JIPDECセミナー

令和2年改正
越境移転データの取扱いの実務

MOMO-O, MATSUO & NAMBA

2022年4月12日

桃尾・松尾・難波法律事務所　パートナー弁護士

松尾剛行

目次

1　はじめに

　個人情報保護法の令和2年改正は、国際関係についての規律を強化した。日本企業との関連性が低い域外適用に関する適用範囲以外にも、日本の個人情報取扱事業者との関係が深い規定が多い。とりわけ、個人データの外国第三者提供に関する規律、安全管理措置の一環としての自社の個人データを外国で取り扱う場合に係る外部環境の把握及び講じた安全管理措置の公表等に関する規律等が重要である。本セミナーでは、規制概要を説明した上で、各類型ごとの実務対応を説明したい。

2　規制の概要

（1）　個人データの外国第三者提供に関する規律の概要（続く）

平成27年改正により、外国にある第三者への個人データの提供（外国第三者提供）についての原則本人同意規制（旧24条）が入った。その後、令和2年改正に伴い、外国にある第三者への個人データの提供時における本人への情報提供の充実等の規制強化（新28条）が行われた。

2　規制の概要

（1）　個人データの外国第三者提供に関する規律の概要

すなわち、概ね以下の外国第三者提供の各類型ごとに各規制が入っている。

同意	同意取得時に①国名、②移転先の個人情報保護に関する制度、③移転先が講じる個人情報保護のための措置等の情報を提供する必要がある
相当措置 （委託・共同利用等）	相当措置の確保に加え、①移転先に対して適正扱い実施状況の定期的確認や問題が生じた場合の対応、及び、②本人の求めに応じて情報を提供する必要がある
EEA・英国	外国第三者提供対応という意味では特になし＊

なお、法令等やCBPR等の外国第三者提供類型もあるが、ここでは詳述しない。

＊但し、契約等で最低限の措置の確保を求めることが望ましい。また、第三者提供規制に服する。

2　規制の概要

（2）　外的環境の把握の概要

加えて、安全管理措置の一環としての自社の個人データを外国で取り扱う場合に係る外的環境の把握が必要である。

更に、講じた安全管理措置の公表等に関する規律等が追加されている。

2　規制の概要

（3）　越境移転規制を甘く見ると･･･

- 国内の委託先が無断で外国に再委託したことが発覚！（マイナンバー海外無断委託事件参照）
- 外国の委託先で漏洩が起こったが、状況が把握できていないので、本人から「どうなっているのか」とクレームを受ける
- クラウドサーバ設置先の外国の個人情報保護法制では日本と同等レベルが確保できない

等々のリスクがあり、重要な問題である。

３　個人データの外国第三者提供に関する規律対応の実務

（１）　外国第三者提供該当性

外国第三者提供規制を遵守する上では、自社がそもそも外国第三者提供を行っているか、外国第三者提供該当性が問題となる。外国にあるグループ会社等との個人データのやりとりは典型的な国第三者提供である。

外国クラウドサーバや（クラウドではない）外国サーバの利用については、個人情報取扱事業者との契約条項によって当該提供事業者がそのサーバに保存された当該個人データを取り扱わない旨が定められている場合で、かつ、適切にアクセス制御を行っている場合には、外国第三者提供にはならないものの、次の外国における個人データの取り扱いの問題がなお残る（Q&A12-3、12-4、Q&A7-53）。

3　個人データの外国第三者提供に関する規律対応の実務

（2）　どのスキームで外国に提供するのか

上記の通り

- 同意
- 相当措置
- EEA・英国

等のいずれかのスキームを利用する必要がある。

3　個人データの外国第三者提供に関する規律対応の実務

（3）　それぞれのスキームごとの要件を満たすかその1―同意

同意スキームを利用するのであれば、本人からの同意取得時に以下の情報を本人が確実に認識できると考えられる適切な方法で提供しなければならない（新第28条第2項、規則第 17 条）。

提供先の第三者の所在国の名称

適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報

当該第三者が講ずる個人情報の保護のための措置に関する情報

3　個人データの外国第三者提供に関する規律対応の実務

（4）　それぞれのスキームごとの要件を満たすかその2―相当措置

旧法から存在した相当措置の確保に加え、以下の対応が必要となる。

当該第三者による相当措置の実施状況並びに当該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

当該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

相当措置の継続的な実施を確保するために必要な措置に関する情報提供

4　外的環境把握の実務

（1）　外国における個人データの取り扱いの有無の確認（続く）

上記の検討の結果、外国第三者提供になる/ならないを問わず、外的環境把握規制対応として、自社が外国における個人データの取り扱いを行っているかを確認しなければならない。（典型的には委託＋相当措置の場合においては、外国第三者提供規制を受けるだけではなく、それに加えて、外的環境把握規制を受ける）。

4　外的環境把握の実務

（1）　外国における個人データの取り扱いの有無の確認

典型的には、

- 外国クラウドサーバを利用しているところ、個人情報取扱事業者との契約条項によって当該提供事業者がそのサーバに保存された当該個人データを取り扱わない旨が定められている場合で、かつ、適切にアクセス制御を行っている場合(Q&A10-25)
- 外国の（クラウド以外の）サーバを利用しているところ、個人情報取扱事業者との契約条項によって当該提供事業者がそのサーバに保存された当該個人データを取り扱わない旨が定められている場合で、かつ、適切にアクセス制御を行っている場合（Q&A12-3参照）
- 外国にある支店・営業所に個人データを取り扱わせる場合(Q&A10-23)
- 外国にある第三者に個人データの取り扱いを委託する場合(Q&A10-24)

等が挙げられる（なお、外国企業が個人情報保護法の域外適用を受ける場合において個人データを取り扱う場合にも問題となるが、本セミナーでは対象としない）。

４　外的環境把握の実務

（２）　外的環境の把握の実務その１（続く）

―個人情報取扱事業者が、外国にある支店・営業所に個人データを取り扱わせる場合

外国支店・営業所で個人データの取扱いをする企業は、外国において個人データを取り扱うこととなるため、支店等が所在する外国の個人情報の保護に関する制度等を把握したうえで、安全管理措置を講じる必要がある。これは、外国にある支店等や従業者が、日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合においても同様である（Q＆A10-23）。

4　外的環境把握の実務

（2）　外的環境の把握の実務その1（続く）

―個人情報取扱事業者が、外国にある支店・営業所に個人データを取り扱わせる場合

ここで、外国支店・営業所は、本社と法人格において同一であり、基本的には、本社の（日本の個人情報保護法に準拠した）社内ルールが適用されると思われる。そこで、少なくとも、適用法令上必ずしもOECDプライバシーガイドライン8原則のすべてが要請されていない場合であっても、日本の個人情報保護法に準拠した社内ルールの適用によりその「差分」を埋めているという説明ができることになるだろう。ただし、それだけでは必ずしもデータローカリゼーション規制やガバメントアクセス等について当然に対応できるわけではなく、このような規制が存在する国および地域については、別途現地法をベースにした内部規程による対応等、別の方法を考える必要があるだろう。

４　外的環境把握の実務

（２）　外的環境の把握の実務その１

―個人情報取扱事業者が、外国にある支店・営業所に個人データを取り扱わせる場合

加えて、Ｑ＆A10-23が越境テレワークを想定した記述を含んでいることも重要である。例えば、外国に居住してテレワークをしている従業者に個人データを取り扱う業務を担当させる場合には、当該従業者の所在する外国の制度等も把握して安全管理措置を講じる必要があるとされている。新型コロナウイルス感染症対策としてテレワークが急速に普及しており、従業員が事業者の取り扱う個人情報データベース等に通信回線を通じてアクセスする場面も増加している。その場合でも外国からの越境テレワークはまだ一般的ではないと思われるものの、外国からアクセスさせる場合には、外的環境把握規制がかかることに留意が必要である。

なお、金融機関等の場合には、別途金融機関に適用されるガイドライン等を参照されたい。

４　外的環境把握の実務

（３）　外的環境の把握の実務その２―委託の場合（続く）

委託や再委託（再々委託やそれ以降も含み、以下、そのような先を「（再）委託先」と総称する）のいずれかの過程で外国にある第三者が個人データの取扱いをする場合、委託元は、（再）委託先を通じて外国において個人データを取り扱うこととなるため、（再）委託先が所在する外国の個人情報の保護に関する制度等を把握したうえで、（再）委託先の監督その他の安全管理措置を講じる必要がある（Q＆A10-24）。

4　外的環境把握の実務

（3）　外的環境の把握の実務その2―委託の場合（続く）

外国の（再）委託先が日本国内に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合において外的環境把握規制がかかることは既にQ＆Aに明記されている（Q&A10-24）。しかし、日本の（再）委託先が外国に所在するサーバに保存されている個人データにアクセスして、これを取り扱う場合においてこの義務がかかるかは明確ではない。とはいえ、この場合でも、「（再）委託先を通じて外国において個人データを取り扱うこととなる」という点は、Q＆A10-25のクラウドと同様であり、保守的対応としてはこれに含めるべきだろう。

4　外的環境把握の実務

（3）　外的環境の把握の実務その2―委託の場合（続く）

法人/サーバ所在地	日本サーバ	外国サーバ
日本法人の（再）委託先	外的環境把握義務なし	明記なし（ただし、保守的対応としては外的環境把握を行うべき）
外国法人の（再）委託先	外的環境把握義務あり（Q＆A10-24で明記）	外的環境把握義務あり（典型例）

４　外的環境把握の実務

（３）　外的環境の把握の実務その２―委託の場合（続く）

外国にある第三者たる（再）委託先への委託の場合には、①個人データの外国第三者提供規制と、②外的環境把握規制の双方がかかると解されていることに留意されたい（Ｑ＆Ａ10-24）。そして、実務上は、①個人データの外国第三者提供規制への対応として、相当措置（新２８条１項）を継続的に講ずるための体制を整備するために、委託に関する個人データ取り扱いに係る覚書等が締結されていると思われる。

４　外的環境把握の実務

（３）　外的環境の把握の実務その２―委託の場合

この場合には、新28条１項による本人同意義務を免れることができ、本人の同意なく外国に所在する第三者への個人データの提供が可能となるが、それでもなお外的環境把握規制がかかることになる。覚書等により本人の権利利益を確保する措置を担保すること持って、個人データの安全管理のために必要かつ適切な措置とすることが多いと思われるが、これまでの委託に関する個人データ取扱いに係る覚書等において、外的環境把握規制への対応が不十分であれば、改正を機に覚書等の雛形を変更すべきであろう。

４　外的環境把握の実務

（４） 外的環境の把握の実務その３―クラウドその他外国サーバの場合（続く）

クラウドサービスの利用が委託になるかどうかは、個人情報取扱事業者との契約条項によって当該提供事業者がそのサーバに保存された当該個人データを取り扱わない旨が定められている場合で、かつ、適切にアクセス制御を行っている場合であるかの問題である(Q&A12-3、12-4、Q&A7-53）。

４　外的環境把握の実務

（４）　外的環境の把握の実務その３―クラウドその他外国サーバの場合（続く）

①外国にある第三者の提供するクラウドサービスを利用する場合（日本国内に所在するサーバに個人データが保存される場合も外的環境把握義務がかかる）で（委託にならない場合）か、または②（クラウドでなくとも）外国のサーバに個人データが保存される場合で（委託にならない場合）あれば、当該外国の個人情報の保護に関する制度等を把握したうえで、個人データの安全管理のために必要かつ適切な措置を講じることになる。

4　外的環境把握の実務

（4）　外的環境の把握の実務その3―クラウドその他外国サーバの場合

そして、クラウドの場合には、覚書等を締結することができないことも多いものの、クラウドベンダがホワイトペーパー等で基準・規格の準拠や認証取得、第三者監査等を謳っていることが多い。そこで、上記の「差分」がこのような内容によって担保されているかを確認するのが実務的であろう。

上記の確認の結果、自社が外国における個人データの取り扱いを行っているのであれば外的環境を把握しなければならない。

なお、サーバ所在国を日本とすることでは完全に義務を免れることはできないものの、相当リスクが軽減することから、実務上検討すべきである。

5　プライバシーポリシー上の規定方法（続く）

それでは、プライバシーポリシー上において、外的環境把握義務に関し、何を規定すべきか。新32条1項4号、施行令10条1号によれば、保有個人データの安全管理のために講じた措置を本人の知り得る状態に置く必要がある。そして（改正前の保有個人データに関する規律に従い）本人の知り得る状態に置く方法としてはプライバシーポリシーが利用されてきた。

5　プライバシーポリシー上の規定方法（続く）

外国の支店・営業所の場合、外国の制度等を把握して安全管理措置を講じる場合には、「保有個人データの安全管理のために講じた措置」として、支店等や従業者が所在する外国の名称を明らかにし、当該外国の制度等を把握したうえで講じた措置の内容を本人の知り得る状態に置く必要があるとされている（Q＆A10−23）。

5　プライバシーポリシー上の規定方法（続く）

委託の場合、「保有個人データの安全管理のために講じた措置」として、（再）委託先が所在する外国の名称を明らかにし、当該外国の制度等を把握したうえで講じた措置の内容を本人の知り得る状態に置く必要があるとされている（Q＆A10−24）。

5　プライバシーポリシー上の規定方法（続く）

クラウドの場合、「保有個人データの安全管理のために講じた措置」として、クラウドサービス提供事業者が所在する外国の名称および個人データが保存されるサーバが所在する外国の名称を明らかにし、当該外国の制度等を把握したうえで講じた措置の内容を本人の知り得る状態に置く必要があるところ、個人データが保存されるサーバが所在する国を特定できない場合には、サーバが所在する外国の名称に代えて、①サーバが所在する 国を特定できない旨およびその理由、および、②本人に参考となるべき情報を本人の知り得る状態に置く必要がある。②本人に参考となるべき情報としては、例えば、サーバが所在する外国の候補が具体的に定まっている場合における当該候補となる外国の名称等が考えられるとされている（Q＆A10−25）。

5　プライバシーポリシー上の規定方法

ここで、多数の個人情報を取り扱う企業では、多数の関係する外国での個人データの取扱いがあり取扱いをプライバシーポリシーにすべて記載する場合には非常に長くなってしまう可能性がある。そこで、講師らが関与する案件では、新32条1項柱書括弧書の「本人の求めに応じて遅滞なく回答する場合」を利用する方式、つまり、本人が求めた場合に、保有個人データを保有していることを確認した上で、遅滞なく回答する方式を採用するようアドバイスすることが多い（Q＆A9-3は、問合せに対して安全管理措置の具体的な内容を遅滞なく回答する体制を構築している場合には、「本人の知り得る状態」に置いたこととなるとしている）。

ご清聴ありがとうございました

ご質問は takayuki.matsuo@mmn-law.gr.jpへ

＊セミナーの質疑の範囲であれば無償で対応いたします。

このスライドは早稲田大学博士課程杜雪雯さんに多大な協力をいただいた。ここに感謝の意を表する。