

【講演レポート】JIPDECセミナー

当日いただいた主なご質問と回答

回答：牛島総合法律事務所

弁護士 影島 広泰氏

●外的環境の把握

【質問】

保有個人データに関する公表事項の追加で、外的環境の把握の一環で国名を特定する必要がありましたが、クラウドサービス等で国名がわからない場合はどうしたらよいですか？

【回答】

現時点では、プライバシーポリシー、保有個人データの公表に関して、国名がわからない場合の対応はガイドラインのパブコメ結果を見ないとわかりません。一方で、24条で外国移転に際して同意を求める時には国名を特定しなければならないとなっている点については、「特定できない…理由」を説明することが求められています。

【質問】

保管している国名を記載する必要があるのは、あくまでも日本で取得した個人データの話であり、米国展開するサービスに伴って取得した個人データを米国にあるサーバに保管している場合、保管している国名の記載は不要という理解でよいですか？

【回答】

日本の個人情報取扱事業者が取り扱う以上、米国で展開するサービスで取得したデータであっても、海外で保管している場合には、「外的環境の把握」として国名を公表する義務があると考えられます。

【質問】

外国の第三者に提供しない（アクセス権等で海外では触らせない）場合でも、個人データの海外にあるIS等に保管する場合は保管する海外の国名やその制度に応じた安全管理措置を記載しないといけないのでしょうか？

【回答】

「提供」しない場合には自社で保管している形になりますので、「外的環境の把握」として、国名等を公表する必要があると考えられます。

●委託と提供

【質問】

システム保守で触る可能性がある、と利用規約に書かれているクラウドは、提供にあたりますか。

【回答】

どのような場合に取り扱わないと言えるかは、ガイドラインのQ&Aに具体的な例が挙げられています。バックアップデータから復旧する場合等では、閲覧は可能でも取得できないように措置がされていれば、取り扱っていないとみなせるとなっています。要は、「盗めないようになっている」ことが重要なポイントになるということです。これは、技術的にということだけでなく運用全体でそのようになっているかどうかを判断することになります。

【質問】

委託と提供において、クレジットカード決済ベンダは情報を分けて管理も難しいと思われませんが、この場合委託になるのでしょうか

【回答】

具体的な事案によりますが、委託と構成することが難しいケースも多いのではないかと考えられます。

【質問】

クラウドベンダーが個人データを扱わないので提供に当たらない場合、それを明記する必要があると思いますか？利用目的に書かれていないことを以て、提供していないということになりますか？

【回答】

提供に当たらない場合、クラウドベンダーを利用していることを利用目的として特定する義務はないと考えられます。

なお、提供に当たるかどうかは、クラウドベンダー側における情報の取扱いの客観的な状態で判断することになりますので、利用目的に書かれていないからといって提供していないことにはならないと思われます。

●保有個人データ、開示、利用停止

【質問】

行政機関などに提出が必要な資料作成などのため、個人データを入手して資料を作成して数日間のみ保持する場合でも保有個人データとなりますか？

【回答】

なると考えられます（法2条7項・施行令4条の例外に該当する場合は別です）。

【質問】

顔や指紋の特徴のみを保存した照合用データも、ユーザから全部開示と請求が来たら開示対象となりますか。

【回答】

個人識別符号に該当する場合には、開示対象となり得ます。個人識別符号に該当しない場合には、単体での識別性と容易照合性を検討し、個人情報（保有個人データ）に該当するかを考えることとなります。

【質問】

仮名加工情報は、氏名、個人識別符号以外は削除不要となっていました。が、「ポイントカード番号」は削除不要ということでしょうか？

【回答】

削除不要と考えられます。

【質問】

個人情報消去の本人へのエビデンス提示についてですが、どのような提示が必要でしょうか。

【回答】

特別のルールはございませんので、消去を行った旨を通知（説明）すればよいと考えられます。

【質問】

「保有個人データが漏えい等するおそれがある」として本人から利用停止等の請求があった場合、当該理由による請求に応じない際には、理由としてなんらかの形で安全管理措置の充分性を示す義務が生じると考えるべきでしょうか。

【回答】

法30条7項（現行法では5項）は、「利用停止等を行わない旨を決定したとき…は、…その旨を通知しなければならない。」としているのみですので、理由を説明する義務は法的にはないものと存じます。なお、法27条1項4号及び施行令8条1号により「安全管理のために講じた措置」について「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない」ため、安全管理措置については、ガイドラインに例示されている粒度で、公表するかあるいは本人から求めがあれば回答しなければならないことになります。

●同意について

【質問】

改正法に合わせて、利用目的の書き方を含めて見直した個人情報保護方針や取り扱いについて、すでに同意取得済みの人に対して同意取り直しが必要でしょうか。

【回答】

利用目的の記載を詳細化して分かりやすくしただけであれば、通常、利用目的の変更（15条2項）には当たらず、同意は必要ないと思われます。これに対し、個人関連情報を取得して個人データとして取り扱うための同意を取得する必要がある場合や、これまで委託に伴う提供であると整理してきたものが第三者提供であると分かって同意を取得する必要があると判断した場合などには、同意を取り直す必要が出てくると考えられます。

【質問】

プライバシーポリシーが掲載されていて一括して「同意する」というボタンを押す形式・方法が一般的ですが、第三者提供先や共同利用先の安全管理措置を毎年監査するわけではない現状では、少なくとも第三者提供、共同利用については独立して同意取得すべきだと考えていますが、いかがでしょうか。

【回答】

ご指摘のとおり、プライバシーポリシーには同意の対象となるものと同意の対象とならないものが混在し、記載量も多くなっているのが一般的ですので、同意が必要なものについては独立して同意をとった方がより良いといえると資料いたします。

【質問】

物理的にデータを国外に出すことだけが越境ではなく、国内にあっても、国外からデータにアクセスする場合は、越境になると伺いましたが、こちらはガイドライン、またはQ&Aに記載がありますか？

【回答】

[通則ガイドライン2-13](#)に「個人データ等が、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データ等を利用できる状態にあれば（利用する権限が与えられていれば）、「提供」に当たる。」と記載されております。

●確認記録義務

【質問】

トレーサビリティ（資料32ページ）について、「名簿業者から個人データを購入するような場合を除いて、確認記録義務を果たす必要がないのが一般的」と書かれていますが、今回の法改正で、個人関連

情報の提供についても記録義務（提供元、提供先）が設けられます。名簿屋がからまなければ、確認記録義務は気にしなくてよいというわけでもないように思いますが、いかがでしょうか？

【回答】

資料の記載は、委託に伴う提供や共同利用、本人に代わっての提供など、様々な例外があることを記載したものであり、ご指摘のとおり、名簿屋がからまなければ確認記録義務は気にしなくてよいことではございません。確認記録義務の対象となるか否かは、法令及びガイドラインに照らして、厳密に判断する必要がございます。

●認定個人情報保護団体への報告**【質問】**

法改正によって、個人情報の漏えい等の事故が発生し、一定の基準に該当する場合は、個人情報保護委員会への報告が義務化されましたが、今まではPマーク取得事業者の場合、認定個人情報保護団体（例えばJIPDEさん）を通じて、委員会へ報告することができていました。今後法改正によって、この中継機能的なものはなくなるのでしょうか？（事業者が直接委員会へ報告する？）

【回答】

法令上の義務である個人情報保護委員会等への報告（法令上の義務の対象となる漏えい等事案4要件）は、全ての事業者様が個人情報保護委員会等へ、所定の様式に基づき報告することが必要となります。したがって、これまで実施していた認定団体を通じた中継機能的な役割はなくなります。

但し、報告が義務化される4要件以外については、[「個人情報の保護に関する法律についてのガイドライン（認定個人情報保護団体編）」](#)9ページにも記載の通り、自主的取り組みの一環として、「情報を受付けることの有効性や漏えい等報告の基準や報告方法といった内容について、個人情報保護指針（詳細は6（個人情報保護指針）参照）を含む自主ルールに盛り込むといった対応も望ましい」とされているため、個々の認定団体が改正法に向けた指針改定時に、新たな運用方針を示すものと思われます。