



- I. 欧州司法裁判所による Schrems II 事件判決と日系企業の GDPR 対応への影響
～SCC 締結企業に課される新たな義務と補完的措置の実装～
- II. 添付資料: 欧州データ保護評議会(EDPB)が公表した Q&A の英日対訳(参考訳)

2020年
7月29日号

I. 欧州司法裁判所による Schrems II 事件判決と日系企業の GDPR 対応への影響 ～SCC 締結企業に課される新たな義務と補完的措置の実装～ 執筆者: 石川 智也、菅 悠人

欧州司法裁判所は、2020年7月16日、いわゆる Schrems II 事件の判決(以下「本判決」という)¹を下しました。本判決は、①EU から米国に個人データを移転するための枠組みの1つであるプライバシーシールドを無効とする一方で、②EU から個人データの保護の水準が十分であるとの認定を受けていない国に個人データを移転するための枠組みである標準契約条項(Standard Contractual Clauses。以下「SCC」という)の有効性は維持しています。本判決は、SCC の有効性が維持されたことから、日系企業の GDPR 対応への影響は限定的であるかのように思われがちですが、**SCC の利用に当たって企業に新たな義務を課しているため、SCC に基づいて十分性認定を受けていない国に個人データを移転している企業にとっては、対応が必要となる可能性があることに注意が必要です。**このような状況を受けて、欧州データ保護評議会(European Data Protection Board。以下「EDPB」という)も、2020年7月23日付けで Q&A²を公表しています。

具体的には、SCC の利用に際して、当事者間で締結されている契約の内容のみならず、移転先の国の公的機関による移転されたデータへのアクセス(いわゆるガバメント・アクセス)に関して移転先の国の法制度を考慮した上で、EU 域内の保証と実質的に同等の水準の個人データの保護を保障することが求められるようになりました。本判決の後、サーベイランスプログラムの存在を理由にプライバシーシールドが無効とされた米国のほか、類似のサーベイランスプログラムの存在が指摘されるいくつかの国については、現行 SCC に基づく個人データの移転が不可能である、又は疑義がある旨を表明するデータ保護監督当局も現れています。

また、SCC だけでは EU 域内の保障と本質的に同等の水準の個人データの保護が保障できないおそれがある場合には、補完的措置(supplemental measures)を講じて対応する必要があるとされており、その具体的内容については EDPB が今後指針を公表

¹ Case C-311/18, Data Protection Commissioner v. Facebook Ireland Ltd & Maximilian Schrems, ECLI:EU:C:2020:559 (Jul. 16, 2020), available at <https://curia.europa.eu/juris/document/document.jsf?jsessionid=BD731F5130B963C7072D2F6851E77B5E?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=11046615>

² European Data Protection Board, *European Data Protection Board publishes FAQ document on CJEU judgment C-311/18 (Schrems II)* (Jul. 24, 2020), available at https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en.

本ニュースレターは法的助言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助言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。

本ニュースレターに関する一般的なお問い合わせは、下記までご連絡ください。

西村あさひ法律事務所 広報室 (E-mail: newsletter@jurists.co.jp)

することが予定されています。

したがって、GDPR の適用を受ける個人データを十分性認定を受けていない国に移転している日系企業においては、①越境移転の根拠を確認し、②プライバシーシールドに基づいて移転を行っているものについては SCC を締結する等して根拠を改める、③SCC に基づいて移転を行っているものについては、本判決と EDPB の公表している Q&A に沿って移転先の国の法制度の調査・評価を開始し、ガバメント・アクセスによる影響があり得る法域については、今後 EDPB が公表する補完的措置の実装を検討することが必要になります。

なお、移転先の国における個人データへのガバメント・アクセスの問題については、2020 年改正個人情報保護法により強化された国外移転規制にも関係があります。すなわち、改正後は、本人の同意に基づいて外国にある第三者に個人データを提供する場合には、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供する必要があるとされており、「当該外国における個人情報の保護に関する制度」としては、移転先の国における個人データへのガバメント・アクセスの有無も論点として指摘されているところです。したがって、日本企業としては、本判決への対応のみならず、2022 年春に施行予定の改正個人情報保護法との関係でも、ガバメント・アクセスの動向について把握することが求められています。

添付は、EDPB が 2020 年 7 月 23 日付けで公表した Q&A の参考訳となりますので、ご参照ください。

また、本判決については、2020 年 7 月 31 日から 8 月 31 日まで、7 月 29 日に当事務所で開催したリーガルフォーラムオンラインを収録したものを放映しますので、そちらもご参照ください。



いしかわ のりや
石川 智也

西村あさひ法律事務所 パートナー弁護士

n_ishikawa@jurists.co.jp

2006年弁護士登録。2005年東京大学法学部卒業、2015年バージニア大学ロースクール卒業(LL.M.)、2016年ミュンヘン知的財産法センター卒業(LL.M.)、Noerr法律事務所ミュンヘンオフィスに出向、2017年ニューヨーク州弁護士登録。GDPR、CCPA、タイの個人情報保護法を初めとするグローバルでの個人情報保護法制・データ規制へのコンプライアンス対応について多くの日本企業にアドバイスを提供しており、関連する講演・執筆記事も多数。日本経済新聞社による「2019年に活躍した弁護士ランキング」の「データ関連分野」で、総合ランキング1位(企業票+弁護士票)。情報法制学会会員、Certified Information Privacy Professional/Europe(CIPP/E)。2020年にドイツのフランクフルト・デュッセルドルフに開設予定の西村あさひ法律事務所欧州拠点の代表に就任予定。



すが ゆうじん
菅 悠人

西村あさひ法律事務所 弁護士

y_suga@jurists.co.jp

2009年弁護士登録。2016年コロンビア大学ロースクール卒業(LL.M.)。2017年パリ第二大学修士課程卒業(LL.M. de droit français, européen et international des affaires)、フランス・パリ弁護士会登録。2017年より2018年までウィルマーヘイル法律事務所(ロンドン及びブリュッセルオフィス)へ出向。国際案件の経験が豊富で、外国の法令に関する知見も広い。特にEUにおける規制関連法全般について現地実務や法令改正等、最新の動向を踏まえた助言を行っている。

II. 添付資料: 欧州データ保護評議会(EDPB)が公表した Q&A の英日対訳(参考訳)

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*
*Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and
Maximillian Schrems*における欧州司法裁判所の判決に関するFAQ

Adopted on 23 July 2020

2020年7月23日採択

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”).

本文書は、監督当局(以下「当局」という)に頻繁に寄せられるご質問に回答することを目的としています。EDPBは、引き続き欧州司法裁判所(以下「裁判所」という)の判決を検討及び評価しているため、本文書はアップデートされ、また、更なる分析によって補完される予定です。

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

C-311/18の判決は[ここ](#)(訳注: 原文のリンク先参照)で、裁判所のプレスリリースは[ここ](#)(訳注: 原文のリンク先参照)で、それぞれ見ることができます。

1) What did the Court rule in its judgment?

裁判所は本判決において、どのような判示をしましたか。

- 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.

本判決において、裁判所は、標準契約条項(以下「SCC」という)に関する欧州委員会の決定2010/87/ECの有効性を検討し、それが有効であると判断した。実際、決定の有効性は、その決定における標準データ保護条項が、その性質上契約であるとすれば、データが移転される可能性のある第三国の権能を拘束しないという事実によって問題視されるものではない。

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.

しかし、裁判所は、2010/87/ECの決定の有効性は、GDPRによってEU域内で保証された保護水準と実質的に同等の保護水準の遵守の確保を可能にするための効果的なメカニズムがその決定に含まれているか、また、当該条項に違反した場合、又は当該条項を遵守することが不可能な場合に、当該条項に基づく個人データの移転が停止又は禁止されるか次第である、とも示している。

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

この点に関し、裁判所は、とりわけ、2010/87/EC決定は、データ輸出者及びデータの受領者(以下「データ輸入者」という)に対し、移転前に、かつ移転の状況を考慮して、当該第三国において上記保護水準が尊重されているか検証する義務を負い、かつ、2010/87/EC決定は、データ輸入者に対し、標準データ保護条項、及び、必要な場合には当該条項によって提供されている措置への補完的措置を遵守できない旨をデータ輸出者に通知することを要求し、そして、データ輸出者は、データの移転を停止し、及び/又はデータ輸入者との契約を終了する義務を負うと指摘する。

- 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.”).

裁判所は、先決裁定の要請に繋がる国内紛争の文脈で問題となった移転がEUとアメリカ合衆国(以下「米国」という)の間で行われたものであるため、プライバシーシールド決定(EU-米国プライバシーシールドによって提供される保護の十分性に関する決定2016/1250)の有効性も検討した。

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 law³, and that this legislation does not grant data subjects actionable rights before the courts against the U.S. authorities.

裁判所は、米国の国内法の要件、及び、特に国家安全保障の目的でEUから米国へ移送された個人データへの米国の公的機関によるアクセスを可能にする一定のプログラムは、個人データの保護に制限を生じさせるものであり、その制限はEU法で要求されている要件と実質的に同等の要件を満たす方法に限られていないこと、及び、この法律は、米国当局に対する裁判での請求を可能とする権利をデータ主体に付与するものではないことを検討した。

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.

裁判所は、データが第三国に移転された人々の基本的権利への干渉がこのような程度にまで及ぶ結果として、プライバシーシールドの十分性認定は無効であると宣言した。

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

裁判所の判断は、プライバシーシールド以外の移転手段に影響を及ぼしますか。

- 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

³ 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.

裁判所は、米国の公的機関が国家安全保障の目的でEUから米国に移転される個人データにアクセスできるようになる特定の監視プログラムが、米国当局に付与される権限に何ら制限を設けておらず、また、ターゲットとされる可能性のある米国民以外の者への保証を設けていないことを強調する。

of the transfer tool used for the transfer⁴.

一般論として、第三国にとって、裁判所によって設定された限界は、EEAから第三国へのデータ移転のために利用されるGDPR46条の下での適切な保護措置の全てに適用される。

裁判所により言及された米国法(すなわち、外国諜報監視法(FISA)702項及び大統領令(EO)12333)は、移転²に利用される移転ツールにかかわらず、当該米国法の適用範囲に該当する電子的手段による米国への移転に適用される。

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?

移転の法的根拠を評価することなく、米国へのデータ移転を継続できる猶予期間はありますか。

→ 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.

ない。裁判所は、裁判所によって評価された米国法がEUと実質的に同等の保護水準を提供していないため、その効果を維持することなくプライバシーシールドの決定を無効にしている。米国への移転については、この判断を考慮しなければならない。

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

私はプライバシーシールドに準拠して米国のデータ輸入者にデータを移転していましたが、現時点でどうすべきでしょうか。

→ 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.

この法的枠組みに基づく移転は違法である。米国へのデータ移転を継続したい場合には、以下に規定する条件でデータ移転が可能か確認する必要がある。

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

私は米国のデータ輸入者との間でSCCを利用していますが、どうすべきでしょうか。

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

裁判所は、米国法(すなわち、外国諜報監視法(FISA)702項及び大統領令(EO)12333)は、実質的に同等の保護水準を確保していないと判断した。

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 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.

SCCに基づいて個人データを移転できるかは、移転の状況や実施可能な補完的措置を考慮した上での、評価の結果次第である。移転を巡る状況をケース・バイ・ケースで分析し、SCCに加えて講じられる補完的措置によって、SCCが保障する十

⁴ 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)).

外国諜報監視法(FISA)702 条は、全ての「電子通信サービスプロバイダ」(合衆国法典 50 編 1881 条(b)(4)に基づく定義を参照)に適用され、一方、大統領令(EO)12333 は、「電子通信の当事者である者の同意なしに、又は非電子通信の場合には、通信場所で目に見える形で存在する者の同意なしに、ただし、送信機の位置を決定するためだけに無線方向探知機を使用することを含まない、電子手段による非公開通信の取得」(3.4; b)として定義される電子的な監視を組織する。

分な水準の保護に米国法が影響を及ぼさないようにすることを確保する必要があると考えられる。

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 SA⁵.

移転の状況及び実施可能な補完的措置を考慮しても、適切な保護措置が確保されない可能性があるという結論に達した場合、個人データの移転を停止又は終了する必要がある。但し、上記結論にもかかわらず移転の継続を希望する場合には、管轄する当局に通知しなければならない。

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

私は米国企業との間で拘束的企業準則(BCR)を利用していますが、どうすべきでしょうか。

- 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.

データが第三国に移転される者の基本的権利に対する米国法による干渉の程度を理由にプライバシーシールドを無効とした裁判所の判決と、プライバシーシールドがBCRのような他のツールで移転されたデータに保証を与えるために設計されたという事実を踏まえると、米国法がBCRにも優先するため、裁判所の評価はBCRの文脈においても適用される。

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. BCRに基づいて個人データを移転できるかは、移転の状況や実施可能な補完的措置を考慮した上での、評価の結果次第である。移転を巡る状況をケース・バイ・ケースで分析し、BCRに加えて講じられる補完的措置によって、BCRが保障する十分な水準の保護に米国法が影響を及ぼさないようにすることを確保する必要があると考えられる。

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 SA⁶.

移転の状況及び実施可能な補完的措置を考慮しても、適切な保護措置が確保されない可能性があるという結論に達した場合、個人データの移転を停止又は終了する必要がある。但し、上記結論にもかかわらず移転の継続を希望する場合には、管轄する当局⁴に通知しなければならない。

⁵ 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.

特に、本判決の前文 145、並びに、委員会決定 2010/87/EU の 4(g)項、委員会決定 2001/497/EC の 5(a)項、及び委員会決定 2004/915/EC の別紙セット II(c)を参照のこと。

⁶ 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, https://ec.europa.eu/newsroom/article29/item-detail.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, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110).

特に、本判決の前文 145、委員会決定 2010/87/EU の 4(g)項を参照のこと。WP256 rev.01(29 条作業部会。BCR において判断される要素及び原則を備えた一覧を設定する作業文書。EDPB によって承認。https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614109)の 6.3 節、及び、WP257 rev.01(29 条作業部会。処理者 BCR において判断される要素及び原則を備えた一覧を設定する作業文書。EDPB によって承認。https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614110)の 6.3 節も参照のこと。

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

GDPR46条において認められている他の移転ツールはどうでしょうか。

→ 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”.

EDPBは、SCCとBCR以外の移転ツールへの本判決の影響を評価する予定である。本判決は、GDPR46条における適切な保障措置の基準が「実質的に同等」という基準であることを明確にしている。

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*”.

裁判所によって強調されているように、46条は、GDPRのV章に規定されており、したがって、「この章のすべての規定は、GDPRによって保障される自然人の保護の水準が損なわれないようにするために適用される」と規定しているGDPR44条に鑑みて解釈されなければならないということに留意すべきである。

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

米国にデータを移転するために、GDPR49条の特例(derogation)の一つに依拠できますか。

→ 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 provision⁷.

GDPR49条に定める条件が適用される場合には、同条が予定する特例に基づいてEEAから米国にデータを移転することも可能である。EDPBは、この条項に関する指針を参照する。

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

特に、移転がデータ主体の同意に基づく場合には、同意が以下の要件を満たす必要があることに留意すべきである。

- explicit,
- 明示的であること。
- 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
- 特定の1回又は一組のデータ移転のためのものであること(データの収集後にデータの移転が行われる場合であっても、移転が行われる前にデータ輸出者が確実に特定の同意を取得するようにしなければならないことを意味する)。
- 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).
- 特に、移転により生じるおそれのあるリスクについて情報提供されなければならないこと(データ主体は、データが適切な保護を提供していない国に移転されること、及びデータの保護を提供することを目的とした適切な保護措置が実施されていないこと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ことを意味する)。

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.

⁷ 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.

2018年5月25日に採択された、規則2016/679に基づく49条の特例に関するEDPBガイドライン2/2018(https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf)の3頁を参照のこと。

データ主体と管理者間の契約の履行のために必要な移転に関しては、移転が時折行われる場合にのみ個人データを移転できることに留意する必要がある。データ移転が「時折」又は「時折ではない」との判断は、ケースバイケースで行われる必要がある。何れにせよ、この特例は、移転が客観的に契約の履行のために必要な場合に限り依拠することができる。

In relation to transfers necessary for important reasons of public interest (which must be recognized in EU or Member States’⁸ 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.

公益上の重要な理由のために必要な移転に関連しては(公益は、EU又は加盟国⁶法により認められなければならない)、EDPBは、この特例適用にあたっての本質的な要件は、重要な公益の認定であって、組織の性質ではないこと、また、この特例は「時折」起こるデータの移転に限られるものではないが、重要な公益の特例に基づくデータの移転を大規模かつ体系的に行うことができるということの意味するものではないということを喚起する。むしろ、原則として尊重されるべきことは、GDPR49条に規定されている特例が実際に「原則」になるべきではなく、特定の状況に限定される必要があること、そして、各データ輸出者は移転が厳格な必要性のテストを満たすようにする必要があることである。

**9) Can I continue to use SCCs or BCRs to transfer data to another third country than the U.S.?
米国以外の第三国にデータを移転するために、引き続きSCCやBCRを利用できますか。**

→ 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. 裁判所は、原則としてSCCを第三国へのデータ移転に使用できると示しているが、米国への移転のために裁判所によって設定された限界は、いかなる第三国に対しても適用される。BCRについても同じことがいえる。

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.

裁判所は、SCC又はBCRによって提供されている保証が実際に遵守できるかどうかを判断するために、EU法によって要求される保護水準が当該第三国において遵守されているかを評価することは、データ輸出者及びデータ輸入者の責任であることを強調した。もし遵守されていないのであれば、EEAにおいて提供されているのと実質的に同等の水準の保護を確保するための補完的措置を提供できるか、また、当該第三国の法律がそれらの補完的措置に影響せず、その有効性を阻害することがないかを評価すべきである。

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

⁸ References to “Member States” should be understood as references to “EEA Member States”.

「加盟国」への言及は、「EEA加盟国」への言及として理解されるべきである。

transfers. In case you do not, you must notify your competent SA⁹.

あなたは、データ輸入者に問い合わせ、その国の法律を確認し、評価のために協力することができる。あなた又は第三国のデータ輸入者が、SCC又はBCRに基づいて移転されたデータがEEA域内で保証された保護水準と実質的に同等の保護水準を与えられていないと判断した場合には、直ちに移転を停止すべきである。停止しない場合には、管轄する当局に通知しなければならない。

- 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.

裁判所によって強調されているように、移転先の第三国の法律の下でデータ輸入者が標準データ保護条項やBCRを遵守できるか、当該第三国に個人データを移転する前に自ら評価することがデータ輸出者とデータ輸入者の主要な責務である。もっとも、GDPRの法的な強制や第三国への移転に関する更なる決定を行う際には、当局も重要な役割を果たすことになる。

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.

裁判所に求められたように、区々な決定となることを回避するために、当局はEDPB内で更なる作業を行い、一貫性を確保する。このことは特に第三国への移転を禁止する必要がある場合にあってはまる。

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

第三国にデータを移転するためにSCCやBCRを利用している場合、どのような補完的措置を講じることができますか。

- 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.

必要な場合に講じる可能性のある補完的措置は、当該措置が十分な水準の保護を保障するか確認するために、移転の全ての状況を考慮に入れ、かつ、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る。

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.

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、データ輸出者及びデータ輸入者の主要な責務であることを強調した。

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.

EDPBは、現在、SCCやBCRが単独では十分な水準の保証を提供しない第三国にデータを移転するために、法的、技術的、組織的の何れの措置にかかわらず、SCCやBCRに加え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る。

⁹ 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).

特に、本判決の前文 145 参照。SCC に関しては、委員会決定 2010/87/EU の 4(g)項、委員会決定 2001/497/EC の 5(a)項及び委員会決定 2004/915/EC の別紙セット II(c)項を参照のこと。BCR に関しては、WP256 rev.01(EDPB により承認)の 6.3 項及び WP257 rev.01(EDPB により承認)の 6.3 項を参照のこと。

→ The EDPB is looking further into what these supplementary measures could consist of and will provide more guidance.
EDPBは、何がこれらの補完的措置を構成する可能性があるか更に調査を行い、更なる指針を提供するつもりである。

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?

私は、自身が管理者として責任を有するデータを処理する処理者を利用していますが、この処理者が米国又は他の第三国にデータを移転しているか、どのようにして知ることができるのでしょうか。

→ 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).

GDPR28条3項に従って処理者と締結した契約書には、移転が承認されているか否かを規定しなければならない(例えば、管理目的のために第三国からのデータへのアクセスを提供するだけでも移転に相当することに留意すべきである)。

→ 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).

また、処理者に関しては、復処理者に第三国にデータを移転することを委託する権限も与えられなければならない。多種多様なコンピューティングソリューションは、個人データの第三国への移転(例えば、保管又は保守の目的)を意味する可能性があるため、注意を払う必要がある。

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?

GDPR28条3項に従って締結された契約において、データが米国又は他の第三国に移転する可能性が示されている場合、処理者のサービスを利用し続けるために何ができますか。

→ 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.

あなたのデータが米国に移転される可能性があり、かつ、移転ツールによって提供されるEEAに与えられる実質的に同等の保護水準に米国法が影響を及ぼさないようにするための補完的措置が提供されない場合、又はGDPR49条の特例(derogation)が適用されない場合、唯一の解決策は、米国へのデータの移転を禁止するために契約の修正又は補完的条項を求めて交渉することである。データは、米国以外の場所で保存し、管理する必要がある。

→ 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.

あなたのデータが他の第三国に移転される可能性がある場合には、当該第三国の法律を検証し、それが裁判所の要求事項、及び期待される個人データの保護水準に適合しているかを確認する必要がある。第三国への移転のための適切な根拠を見い出せない場合には、個人データはEEA域外に移転されてはならず、全ての処理活動はEEA域内で行われるべきである。

For the European Data Protection Board

欧州データ保護評議会

The Chair

議長

Andrea Jelinek

アンドレア・ジェリネック