JCC・JETRO・S&K Brussels法律事務所 共催ウェビナー
GDPR実務アップデート

S&K Brussels法律事務所 弁護士 杉本 武重 SUGIMOTO Takeshige

7月13日(火)に開催いたしました、JCC・JETRO・S&K Brussels法律事務所共催のGDPR実務アップデートウェビナーの要約をご報告いたします。当ウェビナーは前半・後半の二部構成にて開催されました。

第１部：GDPR適用開始後3年間の欧州のデータ保護監督当局の調査と制裁金決定の要点
S&K Brussels法律事務所　弁護士　川島 章裕

第２部：欧州委員会の新しい標準契約条項（SCC）の発効により必須となる追加的なGDPR対応の実務
S&K Brussels法律事務所　弁護士　杉本 武重

第１部：GDPR適用開始後3年間の欧州のデータ保護監督当局の調査と制裁金決定の要点について

GDPR違反に対する制裁金の上限額には、①2,000万ユーロ以下又は事業者である場合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（83条5項）、②1,000万ユーロ以下又は事業者である場合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（83条4項）と、2つのレベルが定められています。

事業者が遵守しなければならないGDPRの規制を分類すると、以下の①および②の通りとなります。

GDPR上の諸義務①：違反の場合の制裁金の額2,000万ユーロ以下、又は事業者である場合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
1. データ処理に関する原則を遵守しなかった場合（5条）
2. 適法に個人データを処理しなかった場合（6条）
3. 同意の要件を遵守しなかった場合（7条）
4. 特別カテゴリの個人データ処理の条件を遵守しなかった場合（9条）
5. 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（12-22条）
6. 情報通知義務を履行しなかった場合（13、14条）
7. 個人データの移転の条件に従わなかった場合（44-49条）
8. 9章の下で採択された加盟国法に基づく義務に違反した場合
9. 監督当局の命令に従わなかった場合（58条1項、2項）
GDPR上の諸義務②：違反の場合の制裁金の額1,000万ユーロ以下、又は事業者である場合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
10. 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、子どもの保護責任者による同意又は許可を取得しない場合（8条）
11. 適切な技術的・組織的な対策を実施しない処理者を利用した場合（25条、28条）
12. 設計によるデータ保護・デフォルトとしてのデータ保護を確保するために適切な技術的措置及び組織的措置を実装しなかった場合（25条）
13. 義務があるのにEU代理人を選任しない場合（27条）
14. 責任に基づいて処理行為の記録を保持しない場合（30条）
15. 監督当局に協力しない場合（31条）
16. 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（32条）
17. データ侵害通知義務があるのに監督当局に通知せず、又はデータ主体に通知しなかった場合（33条、34条）
18. 義務があるのにデータ保護影響評価を行わなかった場合（35条）
19. 影響評価において緩和できないリスクがあったのに当局に事前相談しなかった場合（36条）
20. データ保護責任者を選任せず、又はその職や役務を尊重しなかった場合（37条から39条）

EUレベルのデータ保護監督当局である欧州データ保護会議（EDPB: European Data Protection Board）は、GDPRの制裁金決定の数について、2018年5月25日から2019年11月30日までに、22のEU/EEAの監督当局が785の制裁金決定を下したと2020年2月18日付け文書で公表しています。

またウェビナー前半では、GDPR制裁金ランキングの上位にある制裁金決定の実例を含め、上記1から20のGDPR上の諸義務の類型の中で代表的なGDPRの執行実例について、その実例の概要と当該実例を踏まえた実務上の対応のポイントについて解説を行いました。

2018年5月のEUのGDPRの適用開始を契機として、データ保護に関する個人の権利意識の向上とともに、EUを中心とするデータ保護監督当局によるデータ保護法違反の摘発と制裁は世界的に強化の流れを辿っています。最近でも、2021年6月10日、欧州のルクセンブルグのデータ保護監督当局がAmazon.com Inc.に対し、同社によるGDPR違反に関して4億2,500万ドル（約459億円）以上の制裁金を賦課する決定をEUの他のデータ保護監督当局に提案したと報道されていました。本ウェビナー開催直後である2021年7月15日には、2018年5月にフランスの市民的自由グループであるLa Quadrature du NetがAmazonに対して10,000名を代理して行った集団的苦情申立てに対して、ルクセンブルクのデータ保護監督当局が2021年7月15日に7億4600万ユーロ（約971億円）の制裁金決定を下したことが明らかになりました。同当局は、La Quadrature du Netが主張した通り、Amazonが法的根拠なしに広告目的でデータ主体をターゲットにしており、したがってGDPRに違反していることを認め、Amazonのサービスを使用するためにデータ主体が締結した契約がデータ主体にターゲティングを受け入れることを強制するとしたAmazonの主張を排斥したようです。Amazonは、法的根拠に基づいてこの欠陥を修正するために、制裁金決定の発出日である2021年7月15日から6か月間の猶予が与えられており、ターゲティング広告を終了するか、ターゲティング広告を行うための自由な同意を取得するかのいずれかを求められています。この猶予期間を超えると、Amazonは1日あたり746,000ユーロの制裁金を支払う必要があるとのことです。ルクセンブルク以外の他のEU加盟国のデータ保護監督当局は、上記ルクセンブルクのデータ保護監督当局による制裁金決定に同意したとのことです。

オランダにおいては、制裁金決定の対象となった事案においては、他のEU加盟国と同様に、GDPR第5条（GDPRの基本原則）、第6条（処理の法的根拠）、第32条（セキュリティ対策）の違反行為が問題となったケースが多く見られます。オランダでは、これまで他のEU加盟国において見られるような高額な制裁金決定は、現時点までには下されていない状況と考えられます。

しかしながら、ルクセンブルグのデータ保護監督当局が2018年5月のAmazonに対して申し立てられた苦情について、2021年7月までおよそ3年以上の月日をかけて、7億4600万ユーロという巨額の制裁金決定を出すに至ったことを踏まえると、今後オランダにおいても、今まで以上に高額の制裁金決定が行われる可能性は大いにあるといえます。また欧州議会では、GDPRの執行権限をEEA加盟国の監督当局から欧州委員会に授権し、EU競争法と同様に中央集権化した強力なGDPR執行を目指すべきという意見も出てきているため、今後のGDPRの執行の動向には注視が必要と考えられます。

第２部：欧州委員会の新しい標準契約条項(SCC)の発効により必須となる追加的なGDPR対応の実務について

GDPR上は、EEA域外への個人データの移転は原則禁止とされており、移転のためには個別の例外の充足が必要です。EEA域外への個人データ移転が許される場合は以下の通りです。

EEA域外への個人データ移転が許される場合
1. 十分性認定による移転（45条）
✓ 日本は民間部門についてのみ十分性認定がなされている（個人情報保護法および十分性認定補完的ルールの適用対象となっている日本の個人情報取扱事業者への個人データの移転の場合のみ十分性認定への依拠が可能）
✓ 米国に関する十分性認定であるプライバシーシールドは、欧州連合司法裁判所のSchrems II先決決定により2020年7月16日より無効
2. SCC（標準契約条項）による移転（46条2項(c) (d)））
✓ 今まではGDPR以前に採択された旧SCCでの対応が許されていたが、新しい改定版SCCが採択され、旧SCCは2021年9月27日に廃止される。
✓ Schrems II先決決定を踏まえたデータ越境移転影響評価が必要
3. BCR（拘束的企業準則）による移転（46条2項(b)・47条）
4. 行動規範による移転（46条2項(e)）
5. 承認された認証メカニズムによる移転（46条2項(f)）
6. データ主体(Data Subject)による同意による移転（49条1項(a)）
7. 同意以外の特定の状況における例外（49条1項(b)～(g)）による移転

GDPRには「移転」の定義規定はありませんが、幅広く移転がカバーされます。データ主体からの直接取得は含まれませんが、欧州内のサーバ上で外国からデータにアクセスする行為やクラウドサーバ上でデータを保存する行為も移転に含まれます。例えば、オランダで事業を行っていて、オランダの拠点の従業員の個人データを、米国のクラウド事業者の提供するクラウド上に保管している場合にも、オランダから米国への個人データの「移転」が生じていますので、個人データの移転の内容を記載したデータ移転契約のひな型であるSCC（標準契約条項）を移転元と移転先との間で締結して遵守することにより、GDPRの移転規制に対応することが必要になります。

このEEA域外への個人データ移転規制をさらに強化したのが、2020年7月16日の欧州連合司法裁判所のSchrems II先決決定です。この先決決定の概要は以下の通りです。

2020年7月16日の欧州連合司法裁判所先決決定（Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems）（Schrems II先決決定）

- ✓ Privacy Shieldを無効と判断
  - ✓ EEA域内⇒米国への個人データの移転は、以前「セーフハーバー」により認められていたが、欧州連合司法裁判所（ECJ）により2016年に無効とされる。その後、「プライバシーシールド」によりEEA⇒米国の個人データ移転が認められていた。
  - ✓ 米国では外国情報監視法（FISA：Foreign Intelligence Surveillance Act）等による政府による個人データのアクセスが可能であり、EEA域内と比べてデータ保護に関する保護が劣る。これについて、データ主体に裁判で、政府に対して争う権利が付与されていないことを根拠にプライバシーシールドは無効と判断された。
- ✓ SCCによる移転の枠組自体は有効としたが、単にSCCを締結することでは足りないと判示
  - ✓ SCCにより与えられている保証が現実に遵守できるか判断するために、EU法で要求されているレベルの保護が第三国で尊重されているかを評価するのは、データの輸出者及び輸入者の責任である。もし、第三国での保護が不十分であれば、EEAでの保護と実質的に同等のレベルの保護を確保するための補完的措置を講じることができるか及び当該第三国の法律が、かかる補完的措置の有効性を阻害するような形で悪影響を与えるものではないかを評価すべきである
  - ✓ 必要な場合に講じる補完的措置は、全ての移転に関する状況を考慮に入れて、第三国の法制度の評価を行い、十分なレベルの保護が確保されているかを確認するために、ケースバイケースで講じられなければならない。
  - → データ輸出者は、データ移転に先立ち、データ移転影響評価（TIA：Transfer Impact Assessment）を行うことが必要であることが明確となった
- ✓ 第三国での保護が不十分という結論であれば、データ移転を停止又は終了すべき
- ✓ ガバメントアクセスがある国（米国以外にも、例えば中国、ロシア、インド、シンガポール等も想定）への移転には慎重な検討が必要

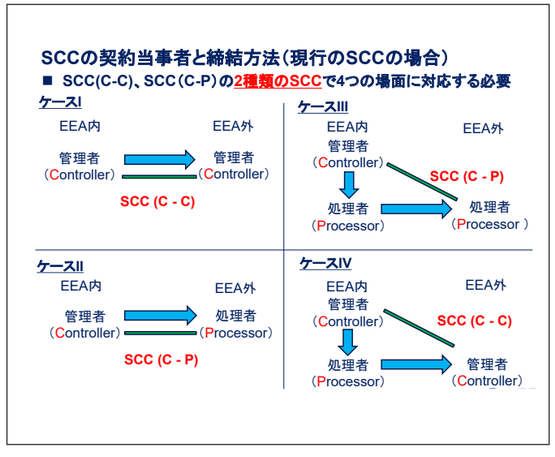
Schrems II先決決定を受けて、欧州のデータ保護監督当局は、EEA域外への個人データの移転規制への違反の執行を強化しました。以下の通り、2021年3月以降、毎月のように執行実例が報告されています。

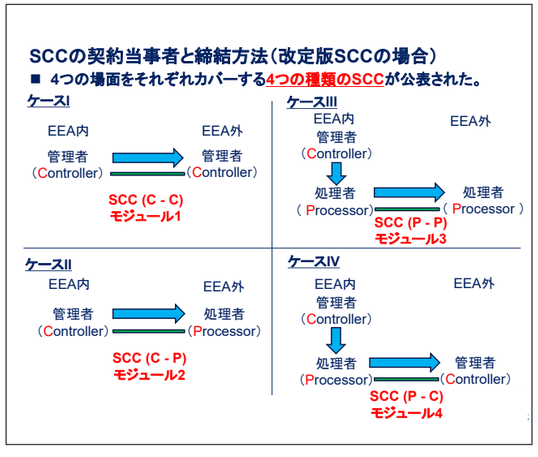
年月日	個人データのEEA域外移転規制を巡る執行動向
2021年3月15日	ドイツのバイエルン州のデータ保護監督当局が、ミュンヘンを本拠とする女性向け生活スタイル雑誌FOGSが、米国企業であるThe Rocket Science Group LLC(Rocket)が運営するメールマガジン管理サービスMailchimpを利用し、Rocketのある米国国内にドイツの居住者のメールアドレスをSCCに基づき移転させたことについて、GDPR違反を認定した。Schrems II先決決定によれば、米国に個人データを移転する場合、公的アクセス制度の運用の影響によりEU基準のデータ保護が侵害されるかどうかについて評価し、必要に応じて補完的措置をとらなければならないところ、FOGSおよびRocketは当該評価を行っていないと判断。FOGSがMailchimpの利用を直ちに中止したため正式処分なしで調査終了。
2021年4月28日	ポルトガルのデータ保護監督当局が、INE（NationalInstituteofStatistics）に対し、2021年の国勢調査の質問に関連する、米国またはデータ保護の十分性のない他の第三国に対する、全ての域外個人データ移転を12時間以内に停止するように命じる決定を出した。INEは、カリフォルニア州の企業であるCloudflare,Inc.に対し、国勢調査の質問の業務を、米国への個人データの移転を規定するデータ処理契約に基づいて委託していた。Cloudflareは国家安全保障の目的で米国監視法制の対象となり、Cloudflareが保持している個人データへの無制限のアクセスを米国当局に与える法的義務が課され、当該アクセスを与えた事実を顧客に知らせることもできない。

JCC・JETRO・S&K Brussels法律事務所共催ウェビナー　GDPR実務アップデート

2021年5月5日	ノルウェーのデータ保護監督当局（Datatilsynet）は、個人データの越境移転規制違反を含むGDPR違反に関して、FERDE ASに対して、500万NOK(ノルウェークローネ)（約6,500万円）の制裁金を科す事前の通知を発した。FERDE ASは、料金が引き落とされるチップが正しく登録されていない車やチップがない車が通過した場合、車のナンバープレートの写真撮影を行い、撮影された画像は自動光学式文字認識に送信されナンバープレートが読み取られる。自動で読み取りができる十分な画質が得られない場合、画像は手動処理に送られる。年間約1,000万枚の画像の自動処理と約2,500万枚の画像の手動処理が行われ、処理画像はナンバープレートを含む車の下部を捉えており、これに加えて、料金所の通過時間の情報と通過した数値コードがデータとして記録されていた。Unitel Bratseth Servicesは、中国にいる従業員にFERDE ASのウェブシステムのシステムを介して画像および関連情報にアクセスさせ手動処理をさせていた。FERDE ASは、ノルウェーから中国への個人データの移転に該当すると認識し、SCCに基づく適法な移転であると主張したが、ノルウェーのデータ保護監督当局は提出されたSCCに日付がなく、有効なSCCの存在を確認できなかった。
2021年5月27日	EDPS（欧州データ保護監察官）は、①EU機関によるアマゾン・ウェブ・サービス（AWS)とマイクロソフトのクラウドサービスの使用、および②欧州委員会によるマイクロソフトオフィス365の使用について、欧州連合司法裁判所のSchrems II先決決定の内容の遵守状況等を目的として調査を開始した。
2021年6月1日	ドイツの8のデータ保護監督当局は、ドイツ国内のデータ管理者に対する協調監査を行うことを公表。当該監査は、2020年7月に欧州連合司法裁判所が下したSchrems II先決決定の要件を執行することを目的とし、EUおよびEEA外への個人データの移転に適用される要件の遵守に焦点を当てたもの。調査対象となった企業には州当局から調査票が送られている。代表的な質問は以下の通り。 ■ 顧客への電子メール送信に委託先を用いているかどうか ■ ウェブサイトのホスティング先 ■ ウェブアクセス解析サービスの利用状況 ■ グループ企業間での顧客データ・従業員データの共有状況 ■ データ輸出者・データ輸入者の役割分担 ■ データ保管場所 ■ 処理される個人データのカテゴリおよび法的根拠 ■ 移転されるデータの保護措置、補完的措置の内容等

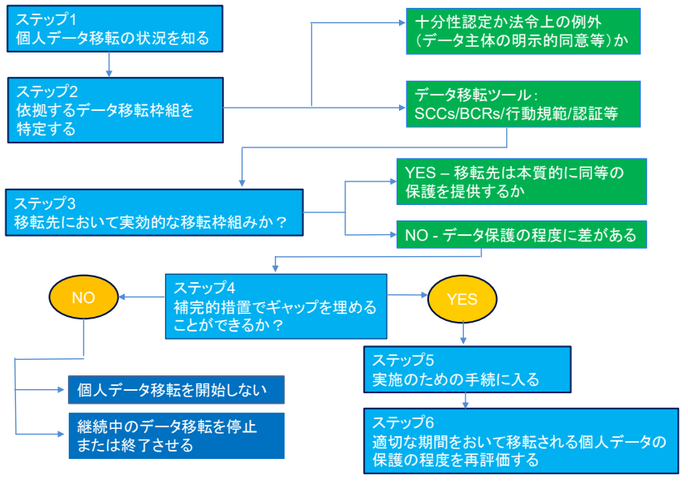
こうした執行強化の流れの中で、2021年6月4日、欧州委員会は、「第三国への個人データ移転のためのSCCに関する決定」を公表しました。当該SCC決定のAPPENDIXとしてSCCの改定版（「改定版SCC」）が添付されています。今までは管理者から管理者への移転について2種類のSCCが、管理者から処理者への移転について1種類のSCCがそれぞれありました。これに対し、改定版SCCでは、一般条項に加えて、具体的なデータ移転の状況に応じて、4つのモジュールの契約条項のうち該当するものを選択することが求められます。図にまとめると以下のようになります。





2021年6月18日、EDPBはEUと同等の個人データの保護水準を確保するためのデータ移転方法を補完する措置に関するレコメンデーションの最終版を採択しました。

ステップ	実施項目
ステップ１	個人データ移転の状況を知る
ステップ２	依拠するデータ移転枠組を特定する
ステップ３	依拠しているGDPR第46条のデータ移転枠組（BCR、SCC等）が当該移転の全ての状況に照らして実効的かどうかを評価する
ステップ４	（GDPR第46条の適切な保護措置のみでは実効性が確保されないことが判明した場合、）補完的措置を採用する
ステップ５	実効的な補完的措置を特定した場合、実施のための手続に入る
ステップ６	適切な期間をおいて再評価を行う



背景としては、Schrems II先決決定において、SCCに基づいてEUの十分性認定を受けていない国へ個人データを移転する場合であって、かつ、SCCの内容からだけでは、移転先国においてEUと同等の個人データ保護水準を保証できない場合には、補完的措置を講じて対応する必要があると示されたことから、本レコメンデーションが当該補完的措置の具体的内容を明らかにしました。EEA内にグループ会社を有する日本企業や、GDPRの域外適用を受ける日本企業や英国子会社は、改定版SCCの締結にあたって上の6つのステップに沿った検討が必要となります。

改定版SCCの実務対応において、重要なポイントは、EEA域内に所在する拠点・グループ会社が「移転」させる個人データについて、①十分性認定に基づくもの（移転先：日本、英国、韓国等）と、②改定版SCCを締結するものを仕分けすることです。ここで、移転先がGDPRの直接適用・域外適用を受けると評価される場合（GDPR第3条の地理的範囲に含まれる場合）は、そもそも、移転元→移転先への個人データの流れが「移転」ではなく「処理」となり、移転元において越境移転規制に対応する必要がないことに注意が必要です。GDPRの直接適用を受ける日本企業は、越境移転規制を含めGDPR対応が必要となり、日本から十分性認定のない第三国の第三者に当該個人データを移転させる場合、改定版SCCの締結等が必要となります。

日本企業がGDPRの直接適用・域外適用を受ける可能性があるケースの例

① 日本企業（EEA域内にグループ会社や支店等の拠点があるケース）が、EEA域内の取引先の従業員の個人データを直接取得して処理する場合（マーケティング目的での取引先情報の共有）
② 日本本社のプロジェクトとして、EEA域内の子会社等を含め、内部通報制度のホットラインやグローバルタレントマネジメントシステムを構築し、日本本社において直接にEEA域内の子会社等の従業員からの内部通報や人事データ等の個人データを処理する場合
③ 日本企業がウェブサイトを通じてEEA域内にいる者に対して商品を販売したりサービスを提供したりすることに際して個人データを処理する場合

また、上記①十分性認定に基づくもの（移転先：日本、英国、韓国等）の場合にも、移転先からの再移転を予定しているケースでは、欧州のデータ保護監督当局から「移転元（EEA内）から再移転先（十分性認定のない第三国）への移転であり改定版SCCの締結等が必要であった」と主張されるリスクがないかに注意が必要です。すなわち、上述のEDPBレコメンデーションのステップに従うと実行に手間がかかるEEA内→再移転先への移転を、十分性認定を受けた国の法的主体を形式的に経由させ、実行したという批判が当てはまらないように注意する必要があります。

JCC・JETRO・S&K Brussels法律事務所共催ウェビナー　GDPR実務アップデート

例えば、個人データの流れが、移転元（EEA内・管理者）→移転先（日本・処理者）→再移転先（中国・管理者）の場合などが考えられ、改定版SCCで対応する場合は、移転元と移転先の間、移転元と再移転先との間でそれぞれ改定版SCCの締結が必要と考えられます。

上記のような批判が妥当しかねないケースでは、移転元から移転先（十分性認定のある国）への移転は十分性認定に依拠し、移転先から再移転先への再移転は移転先国法に従うとともに、移転元と再移転先との間でも改定版SCCを締結することで対応することが現状では望ましいと考えられます。また、グループ内での個人データの移転については、②の改定版SCCを締結する方法で対応することの方が、日本本社からの再移転の問題や、移転後の個人データの管理が容易である場合もあり得るため、十分性認定を受けた国である日本等への移転についても改定版SCCでの対応を行うことが実務的により効率的な対応となる場合も考えられます。

以上のような様々なGDPR上のEEA域外への個人データ移転規制を踏まえると、オランダの日本企業においても、追加的なGDPRへの対応が必要となると考えられます。改定版SCC対応のアクションプランの一例としては以下のようなものが考えられます。

オランダの日本企業における改定版SCC対応のアクションプラン

フェーズ１－これまでの自社拠点のGDPRへの対応状況を整理し、既存のSCCまたは改定版SCC締結の対応を行う（2021年9月27日までを目途）

1.1 GDPR第30条の処理行為の記録（EEA内の拠点・グループ会社、GDPRの域外適用・直接適用を受ける日本本社・EEA外拠点）をアップデートする。
1.2 処理行為の記録の中で、EEA外への越境データ移転、EEA域内の外部ベンダーへの個人データ処理の委託が行われているものを特定する。
1.3 処理行為の記録の中で「移転」と整理されるものについて、既存のSCC締結等がなされているかをチェックし、既存のSCC締結等がなされていない場合、2021年9月27日までに既存のSCCを締結することを検討する。また、外部ベンダーへの個人データ処理の委託についてはデータ処理契約のSCCを締結する。

フェーズ２ － EDPBの補完的措置に関するレコメンデーションを踏まえた対応（2022年6月末を目途）

2.1 移転先が十分性認定を受けている国（日本、韓国、英国等）にある場合、十分性認定に基づくことを検討するが、移転先からの再移転がある場合、再移転の内容次第で移転元と再移転先との間での改定版SCC締結の要否を検討
✓ 既存のSCC締結で対応済みの「移転」について今後は十分性認定に基づいて行う場合、EEA域内の拠点において以下の対応を行う。
① プライバシーポリシー中および顧客・従業員・取引先担当者への情報通知中の移転の法的根拠への改訂および通知
② 処理行為の記録において十分性認定に基づくことの明記
③ 移転先の拠点での移転したEEA個人データの処理行為の記録の作成等
2.2 移転先が十分性認定を受けていない国にある場合、移転先との間で改定版SCCの締結を行う。また、その際に、データ越境移転影響評価（TIA）を実行する。

以上は当ウェビナーの要約となります。記述についてはウェビナー開催当時のものとなります。内容に関してご質問、ご不明な点等ございましたら、以下までお問い合わせください。

S&K Brussels法律事務所

弁護士 杉本 武重（SUGIMOTO Takeshige）
Tel:　+32 494 673351 (Belgium)　+81 3 6429 8040 (Japan)
Email: takeshige.sugimoto@sandkbrussels.com

弁護士 川島 章裕 (KAWASHIMA Akihiro)
Tel:　+32 2 550 3759 (Belgium)　+81 3 6429 8225 (Japan)
Email: akihiro.kawashima@sandkbrussels.com