Newsletter

ATSUMI & SAKAI
TOKYO | NEW YORK | LONDON | FRANKFURT
www.aplaw.jp

▶ About us

渥美坂井法律事務所・外国法共同事業は、国内系法律事務所として初めて、完全に独立した形で外国法共同事業を立ち上げた総合法律事務所です。ロンドン、ニューヨーク及びフランクフルトに拠点を有し、国際業務経験豊富な弁護士等が、欧米から中東・アフリカまで約120か国におよぶ広範な海外ネットワークを活用し、国際案件にも適時に対応可能な体制を整えております。提携グループを中心とした様々な内外のプロフェッショナルと協力し、時代とともに複雑化・国際化するニーズに柔軟に対応してシナジーを発揮し、真のワンストップリーガルソリューションを提供いたします。

改正個人情報保護法ニューズレター（2021 年 7 月版）

2021 年 7 月 A&S_013

はじめに

ご質問（動画のアメリカへの移転について）：

私はゲーム制作会社の法務部員をしています。弊社は、米国企業（カリフォルニア州）に出資し、その米国企業と業務委託契約を締結しております。

弊社では、お客さまに弊社製のカメラを自室のテレビに取り付け、また、コントローラーを自分の身体に取り付けてもらうことで、お客さまの動きに連動してキャラクターを動かすことのできる体感型ゲームソフトを販売しています。また、コロナ禍によるお客さまの運動不足を少しでも解消し、社会貢献度の高いゲームソフトを制作したいとの思いから、より忠実にお客さまの動きに連動するゲームソフトの開発にも取り組んでいます。そのため、弊社としては、お客さまのゲーム利用状況を把握したいと考えており、画面上でお客さまの同意を取得した上、ゲーム利用中のお客さまの様子（表情や姿勢等）を撮影し、米国の委託先企業と当該画像の分析を行い、新商品の開発を行うことを企画しております。

お客さま個人を特定できる動画を大量に取得することとなりますので、個人情報保護法に対応する必要があると考えています。特に米国企業と動画を共有する点を心配しており、どのような規制があるのか、アドバイスをお願いします。また、最近、サイバーセキュリティ―に関するニュースをよく見るようになりました。動画が漏えいした場合、どのように対応すればよいか教えてください。

回答項目：

1. 米国企業と動画を共有する場合の個人情報保護法による規制

（1）個人情報保護法 24 条 [1]

日本国外に個人データを移転する場合、個人情報保護法 24 条（外国にある第三者への提供の制限）の適用が問題となります。

本件のような製品開発の委託のために米国企業と動画を共有する場合、「①同意による方法」（個人情報保護法 24 条 1 項、2 項）、または、「②米国企業が基準適合体制を整備している企業であることを根拠とする方法」（同条 1 項、3 項）を検討する必要があります。[2]

---

[1] このニューズレターは、令和 2 年改正による条文番号を前提としており、令和 3 年改正による条文番号を前提としていません。令和 3 年改正による条文番号につきましては、以下のウェブサイトをご参照ください。
https://www.ppc.go.jp/files/pdf/seibihou_sinkyuutaisyouhyou_50jou.pdf （デジタル社会形成整備法第 50 条による個人情報保護法の改正）
https://www.ppc.go.jp/files/pdf/seibihou_sinkyuutaisyouhyou_51jou.pdf （デジタル社会形成整備法第 51 条による個人情報保護法の改正）

[2] 仮に個人データの移転が欧州への移転や個人情報保護法 23 条 1 項各号（法令に基づく場合等）に該当する場合、「①同意による方法」や「②米国企業が基準適合体制を整備している企業であることを根拠とする方法」を検討することは不要となります。設例は、そのような場合に該当しないため、①、②の方法を検討する必要があります。

(2) 個人情報保護法 24 条の改正に関する熊澤春陽元個人情報保護委員会委員のコメント

ア　個人情報保護法 24 条の改正の理由となった問題意識

グローバリゼーションの一層の進展により、個人情報が多様な形で国境を越える局面が増えると共に、個人が直面するリスクも多様化し高まってきています。近年、個人データ保護に関する法や制度が、政治体制等の異なる国にも広がったことにより、国家管理的な規制がみられるようになりましたが、改正前の個人情報保護法においては、提供先の国名やその国における個人情報保護制度等についての情報提供までは必要とされていませんでした。このことから、個人データの外国における取り扱いについて、データ主体に十分な情報が与えられていないという懸念の声が高まっていました。

また、日本企業の観点からは、国や地域の制度の変化や相違は流動的かつ多様であることから、海外の法制度を予見し難いため、意図しない個人の権利利益の侵害のリスクを生じさせています。このことから、日本企業にとっても意図しない個人の権利利益の侵害のリスクを避ける必要があります。

このような問題意識に基づき個人情報保護法 24 条が改正され、情報提供義務等が明記されました。

イ　EU 及び英国との相互認証と個人情報保護法 24 条の改正との関係

個人情報保護法 24 条の改正の際には、2019 年 1 月に施行された日 EU 間の越境データ移転ルールである、いわゆる補完的ルール（Supplementary Rules）[3] についても議論されました。

補完的ルールは、「個人情報取扱事業者は、EU 又は英国域内から十分性認定に基づき提供を受けた個人データを外国にある第三者へ提供するに当たっては、法第 24 条に従い・・・本人が同意に係る判断を行うために必要な移転先の状況についての情報を提供した上で、あらかじめ外国にある第三者への個人データの提供を認める旨の本人の同意を得ることとする」と定めています（補完的ルール p8）。この規定により、日本企業は、2019 年 1 月の時点で、EU 及び英国からの越境データを日本国外へ移転させる場合、外国法に関する情報提供が必要となりました。

これに対して、日本居住者の個人データを日本国外へ移転させる場合、外国法に関する情報提供義務は課せられませんでしたので、制度のバランスについて議論されました。この議論も経て、外国法に関する情報提供義務を日本居住者の個人データにも適用することとしたものが改正法 24 条となります。

ウ　越境データ移転について企業に望まれる対応

個人情報保護法では、過剰反応による個人データ利用の萎縮を避けるため、法令やガイドラインでの記述が抑制的であり、企業の負担に配慮したものとなっています。そのため、法令やガイドラインの表面上の文言を遵守するだけでは不足となる場合があり、法の趣旨を考慮しなければ適切に個人情報を取り扱っているとはいえないと判断されるおそれがあります。

特に個人データの越境移転は複雑であり、企業自らのポリシーに負うところが大きくなっています。企業としてはガイドラインに頼るだけでなく、自らのユーザー視点に立って、海外の法制等最新の情報を基に安全安心な取り扱いが担保されるよう、不断の見直しが必要となります。

(3) ①同意による方法（個人情報保護法 24 条 1 項、2 項）

本人から同意を得て個人データを日本国外へ移転させる場合、個人情報取扱事業者は、以下の情報を提供する必要があります（改正法 24 条 2 項、改正規則 11 条の 3 第 2 項、改正ガイドライン案（外国にある第三者への提供編）5-2）。

ア　外国の名称

(ア) 移転先の第三者が所在する外国の名称が示されていれば足り、必ずしも正式名称を求めるものではありませんが、本人が自己の個人データの移転先を合理的に認識できると考えられる名称でなければなりません。設例の場合、移転先は「アメリカ」と表記することで足りると思われます。

(イ) 外国の名称に加えて、当該第三者が所在する州等の名称を示すことまでは求められません。もっとも、個人データの越境移転に伴うリスクについて、本人の予測可能性を高めるという個人情報保護法 24 条の趣旨を踏まえると、例えば、州法が主要な規律となっている等、州法に関する情報提供が本人の予測可能性の向上に資する場合には、移転先の外国にある第三者が所在する州を示した上で、州単位での制度についても情報提供を行うことが望ましいとされています。

---

[3] EU 及び英国の GDPR 十分制認定と日本の個人情報保護法 24 条の国指定の相互認証の際に定められたものです。
https://www.ppc.go.jp/files/pdf/Supplementary_Rules.pdf

イ　外国の個人情報保護制度

ガイドライン案では、以下の 4 項目の情報を提供する必要があるとされています（改正ガイドライン案（外国にある第三者への提供編）5-2）。

(ア) 外国における個人情報保護制度の有無（個人情報保護法を制定していない国は少なくありません）

(イ) 外国の個人情報保護制度についての指標となり得る情報の存在（例えば、「GDPR に基づく十分性認定がされた国」、「APEC の CBPR システムの加盟国」）

(ウ) OECD プライバシーガイドライン 8 原則に対応する事業者の義務又は本人の権利の不存在（例えば、「あらかじめ利用目的の範囲内で利用しなければならないルールの不存在」、「開示請求が認められていない」。OECD プライバシーガイドライン 8 原則については、下記「(4)」をご確認ください。）

(エ) その他本人の権利利益に重大な影響を及ぼす可能性のある制度の存在（例えば、「外国政府による広範な情報収集が可能[4] 」、「外国国内のデータ保存義務」）

ウ　外国にある第三者が講ずる個人情報保護のための措置に関する情報

外国にある第三者が、OECDプライバシーガイドライン 8 原則に対応する措置を講じていない場合には、当該講じていない措置の内容について、情報提供しなければなりません（例えば、「利用目的の通知・公表を行っていない」）。

(4) OECD プライバシーガイドライン 8 原則

1980 年 9 月 23 日、経済協力開発機構（OECD）の理事会は「プライバシー保護と個人データの国際流通についてのガイドライン案に関する OECD 理事会勧告」を採択（2013 年に改正）しました。当該勧告の附属文書の中で、個人データの流通に関して、OECD 加盟国内における法整備の指針として規定された 8 原則を「OECD プライバシーガイドライン 8 原則」といいます。

日本の個人情報保護法についても、OECD プライバシーガイドライン 8 原則を法整備の指針としており、以下のとおり、当該 8 原則の内容に対応する形で規定が置かれています[5]。

OECD プライバシーガイドライン 8 原則	個人情報保護法の対応
収集制限の原則 (Collection Limitation Principle)	適正な取得（改正法 17 条）、取得に際しての利用目的の通知等（改正法 18 条）、第三者提供に係る記録の作成等（改正法 25 条）、第三者提供を受ける際の確認等（改正法 26 条）、個人関連情報の第三者提供の制限等（改正法 26 条の 2）
データ内容の原則 (Data Quality Principle)	データ内容の正確性の確保等（改正法 19 条）
目的明確化の原則 (Purpose Specification Principle)	利用目的の特定（改正法 15 条）
利用制限の原則 (Use Limitation Principle)	利用目的による制限（改正法 16 条）、不適正な利用の禁止（改正法 16 条の 2）、第三者提供の制限（改正法 23 条）
安全保護措置の原則 (Security Safeguards Principle)	安全管理措置（改正法 20 条）、従業者の監督（改正法 21 条）、委託先の監督（改正法 22 条）
公開の原則 (Openness Principle)	保有個人データに関する事項の公表等（改正法 27 条）
個人参加の原則 (Individual Participation Principle)	開示（改正法 28 条）、訂正等（改正法 29 条）、利用停止等（改正法 30 条）、理由の説明（改正法 31 条）、開示等の請求に応じる手続（改正法 32 条）、手数料（改正法 33 条）
責任の原則 (Accountability Principle)	個人情報取扱事業者による苦情の処理（改正法 35 条）

(5)「②米国企業が基準適合体制を整備している企業であることを根拠とする方法」（個人情報保護法 24 条 1 項、3 項）

ア　事業者が実施する必要がある措置

個人情報取扱事業者が、改正規則で定める基準に適合する体制を整備している移転先に個人データを移転する場合、本人から同意を取得する必要はありません。

---

[4] ガバメントアクセスに関する情報を意味します。2020 年 7 月 16 日の欧州司法裁判所による、いわゆる Schrems II 事件の判決（プライバシーシールドを無効とした判決）においても指摘されている通り、ガバメントアクセスは、個人情報保護の観点から問題視されています。

[5] 個人情報保護委員会による資料（https://www.ppc.go.jp/files/pdf/310118_siryou1-1_betten2.pdf）を参考に対応関係を整理しています。

しかし、個人情報取扱事業者は、国外へ個人データを提供した後も継続的に、以下の (i) 及び (ii) の措置を講ずる必要があることに注意する必要があります（改正規則 11 条の 4 第 1 項、改正ガイドライン案（外国にある第三者への提供編）6-1）。

(i)「移転先における個人データの取扱状況」及び「それに影響を及ぼしうる移転先の外国の制度の有無及び内容」を適切かつ合理的な方法により定期的に確認すること

- ✓「移転先における個人データの取扱状況」を確認とは、例えば、外国企業との間の契約を締結することにより、外国企業の基準適合体制を整備している場合、当該契約の履行状況を確認すること
- ✓「それに影響を及ぼしうる移転先の外国の制度」とは、例えば、政府による広範な情報収集が可能となる制度

(ii) 外国にある第三者による相当措置の実施に支障が生じたときは、必要かつ適切な措置を講ずるとともに、当該相当措置の継続的な実施の確保が困難となったときは、個人データの当該第三者への提供を停止すること

設例において、「②米国企業が基準適合体制を整備している企業であることを根拠とする方法」により個人データを移転させる場合、外国企業との関係で継続的な措置を講ずるために、米国企業との契約により個人データの取扱状況の確認について規定する必要があります。具体的な契約条項が存在しない場合、日本企業による個人データの取扱状況の確認を認める外国企業は多いとはいえないと思われます[6]（契約については、下記「3（2）」もご参照ください）。

改正前には「基準適合体制を整備している企業であることを根拠とする方法」は、「同意による方法」と比較すると、困難ではないと思われる場合もありました。しかし、改正により基準適合体制の継続的な確認が必要となりましたので、基準適合体制を整備している企業であることを根拠とする方法も容易ではない場合が増加すると思われます。

イ　情報提供

個人情報取扱事業者は、本人の求めがあった場合には、上記措置に関する情報を遅滞なく本人に提供する必要があります。

提供すべき情報として、改正規則では以下の情報が定められています（改正法 24 条 3 項、改正規則 11 条の 4 第 3 項、改正ガイドライン案（外国にある第三者への提供編）6-2-2 参照）。

① 移転先による改正法 24 条 1 項に規定する体制の整備の方法
移転先における基準適合体制を整備する「方法」について情報提供を行うことが求められています。例えば、移転先との契約締結により、当該移転先の基準適合体制を整備している場合、「移転先との契約」である旨の情報提供を行うこと。

② 移転先が実施する相当措置の概要
移転先における基準適合体制の「内容」について情報提供を行うことが求められています。例えば、移転先との契約締結により、当該移転先の基準適合体制を整備している場合、「契約において、特定した利用目的の範囲内で個人データを取り扱う旨、不適正利用の禁止、必要かつ適切な安全管理措置を講ずる旨、従業員に対する必要かつ適切な監督を行う旨、再委託の禁止、漏えい等が発生した場合には提供元が個人情報保護委員会への報告及び本人通知を行う旨、個人データの第三者提供の禁止等を定めている」旨の情報提供を行うこと。

③ 個人情報取扱事業者による、移転先における個人データの取扱状況及びそれに影響を及ぼしうる移転先の外国の制度の有無及び内容の確認の頻度及び方法
例えば、移転先における相当措置の実施状況についての確認の方法及び頻度として、「毎年、書面による報告を受ける形で確認している旨」の情報提供を行うこと、また、当該相当措置の実施に影響を及ぼすおそれのある制度の有無及びその内容の確認の方法及び頻度として、「毎年、我が国の行政機関等が公表している情報を確認している」旨の情報提供を行うこと。

④ 当該外国の名称

⑤ 移転先による相当措置の実施に影響を及ぼすおそれのある当該外国の制度の有無及びその概要
例えば、「事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度が存在する」旨、また、「事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義務に係る制度が存在する」旨の情報提供を行うこと。

---

[6] 個人情報保護法 24 条 3 項の規定は、令和 2 年改正法の施行日以後に同項に規定する外国にある第三者に個人データを提供した場合について適用されます（改正ガイドライン案（外国にある第三者への提供編）6）。この適用開始を考慮して、外国企業との契約内容を見直す必要があります。

⑥ 移転先による相当措置の実施に関する支障の有無及びその概要
例えば、「提供先が契約において特定された利用目的の範囲を超えて個人データの取扱いを行っていた」旨の情報提供を行うこと。

⑦ 上記支障に関して個人情報取扱事業者が講ずる措置の概要
個人データの移転先である外国にある第三者による相当措置の実施に支障が生じた場合において、当該支障の解消・改善のために提供元の個人情報取扱事業者が講ずる措置の概要について情報提供を行うことが求められています。例えば、「提供先が契約において特定された利用目的の範囲を超えて個人データの取扱いを行っていたため、速やかに当該取扱いを是正するように要請した」旨、また、「提供先が契約において特定された利用目的の範囲を超えて個人データの取扱いを行っていたため、速やかに当該取扱いを是正するように要請したものの、これが合理的期間内に是正されず、相当措置の継続的な実施の確保が困難であるため、個人データの提供を停止した」旨の情報提供を行うこと。

2. 動画が漏えいした場合の緊急対応

(1)「どのような漏えいの場合」に報告義務が生じるのか

改正法 22 条の 2 は、漏えい時の個人情報保護委員会への報告義務及び本人への通知義務を規定しました。この新しい規定に基づき以下の場合に報告義務が生じるとされています（改正規則 6 条の 2、改正ガイドライン案（通則編）3−5−3−1）。

① 要配慮個人情報が含まれる場合
事例 1：病院における患者の診療情報や調剤情報を含む個人データを記録した USB メモリーを紛失した場合
事例 2：従業員の健康診断等の結果を含む個人データが漏えいした場合

② 不正利用により財産的被害が生じるおそれがある場合
事例 1：EC サイトからクレジットカード番号を含む個人データが漏えいした場合
事例 2：送金や決済機能のあるウェブサービスのログイン ID とパスワードの組み合わせを含む個人データが漏えいした場合

③ 不正の目的をもって行われた（不正アクセス等故意による）おそれがある場合
事例 1：不正アクセスにより個人データが漏えいした場合
事例 2：ランサムウェア等により個人データが暗号化され、復元できなくなった場合
事例 3：個人データが記載又は記録された書類・媒体等が盗難された場合
事例 4：従業者が顧客の個人データを不正に持ち出して第三者に提供した場合

④ 対象となる個人データに係る本人が 1,000 人を超える場合
事例：システムの設定ミス等によりインターネット上で個人データの閲覧が可能な状態となり、当該個人データに係る本人の数が 1,000 人を超える場合

(2)「いつまでに」報告しなければならないか

改正規則 6 条の 3 は、報告義務の期限について、以下の通り定めています。

第 1 段階：速報⇒上記①〜④の事態を知った後、速やかに
第 2 段階：確報⇒当該漏えいの事態を知った日から 30 日（上記③の場合は 60 日）以内に

速報の目安については、「知った」時点から概ね 3 〜 5 日以内とされています（改正ガイドライン案（通則編）3−5−3−3）。

また、「知った」時点は、会社のいずれかの部署が当該事態を知った時点を基準とするとされています（改正ガイドライン案（通則編）3−5−3−3、3−5−3−4）。個人情報保護法のルールに必ずしも詳しくない部署の従業員が漏えいを把握して、報告義務の期限を徒過した場合、報告義務違反となります。この報告義務違反を防ぐために、全ての部署の従業員に対する研修・教育を徹底する必要があります。

(3) 漏えい時に必要な措置

改正ガイドライン案（通則編）3−5−2 によると、個人データを扱う事業者は、漏えい等が発覚した場合には、以下の 5 つに掲げる事項について必要な措置を講じなければならないとされています。

（1）事業者内部における報告及び被害の拡大防止
責任ある立場の者に直ちに報告するとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずる。

（2）事実関係の調査及び原因の究明
漏えい等事案の事実関係の調査及び原因の究明に必要な措置を講ずる。

（3）影響範囲の特定
上記（2）で把握した事実関係による影響範囲の特定のために必要な措置を講ずる。

（4）再発防止策の検討及び実施
上記（2）の結果を踏まえ、漏えい等事案の再発防止策の検討及び実施に必要な措置を講ずる。

（5）個人情報保護委員会への報告及び本人への通知

（4）委託と報告・通知の主体

報告義務及び通知義務を負う主体は、漏えい等が発生し、又は発生したおそれがある個人データを取り扱う個人情報取扱事業者です。個人データの取扱いを委託している場合においては、委託元と委託先の双方が個人データを取り扱っていることになるため、報告対象事態に該当する場合には、原則として委託元と委託先の双方が報告する義務を負うことになります。この場合、委託元及び委託先の連名で報告することができます（改正ガイドライン案（通則編）3－5－3－2）。

もっとも、委託先が、報告義務を負っている委託元に当該事態が発生したことを通知したときは、委託先は報告義務を免除されます（改正ガイドライン案（通則編）3－5－3－5）。また、個人データの取扱いを委託している場合において、委託先が、報告義務を負っている委託元に一定事項を通知したときは、委託先は報告義務を免除されるとともに、本人への通知義務も免除されます（改正ガイドライン案（通則編）3－5－4－1）。

（5）外国事業者への域外適用

改正法 75 条によると、個人情報取扱事業者等が、国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人情報等を、外国において取り扱う場合には、当該個人情報取扱事業者等は、個人情報保護法の適用を受けることになります。設例では、米国の委託先企業は、ゲームソフトの開発を行うためにお客さまの個人データを取得し、利用することになりますので、当該米国の委託先企業についても個人情報保護法上の義務を負うことになります（改正ガイドライン案（通則編）5－1参照）。

米国の委託先企業において、動画の漏えい等が発生し、又は発生したおそれがあり、それが報告対象事態に該当する場合には、当該米国の委託先企業も、当該事態が生じたことについて、個人情報保護委員会への報告及び本人への通知を行うか、当該事態が生じたことに加え、一定事項を委託元に通知する必要があります。

委託元である日本企業としては、米国企業において動画の漏えいが生じた場合であったとしても、報告義務及び通知義務を負うことに注意が必要です。このことから、下記「3（2）」で述べる通り、米国企業との契約が重要となります。

なお、カリフォルニア州にもデータ漏えいの場合の義務に関するルールが存在します。当該ルールを遵守するためには、カリフォルニア州の弁護士にアドバイスを求めることが必要となります。

3. プライバシーポリシーと契約

設例の場合、会社の対応としては、特にプライバシーポリシー及び外国会社との契約の準備が重要になると思われます。

（1）プライバシーポリシー：情報提供

事業者が個人情報を取得するにあたり、プライバシーポリシーを読んでいただいた上で同意を取得する方法が一般的に採られています。このプライバシーポリシーとは、「事業者の個人情報の取扱いと権利の行使方法について説明をした書面」であり、一般的には、プライバシーポリシーを示すことにより、事業者は情報提供を行います。

設例において、仮に「①同意による方法」を選択した場合、米国の個人情報に関する制度について情報提供する必要があります。この点、上述した通り、ガイドライン案によれば、州法の情報提供は不要とされています。ガイドライン案に基づく限り、カリフォルニア州法の情報提供は必要ない場合が多いと思われます。ただし、カリフォルニア州は実務上重要である CCPA を制定しています。移転させるデータの量や性質によっては、個人情報保護法 24 条の趣旨を踏まえ、州法に関する情報提供が本人の予測可能性の向上に資するとの判断から、カリフォルニア州法についても情報提供をすべき場合もあり得ます。

また、設例の場合、例えば、委託先に対して、子会社に相当する割合の出資をしている場合、「委託」（個人情報保護法 22 条、23 条 5 項 1 号）ではなく、「共同利用」（同項 3 号）として整理することを検討し、プライバシーポリシーに表記することを選択することも考えられます。「委託」の場合、個人情報保護法 22 条に基づく監督義務の履行が重要な課題となること、及び、いずれの方法によるにせよ、海外の会社のコントロールのためには契約が重要となることにご留意ください。

（2）外国会社との契約

日本の会社にとって個人情報保護法を遵守することは当然です。仮に個人データの委託先が日本の会社である場合、個人情報保護法に関して契約に具体的な規定を設けなかった場合でも、委託先に対して個人情報保護法を遵守するためとの説明をすれば委託先の協力を得ることができ、深刻な問題が生じない場合が多いかもしれません。

他方、外国の会社にとって日本の個人情報保護法を遵守することは当然ではありません。個人情報保護法の遵守の必要性や個人情報保護委員会の執行について説明したとしても、必ずしも十分な協力が得られるとは思えません。そこで、外国の会社に個人データを委託する場合、契約内容が重要となります。少なくとも以下の点に注意する必要があります。

- ✓ 個人情報が漏えいした場合の対応
- ✓ 日本の本人の権利行使があった場合の対応
- ✓ （基準適合体制を整備している企業であることを根拠とする方法による場合）継続的な確認のための協力
- ✓ 個人データの利用終了時の抹消

（3）外国会社との契約について、GDPR の観点からフランクフルト提携オフィスのコメント

Under the European General Data Protection Regulation (GDPR) there are two main scenarios when agreements regarding data protection matters have to be entered into with foreign companies (leaving aside the rather rare case of joined controller agreements). The first scenario is the transfer of personal data to a so called “third-country” second scenario is entering into data processing agreements with a foreign processor or a foreign controller (if you are the processor) in accordance with Article 28 GDPR.

According to Article 44 (1) of the GDPR

> *“Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.”* ,

Articles 45 through 47 GDPR describe three main possibilities for the transfer of personal data to a third country.

- Article 45: Transfers on the basis of an adequacy decision
- Article 46: Transfers subject to appropriate safeguards
- Article 47: Binding corporate rules

For various countries, including Japan, an adequacy decision exists which allows for the transfer of data between the EU and the relevant country without addition safeguards (regarding the transfer) – however, this does not mean that a transfer is always justified. There still needs to be a legitimate reason for the foreign recipient of the data and, if a processor controller relationship exists, a data processing agreement (DPA) complying with the conditions of Art. 28 GDPR.

If however no adequacy decision exists for the relevant non-EU country either binding corporate rules (BCR), in accordance with Article 47 can be agreed (which is mainly used within large world-wide corporations) or so called standard contractual clauses (SCCs) as published by the European Commission can be used and executed between the data exporter in the EU and the data importer outside the EU to enable companies to exchange personal data across continental borders in a legally secure manner.

This possibility is mentioned in Recital 109 (Standard Data Protection Clauses) to the GDPR;

> *“The possibility for the controller or processor to use standard data-protection clauses adopted by the Commission or by a supervisory authority should prevent controllers or processors neither from including the standard data-protection clauses in a wider contract, such as a contract between the processor and another processor, nor from adding other clauses or additional safeguards provided that they do not contradict, directly or indirectly, the standard contractual clauses adopted by the Commission or by a supervisory authority or prejudice the fundamental rights or freedoms of the data subjects. Controllers and processors should be encouraged to provide additional safeguards via contractual commitments that supplement standard protection clauses.”*

Numerous EU companies are currently use the SCC’s as published by the EU Commission's as the basis for exchanging data with group companies, business partners and service providers in third countries. The clauses in use to date well before the entry into force of the General Data Protection Regulation (GDPR) in May 2018. Therefore, over time, these “old” contractual clauses caused more and more uncertainties and issues as they were still based on the previous Data Protection Directive. Ultimately, the need for an update of the clauses finally became apparent with the decision of the European Court of Justice (ECJ) on July 16, 2020 in the “Schrems II” case (C-311/18). While the ECJ still found the standard contractual clauses to be a fundamentally sound basis for data transfers to “insecure” third countries, the reasoning of the decision revealed the weaknesses of the contractual framework.

Consequently, on June 4, 2021, the European Commission adopted a new set of contracts for the transfer of personal data to recipients in countries outside the EU[7]. With the new standard contractual clauses, the EU Commission is attempting to eliminate the shortcomings of the old contractual framework and to ensure legal certainty.

Also, under the new set of SCCs, the data protection obligations legally regulated for EU companies in the GDPR are transformed into contractual provisions and thus made binding for the "data importer" in the third country. Therefore, the data importer must in particular cooperate in establishing the transparency of data processing and guarantee the essential data protection rights of the data subjects. The details of the data transfer and the purposes pursued thereby, as well as the technical and organizational data protection measures to be implemented by the data importer, are to be described in an annex to the clauses. The requirements for the level of detail tend to be higher than under the previous legal situation.

The new standard contractual clauses are modular. They take a different form for each of the following situations:

(i) EU controller and third country controller.

(ii) EU controller and third-country processor – an additional data processing agreement is not required (Art. 28 (7) GDPR).

(iii) EU processor and third country sub-processor - the conclusion of an additional data processing agreement is also not required in this constellation.

(iv) EU processor and sub-processor in the third country – this SCC is entirely new and is intended to cover cases in which a company (as controller) from a third country engages a processor in the EU to process personal data that is not subject to the GDPR (e.g., data of US citizens).

As stated above, if a service provider (as processor) processes data on the instructions of a controller, this constitutes "processing"[8] within the meaning of the GDPR (Art. 4 No. 8 GDPR). In this case, a so-called data processing agreement must be concluded (Art. 28 (3) and (4) GDPR). However, the newly published standard contractual clauses now also comply with the requirements for a commissioned processing contract. This means that if a contract is concluded on the basis of the standard contractual clauses, then the conclusion of an additional order processing contract is no longer required (except in Module iv).

Under Article 28 GDPR, a data processing agreement (DPA) must always be concluded if personal data is processed by a service provider who is dependent on instructions. Typical cases of processors are payroll service providers, advertising or marketing agencies, cloud computing providers and web or e-mail hosting service providers.

The DPA regulates the rights and obligations of the controller and processor as well as any sub-processors to be used. The main purpose is to ensure that the processor processes the data entrusted to him only for the purposes for which the controller has collected the data. Above all, however, the processor as service provider is obligated to protect the personal data to an appropriate degree. To ensure this, the DPA grants the customer comprehensive control rights in this regard.

The minimum requirements of the DPA are set forth in Article 28 of the GDPR as listed below:

- Subject matter and duration of processing
- Type and purpose of processing
- Type of personal data, group of data subjects
- Scope of authority to issue instructions
- Duties and rights of the controller
- Obligations of the processor:
- Processing according to documented instructions (of the controller),
- Maintaining confidentiality or secrecy,
- Taking appropriate measures for its own security of processing,
- Lawful use of sub-processors,
- Assisting the controller in responding to requests from data subjects,
- Supporting the controller in complying with its obligations under Articles 32 to 36 GDPR,
- Taking appropriate measures for the security of processing (Art. 28 III 2 lit. f GDPR in conjunction with Art. 32 GDPR),
- Notification of personal data breaches to the supervisory authority (Art. 28 III 2 lit. f GDPR in conjunction with Art. 33 GDPR),
- Notification of the data subject of a personal data breach (Art. 28 III 2 lit. f GDPR in conjunction with Art. 34 GDPR),
- Carrying out a data protection impact assessment (Art. 28 III 2 lit. f DS-GVO in conjunction with Art. 35 GDPR),
- Consultation of the supervisory authority in the case of high-risk processing (Art. 28 III 2 lit. f GDPR in conjunction with Art. 36 GDPR).
- Deletion or return of the personal data after termination of the contract,
- Provision of information and enabling of reviews.

---

[7] EUR-Lex - 32021D0914 - EN - EUR-Lex (europa.eu) (https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?locale=en)

[8] Article 4 No. 8 GDPR stipulates, that: 'processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Also, an important part of the DPA is an annex containing the technical and organizational measures (TOMs) with which the processor guarantees data protection and data security of the data provided to him.

4. 補足①：要配慮個人情報の取得

このニューズレターにおいては、動画が「個人データ」（個人情報保護法 2 条 6 項）に該当することを前提として説明しました。動画が個人データに該当する場合、安全管理措置構築義務（個人情報保護法 20 条）や第三者提供にあたっての同意取得義務（同法 23 条 1 項）等の規定を遵守する必要があります。

他方、実務的には、動画が「要配慮個人情報」（個人情報保護法 2 条 3 項）に該当するかどうかについて、検討しておく必要があります。仮に動画が「要配慮個人情報」に該当する場合、事前の同意が必要となり（個人情報保護法 17 条 2 項）、動画が漏えいした場合に報告義務が生じ、実質的な被害も大きくなります。

「要配慮個人情報」とは、個人情報の中でも「本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するもの」をいいます（個人情報保護法 2 条 7 項）。

設例の場合、人種、信条、病歴を認識し得る動画も取得するものと思われます。したがって、事前の同意や漏えいを防ぐための慎重な安全管理が必要となります。

5. 補足②：商業目的のカメラと防犯カメラの違い

設例のような商業目的のカメラの場合、個人情報の利用目的をできる限り特定し、あらかじめ公表するか、又は個人情報の取得後速やかに本人に通知若しくは公表するとともに、当該利用目的の範囲内でカメラ画像や顔認証データを利用しなければなりません（委員会 QA1-12）。

他方、防犯カメラにより、防犯目的のみのために撮影する場合、「取得の状況からみて利用目的が明らか」（個人情報保護法 18 条 4 項 4 号）であることから、利用目的の通知・公表は不要と解されます（委員会 QA1-11）。[9]

---

[9] なお、防犯カメラが作動中であることを掲示することが望ましく、問い合わせ先等について店舗の入り口や設置場所に明示するか、ウェブサイトの URL 等を示すことが考えられるとされています（委員会 QA1-11）

6. 改正法の公布から施行までのスケジュールの確認

令和 2 年 6 月 12 日	令和 2 年改正法公布
令和 3 年 3 月 24 日	政令・規則公布
令和 3 年 5 月 19 日	令和 3 年改正法（デジタル社会の形成を図るための関係法律の整備に関する法律）公布
令和 3 年 5 月 19 日	改正ガイドライン案公表
令和 3 年夏～秋頃	ガイドラインや Q&A を公表
令和 4 年 4 月 1 日	令和 2 年改正法施行

7. 今後の連載予定について

今後、「位置情報のビジネス的な利用」、「医療製薬ヘルスケア分野」、「金融分野」、「内部統制とデータ」、「中国法」、「韓国法」、「ベトナム法」、「台湾法」をテーマとするニューズレターを連載する予定です。

Author(s) / Contacts

渥美坂井法律事務所・外国法共同事業

〒100-0011 東京都千代田区内幸町2-2-2富国生命ビル (総合受付: 16階)

弁護士 松岡 史朗
パートナー / 第一東京弁護士会
E: fumiaki.matsuoka@aplaw.jp
> View Profile

熊澤 春陽*
顧問
* 弁護士資格はない（法律事務の取扱い・周施はしていない）
> View Profile

弁護士 平岡 亜紀子
アソシエイト / 第一東京弁護士会
E: akiko.hiraoka@aplaw.jp
> View Profile

弁護士 鈴木 陽一
アソシエイト / 東京弁護士会
E: yoichi.suzuki@aplaw.jp
> View Profile

弁護士 福原 聡
アソシエイト / 第二東京弁護士会
E: satoshi.fukuhara@aplaw.jp
> View Profile

フランクフルト提携オフィス
(Atsumi Sakai Janssen Rechtsanwalts- und Steuerberatungsgesellschaft mbH**)

OpernTurm (13th Floor), Bockenheimer Landstraße 2-4, 60306
Frankfurt am Main, Germany

ドイツ連邦共和国弁護士*** フランク・ベッカー
パートナー
E: frank.becker@aplaw.de
> View Profile

** ドイツ連邦共和国における弁護士・税理士法人
*** 但し、日本における外国法事務弁護士の登録はない。

お問合せ先

渥美坂井法律事務所・外国法共同事業
E: info@aplaw.jp