完的措置を導入できますか？

→ 十分なレベルの保護が保証されているかどうか確認するため、補完措置は、越境データ移転のすべての状況を考慮し、第三国の法律の評価に従って、ケースバイケースで提供する必要があります。

本裁判所は、この評価を行い、必要な補完的措置を提供するのは、データ輸出者およびデータ輸入者の主要な責任であると強調しました。

欧州データ保護委員会（EDPB）は現在、標準契約条項（SCC）または拘束的企業準則（BCR）が十分なレベルを提供しない第三国に個人データを移転するために、法的、技術的または組織的措置にかかわらず、標準契約条項（SCC）または拘束的企業準則（BCR）だけでは十分なレベルの保護を提供しない場合において提供できる補完的措置の種類を決定するために裁判所の判断を分析しています。

欧州データ保護委員会（EDPB）は、これらの補完的措置が何を構成できるかをさらに調査しており、今後、追加のガイダンスを提供する予定です。

11) I am using a processor that processes data for which I am responsible as controller, how can I know if this processor transfers data to the U.S. or to another third country?

→ The contract you have concluded with your processor in accordance with Article 28.3 GDPR must provide whether transfers are authorised or not (it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer).

→ Authorization has also to be provided concerning processors to entrust sub-processors to transfer data to third countries. You should pay attention and be careful, because a large variety of computing solutions may imply the transfer of personal data to a third country (e.g., for storage or maintenance purposes).

11）当社が管理者（controller）として責任を有している個人データを取扱う取扱者（processor）を使用していますが、この取扱者が個人データを米国またはその他の第三国に移転するかどうかをどのようにして知ることができますか？

→ GDPR 第 28.3 条に従って管理者が取扱者と締結した契約においては、個人データの移転が許可されているかどうかを規定しておく必要があります（たとえば、管理目的のために、第三国からの個人データへのアクセスを許容することであっても、「移転」に該当することに留意する必要があります。）。

→ 再取扱者に第三国への個人データを移転することを委託するための取扱者に関する権限についても事前に与えて必要があります。様々なコンピューティングソリューションにおいても、（例えば、保管目的で）個人データが第三国に移転される可能性があるため、注意を払っておく必要があります。

12) What can I do to keep using the services of my processor if the contract signed in accordance with Article 28.3 GDPR indicates that data may be transferred to the U.S. or to another third country?

→ If your data may be transferred to the U.S. and neither supplementary measures can be provided to ensure that U.S. law does not impinge on the essentially equivalent level of protection as afforded in the EEA provided by the transfer tools, nor derogations under Article 49 GDPR apply, the only solution is to negotiate an amendment or supplementary clause to your contract to forbid transfers to the U.S. Data should not only be stored but also administered elsewhere than in the U.S.

→ If your data may be transferred to another third country, you should also verify the legislation of that third country to check if it is compliant with the requirements of the Court, and with the level of protection of personal data expected. If no suitable ground for transfers to a third country can be found, personal data should not be transferred outside the EEA territory and all processing activities should take place in the EEA.

12）GDPR 第 28.3 条に基づいて締結された契約において、個人データが米国またはその他の第三国に移転される可能性があることが示されている場合、取扱者のサービスを引き続き使用するにはどうすればよいですか？

→ 個人データが米国に移転される可能性があり、移転手段によって提供される EEA で提供されるものと実質的に同等のレベルの保護に米国法が影響を及ぼさないことを保証するための補完的な手段が提供できない場合、または GDPR 第 49 条に基づく適用除外が適用されない場合、唯一の解決策は、米国への個人データの移転を禁止するために契約の修正条項または補完条項を交渉することです。個人データは米国内以外の場所に保存・管理されないようにする必要があります。

→個人データが別の第三国に移転される可能性がある場合は、当該第三国の法律を検証して、それが本ｎ裁判所の決定で示された要件に準拠しているかどうか、および予想される個人データの保護レベルに準拠しているかどうかを確認する必要があります。 第三国への個人データの移転に適した根拠が見つからない場合、個人データは EEA の域外に移転されるべきではなく、すべての処理活動は EEA で行われるべきです。