牛島総合法律事務所
個人情報/プライバシーニューズレター

クラウドサービスにおける個人情報の取り扱いについての行政指導と実務上の対応

2024 年 3 月 29 日

弁護士　中井　杏

＜目次＞

2024 年 3 月 25 日、個人情報保護委員会は、社会保険申請、給与計算及び人事労務管理等の業務に関するクラウドサービスを提供していた事業者に対し、行政指導を行ったことを公表（リンク）するとともに、「クラウドサービス提供事業者が個人情報保護法上の個人情報取扱事業者に該当する場合の留意点について（注意喚起）」（以下「本件注意喚起」といいます。）を公表しました。
クラウドサービスを利用して個人情報を取り扱う場合、個人情報の委託を行っているかどうかという点はたびたび議論になっていますが、これまで個人情報保護委員会はこの点についての具体的な判断を示してきませんでした。しかし、本件は、個人情報保護委員会が個別のクラウドサービスについて、個人情報を取り扱っているとの判断を公表した珍しい事案です。
本ニューズレターでは、本行政指導を踏まえたユーザー企業への影響について解説します。

1. クラウドサービスにおける個人情報の取り扱いについての問題の所在

個人データを第三者に提供する場合、原則として本人の同意を取得しなければなりませんが（個人情報保護法 27 条 1 項）、個人データの取扱いの委託に伴って個人データが提供される場合、提供先は「第三者」には当たらず、本人の同意は不要となります。ただし、委託先に対しては監督義務があり（同法 25 条）、委託先において漏えい等が発生した場合、委託元も漏えい等報告義務を負うこととなります（通則ガイドライン 3-5-3-2）。
「委託」とは、契約の形態・種類を問わず、個人情報取扱事業者が他の者に個人データの取扱いを行わせることをいうと解されています（通則ガイドライン 3-4-4）。すなわち、提供先において個人データを取り扱っていない場合には、個人データの取扱いを委託していることにはならず、クラウドサービスを利用して自社として個人情報を取り扱っているということになります。
次に、クラウドサービス事業者が個人データを取り扱わないことになっている場合とは、「①契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており、②適切にアクセス制御を行っている場合③等」が考えられると示されています（Q&A7-53）（丸数字は筆者による。）。

なお、保守サービスの提供を受けている場合は、「単純なハードウェア・ソフトウェア保守サービスのみを行う場合で、契約条項によって当該保守サービス事業者が個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等には、個人データの提供に該当しません」と解されており、例えば「保守サービスの作業中に個人データが閲覧可能となる場合であっても、個人データの取得（閲覧するにとどまらず、これを記録・印刷等すること等をいう。）を防止するための措置が講じられている場合」には、個人データの提供には該当しないとされています（Q&A7-55）。
このようにクラウドサービス事業者が個人データを取り扱っているか否かにより法律構成が変わるため、具体的にどのような場合に個人データを取り扱っていることになるのかについて、議論がなされていました。もっとも、後述 3 のとおり、国内のクラウドサービス事業者を利用している限りにおいて、ユーザー企業にとっては実務上の影響は大きくないと考えられます。
なお、個人情報保護委員会は、クラウドサービス事業者が個人データを取り扱っている場合で、当該クラウドサービス事業者への個人データの提供を委託として整理する場合には、ユーザー企業は監督義務等を適切に講じるよう指摘しているのであって（本件注意喚起 2）、クラウドサービス事業者が個人データを取り扱うこと自体について否定的な見解を持っているものではないと考えられます。

2. クラウドサービス事業者に対する行政指導

(1) 事案の概要

本件は、X 社が社会保険/人事労務業務支援システム（以下「本件システム」といいます。）のユーザーである社会保険労務士事務所等に対し、SaaS 環境においてサービス提供をしていたところ、X 社のサーバがランサムウェアによる攻撃を受け、漏えい等のおそれが発生したという事案です。
すなわち、クライアント企業が、社労士事務所に社会保険、人事労務業務等を委託し、社労士事務所が X 社のクラウドサービスを利用して、当該社会保険、人事労務業務等を行っていたという関係になります。
X 社の本件システムの利用実績は、社労士事務所 2754 事業所、管理事業所約 57 万事業所であり、本件システムで管理する本人は最大 2242 万人でした。このうち、個人情報保護委員会が受領した漏えい等報告の件数は、3067 件（本人数計 749 万 6080 人）と、極めて大規模な漏えい等事案となっています。

(2) クラウドサービス事業者が個人情報を取り扱っているとの判断について

本件において、X 社が個人データを取り扱っていたと判断された考慮要素は以下のア～ウです（本件注意喚起 1(2)）。

ア　利用規約

「利用規約において、クラウドサービス提供事業者が保守、運用上等必要であると判断した場合、データ等について、監視、分析、調査等必要な行為を行うことができること及びシステム上のデータについて、一定の場合を除き、許可なく使用し、又は第三者に開示してはならないこと等が規定され、クラウドサービス提供事業者が、特定の場合にクラウドサービス利用者の個人データを使用等できることとなっていたこと。」が考慮要素とされています。これは、Q&A7-53 の①「契約条項によって当該外部事業者がサーバに保存された個人データを取り扱わない旨が定められており」に関連する考慮要素だと考えられます。

イ　アクセス制御

「クラウドサービス提供事業者が保守用 ID を保有し、クラウドサービス利用者の個人データにアクセス可能な状態であり、取扱いを防止するための技術的なアクセス制御等の措置が講じられていなかったこと」が考慮要素とされています。これは、Q&A7-53 の②「適切にアクセス制御を行っている場合」に関連する考慮要素だと考えられます。
この点、上述のとおり「保守サービスの作業中に個人データが閲覧可能となる場合であっても、個人データの取得（閲覧するにとどまらず、これを記録・印刷等すること等をいう。）を防止するための措置が講じられている場合」には、個人データの提供には該当しないとされていますが（Q&A7-55）、本件では、X 社が保有する保守用 ID について、個人データの取得を防止するための技術的な措置が講じられていなかったことから、X 社は個人データを取り扱っていたと判断されています。すなわち、保守のために個人データを閲覧してしま

う場合、個人データを取り扱っていないといえるためには、現に当該個人データの記録や印刷をしていないというだけではなく、取得を防止するための措置まで講じているかまで考慮されています。

ウ　X 社による個人データの取扱いの状況

また、X 社は「クラウドサービス利用者と確認書を取り交わした上で、実際にクラウドサービス利用者の個人データを取り扱っていた」という点が考慮されています。

どのような態様で個人データを取り扱っていたかについては公表されていませんが、令和 5 年上半期において、個人情報授受確認書による X 社の個人データ取扱い実績は合計 20 件だったと認定されています。

エ　その他

本行政指導においては、X 社がユーザーに提供するサービスの性質についても検討されており、X 社がクラウドサービス上で提供するアプリケーションは、社労士事務所等が個人の氏名、生年月日、性別、住所及び電話番号などの個人データを記録して管理することが予定されているものであり、実際に大量の個人データが管理されていたことが指摘されています。

(3) 行政指導の理由

上記のとおり、X 社は個人情報を取り扱っていると判断されたうえで、パスワードルールが脆弱だったこと、管理者権限のパスワードが脆弱で類推可能だったことから、アクセス者の識別と認証に問題があったこと、ソフトウェアのセキュリティ更新が適切に行われておらず、深刻な脆弱性が残存されていただけでなく、ログの保管、管理及び監視が適切に実施されておらず、不正アクセスを迅速に検知するに至らなかったなどとして、技術的安全管理措置に不備があったことが指摘されています。

また、社労士や、そのクライアント企業は公表された行政指導の名宛人にはなっていないものの、個人データの取扱いの委託を行っていたとの認識が薄く、委託先の監督が結果的に不十分になっていた可能性があると指摘されています。

3. ユーザー企業への影響

(1) 国内事業者のクラウドサービスを利用する場合

国内事業者のクラウドサービスを利用することについては、本件による影響はほとんどないものと考えられます。

クラウドサービス事業者が個人情報を取り扱っていると整理した場合、ユーザー企業は委託先の監督義務（個人情報保護法 25 条）として、クラウドサービス事業者における個人情報の取り扱いについて監督しなければならないこととなります。

他方、クラウドサービス事業者が個人情報を取り扱っていないと整理した場合、クラウドサービス上で、ユーザー企業が自ら個人情報を取り扱っていることになり、自らに対する安全管理措置として、クラウドサービス事業者における安全管理措置の状況などを確認することとなります。

したがって、いずれにしても実務上はクラウドサービス事業者における個人情報の取り扱いないしは安全管理措置の状況を確認せざるを得ないこととなります。

また、漏えい等報告については、委託と整理した場合は委託元として漏えい等報告義務を負い、委託と整理しない場合、自らの個人情報の取扱いにおいて漏えい等が発生したとして、漏えい等報告義務を負うことになります。

したがって、国内のクラウドサービス事業者が個人データを取り扱っていないため個人データの取扱いの委託には当たらないと整理することには、ユーザー企業にとってのメリットがほとんどないと考えられます（この論点は、再委託以降に委託元の許諾が必要となるマイナンバー法においてのみ、重大な影響がある論点といえます。）。

むしろ、本行政指導のように、後々クラウドサービス事業者が個人情報を取り扱っていたと判断されるリスクがあることを踏まえれば、ユーザー企業においては、クラウドサービス事業者が個人情報を取り扱っており、個人データの取扱いの委託をしていると整理しておいた方が安全だとも考えられます。

(2) 外国事業者のクラウドサービスを利用する場合

外国事業者のクラウドサービスを利用する場合、当該外国事業者が個人データを取り扱うと判断される場合、外国にある第三者への提供に当たる可能性があり、その場合データ移転契約などを締結し基準適合体制を構築するか、本人の同意を取得するといった対応が必要となります（個人情報保護法 28 条）。

他方、当該クラウドサービス事業者では個人データを取り扱っていないと判断される場合、個人情報取扱事業者が自ら当該クラウドサービスにおいて個人情報を取り扱っていることとなりますので、安全管理措置として外的環境の把握を行い、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こととなります（同法 32 条 1 項 4 号、個人情報保護保施行令 10 条 1 号）。

そこで、例えば、以下の点を考慮し、当該クラウドサービス事業者が個人データを取り扱うことになるかを検討することが考えられます。

①クラウドサービスの契約、利用規約において、クラウドサービス事業者が個人データを取り扱う旨又は例外的な場合には取り扱うことができる旨が定められていないか。

②保守等により、例外的に個人データを閲覧することができる場合であっても、記録・印刷ができないようにするなど、クラウドサービス事業者において個人データを取得できないようにアクセス制御がなされているか。

また、当該クラウドサービス事業者と締結したデータ移転契約が、個人情報保護法が求める基準適合体制の構築に十分な内容であり、安全管理措置についての報告も受けられるような場合には、ユーザー企業としては、個人情報保護法 27 条 1 項 5 号に基づく委託と、同法 28 条の基準適合体制による個人データの提供と整理することも考えられます。

(3) 個人データの取扱いの委託と整理する場合の留意点

本件注意喚起 2 では、クラウドサービス事業者に個人データの取扱いを委託する場合の具体的な安全管理措置として以下の点に留意するよう指摘しています。

①サービスに付随するセキュリティ対策についても十分理解し、確認し、クラウドサービス提供事業者及びサービスを選択すること

②安全管理措置（個人データの取扱いに関する役割や責任の分担を含む）として合意した内容を規約や契約等でできるだけ客観的に明確化すること（Q&A5-8 参照）

③利用しているサービスに関し、セキュリティ対策を含めた安全管理措置の状況について、例えば、クラウドサービス提供事業者から定期的に報告を受ける等の方法により、確認すること

いずれも通則ガイドライン 3-4-4 で指摘された委託先に対する監督の内容ですので、既に対応されている場合もあり得ると思われますが、漏えい等が発生した場合、安全管理措置の不備があったことを理由に行政指導がなされることが多いことから、委託先に対する監督状況を改めて確認する必要があります。

以 上