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）

令和６年３月25日
個人情報保護委員会

今般、クラウドサービス提供事業者が提供する業務システムが不正アクセス被害を受け、クラウド環境で管理されていた多数の個人情報取扱事業者（以下「クラウドサービス利用者」という。）の顧客の従業員の個人データが暗号化され、漏えい等のおそれが生じた事案について、当委員会は、本件クラウドサービス提供事業者が、クラウドサービス利用者から個人データの取扱いの委託を受けて個人データを取り扱うものであり、個人情報の保護に関する法律（平成15年法律第57号。以下「法」という。）上の「個人情報取扱事業者」に該当すると判断しました。

当該事例も踏まえ、クラウドサービスの利用に当たっては、以下の点に留意していただくようお願いいたします。

１　クラウドサービスを利用して個人データを取り扱う場合の留意点

(1) 個人情報取扱事業者が、個人データを含む電子データを取り扱う情報システムに関して、クラウドサービス契約のように外部の事業者を活用する場合、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ずるために、クラウドサービスの利用が、個人データの取扱いの委託（法第27条第５項第１号）に該当するかどうかを判断する必要があります。

また、委託に該当する場合には、クラウドサービス利用者である個人情報取扱事業者は、委託先に対する必要かつ適切な監督を行わなければなりません（法第25条）。

(2)「個人情報の保護に関する法律についてのガイドライン」に関するＱ＆Ａ（以下「ガイドラインＱ＆Ａ」という。）の７－53により、委託（又は本人の同意が必要な第三者提供）に該当するかどうかは、クラウドサービス提供事業者において、個人データを取り扱うこととなっているのか又は取り扱わないこととなっているのかのいずれであるかが判断の基準となります。

当該クラウドサービス提供事業者が、「当該個人データを取り扱わないこととなっている場合」とは、契約条項によって当該クラウドサービス提供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、適切にアクセス制御を行っている場合等が考えられるとされています。

今回の事例において、クラウドサービス提供事業者が個人情報取扱事業者に該当すると判断された考慮要素は以下のとおりですので御留意ください(なお、以下における「クラウドサービス利用者」とは、冒頭に記載したとおり個人情報取扱事業者です。)。

○　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。

○　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。

○　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こと。

２　クラウドサービス利用者による、委託先（クラウドサービス提供事業者）の監督に関する留意点

個人情報の保護に関する法律についてのガイドライン（通則編）（以下「ガイドライン」という。）３－４－４において、個人情報取扱事業者は、個人データの取扱いを委託するに当たって、法第 23 条に基づき自らが講ずべき安全管理措置と同等の措置が委託先において講じられるよう監督を行うものとされています。

特に、個人情報取扱事業者が、クラウドサービス提供事業者に個人データの取扱いを委託する場合には、以下のような点について御留意ください。

- サービスの機能やサポート体制のみならず、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、確認した上で、クラウドサービス提供事業者及びサービスを選択してください。
- 個人データの取扱いに関する、必要かつ適切な安全管理措置（個人データの取扱いに関する役割や責任の分担を含みます。）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してください（ガイドラインＱ＆Ａ５－８参照)。
- 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、確認してください。

３　個人データの取扱いの委託先がクラウドサービスを利用している場合の留意点

例えば、従業者等の個人データを取り扱う個人情報取扱事業者が、個人データの取扱いを外部の事業者に委託している場合に、当該委託先事業者が、クラウドサービス提供事業者が提供するアプリケーションを利用して、委託された個人データを取り扱っているケースがあります。この場合、委託元である個人情報取扱事業者は、委託先事業者に対する監督の一内容として、当該クラウドサービスの安全性などを委託先事業者に確認することが考えられます。

ガイドラインでも、「委託元が委託先について『必要かつ適切な監督』を行っていない場合で、委託先が再委託をした際に、再委託先が不適切な取扱いを行ったときは、元の委託元による法違反と判断され得るので、再委託をする場合は注意を要する」ものとされています（ガイドライン３－４－４）。

委託元である個人情報取扱事業者においては、前記１のとおり、委託先事業者のクラウドサービスの利用によって、当該委託先事業者からクラウドサービス提供事業者に対する「再委託」となっている場合があることを念頭において、法第 23 条が求める個人データの安全管理のために必要かつ適切な措置及び法第 25 条が求める委託先に対する必要かつ適切な監督を行うよう留意してください。

以　上