Newsletter

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

改正個人情報保護法ニューズレター（2021 年 5 月版）

2021 年 5 月 A&S_012

はじめに

現在のデジタル化の飛躍的な進捗により、多くの企業は、日本在住者の個人情報をアメリカやアジアなど日本国外において保管・利用しています。他方、多くのサービス利用者は、そのサービスに関連して収集される個人情報が、日本国外において保管・利用されることを認識していません。また、サービスを提供する企業が外国の制度や海外事業者のデータの取扱状況を把握していないケースもあります。

このような状況下において個人の権利利益を保護するために、GDPR などの各国のプライバシー法制と同様に日本の個人情報保護法は、厳格化の方向にあります。厳格化されたプライバシー法制の下では、データの取扱いに関する企業の説明が不十分とされ、ひいては、そのサービス自体が容認されないものと評価される余地が大きくなっています。

以前と比べると、丁寧な説明が企業に求められており、日本国外にどのように個人情報を移転し、取扱っているかについて、適切に説明するためには、GDPR などの他国の法令を一定程度理解し、外国企業のデータの取扱状況を把握する必要があります。

これは、多くの日本の個人情報保護法の担当者が悩んでいる新しく難しい問題であり、この問題の解決のためには、個人情報保護委員会のガイドラインや執行の意味を理解し、海外企業とのコミュニケーションのために GDPR と個人情報保護法との異同を把握することが必要となります。単に個人情報保護法のみを解説したとしても上記の悩みを解決することは難しいため、今後連載するニューズレターにおいて、個人情報保護委員会の委員を務めた熊澤春陽元委員の見解、及びフランクフルト提携オフィスのコメントを組み合わせた形式で解説していく予定です。

ご質問：

私は、会社で個人情報保護法に関わる業務を担当しています。令和 2 年に個人情報保護法が改正されたので、一般的にどのような対応をどのようなスケジュールですべきか検討する必要があります。スケジュールと令和 2 年改正の内容について教えてください。

回答項目：

1. 令和 2 年改正個人情報保護法の公布から施行までのスケジュールの確認
2. 実務上重要な改正事項
3. 個人データの日本国外への移転
4. 個人関連情報
5. 個人データ漏えい時の義務（Data Breach）
6. 仮名加工情報
7. 今後の連載予定について

1. 令和2年改正個人情報保護法（以下「改正法」という。）の公布から施行までのスケジュールの確認

令和 2 年改正法の公布から施行までのスケジュールは、以下のとおりです。

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 12 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）成立[1]
令和 3 年夏～秋頃	個人情報保護委員会がガイドラインや Q&A を公表（5 月頃にパブコメ）
令和 4 年 4 月 1 日	令和 2 年改正法施行

---

[1] このニューズレターは、令和 3 年改正前の条文番号を前提としています。

実務的には、上記のガイドラインや Q&A が注目されており、多くの会社は来年（令和 4 年）4 月 1 日の施行日までには、対応を終えるものと思われます。

2. 実務上重要な改正事項

改正事項は多岐にわたりますが、よくご相談がある改正事項は、以下のとおりです（詳細は、下記の「3」以降において、説明します）。

（1）日本国外への個人データの移転に関する義務

企業が日本国外へ個人データを移転させる場合、改正法により、外国の個人情報の保護に関する制度などを説明することが必要となりました（改正法 24 条 2 項及び 3 項）。

（2）「個人関連情報」の新設

閲覧履歴、位置情報、Cookie など、それのみでは個人を識別することが難しい情報を利用したサービスに対応するために、改正法は「個人関連情報」という概念を導入し、一定の場合、同意を取得する義務を規定しました（改正法 26 条の 2）。

（3）個人データの漏えい時の義務

改正法は、個人データの漏えいの事案について、個人情報保護委員会への報告及び本人への通知の義務を規定しました（改正法 22 条の 2）。

多くの日本の会社は、改正前の状況でも、インシデントレポートや個人情報保護委員会への報告・本人への通知を定めた内部規程を有していると思われます。改正法の施行までに、ガイドラインなどを検討して、現在の内部規程や契約書を見直す必要があります。

（4）「仮名加工情報」の新設

改正法により、氏名などを削除した情報である「仮名加工情報」に関するルールが追加されました（改正法 2 条 9 項、同条 10 項、35 条の 2、35 条の 3）。「匿名加工情報」より企業が利用しやすい類型であり、「仮名加工情報」のみを取扱う場合、企業に課される義務が軽減されます。

仮名加工情報は、特に、顧客の分析や製薬医療関係情報の取扱いの際の利用が想定されています。

≪改正法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≫

① 個人情報保護法改正の背景

個人情報保護法は「個人情報の利活用と保護」を法の目的としています。これは「個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする」という意味です。

このような目的を有する個人情報保護法の基盤的精神は、「パーソナルデータの利活用と個人の権利利益の保護は相反せず、個人の権利利益の強固な保護が利活用の進展に資する」というものです。つまり、個人情報を保護しないまま利活用を行った場合、個人の権利利益は著しく侵害され、その企業のサービスは非難されることとなりますので、俯瞰的・中長期的観点からは、個人情報の利活用は著しく制限されることとなります。このことから、利活用のために、個人情報を保護する必要があります。このような個人情報保護法の基盤的精神は、GDPR と共通しています。

上記の「個人情報の利活用と保護」という法の目的を達成できるように、個人情報保護法の平成 27 年改正では、国境を越えた情報社会の急激な進展を前提とした「3 年ごと見直し規定」が盛り込まれました。

その見直しを独立行政法人である個人情報保護委員会が初めて担ったのが、令和 2 年の個人情報保護法改正です。

② 個人情報保護委員会の取組みと令和 2 年改正

平成 27 年改正以降の個人情報を取り巻く急激な動きの中で、様々な課題が浮き彫りになってきました。個人情報保護委員会は設立以来、政令、規則、ガイドラインの策定や各種の情報発信等により法制度の円滑な執行を図ると同時に、個人情報の漏えいや不正使用の監視監督事案、個人からの苦情等の斡旋等に一元的に取り組んできました。それにより蓄積した経験に加え、経済団体や消費者団体、学術者や法律家の有識者等、個人情報を取り巻く様々なステークホルダーの意見を傾聴しました。さらに、EU や米国との対話、OECD や APEC 等の国際的な枠組や各国のデータ保護機関との情報交換をいたしました。以上のような取組みを経て、個人情報を取り巻く現状を把握し、将来的な課題を集約し分析し、個人情報保護法改正に至りました。

上記のような取組みに基づき改正が行われましたので、令和 2 年改正は、個人情報保護委員会が直面してきた様々な課題とステークホルダーの声を集約した多面的な問題意識に基づいて、揺らいできた「個人情報の利活用と保護」のバランスを再調整する意味合いを有していると言えます。

③　企業の担当者の方へのメッセージ

個人情報保護法は厳格化の一方向に進んでいるように捉えられがちです。しかし、今回の法改正は、テクノロジーが進化しグローバル化が進展するデータ流通環境においても、企業が個人情報を適切に取り扱い、利活用する実務において陥りやすい落とし穴のようなビジネス分野・事象を規律し、企業の大切な経営資源である個人情報を透明性とアカウンタビリティに基づき扱い活用することを促すものです。

上述した通り、個人情報を保護しなければ、その企業のサービスは社会的非難を受けることとなり得ます。様々な企業の方から意見を拝聴した中では、自社のサービスが個人の権利利益を侵害しているのではないかという不安の声も多くありました。この法改正は、企業にとって自社の個人情報の取扱いを改めて見直し、自社を守るための重要な機会と捉えていただくようお願いいたします。

3. 個人データの日本国外への移転

(1) 個人データの日本国外への移転に関して新しいルールが設けられた理由・背景

個人情報保護法は、日本国外へ個人データを提供する場合、原則として本人の同意を得なければならないとしていますが、改正前は、当該外国の国名や当該外国における個人情報保護に関する制度についての情報提供までは必ずしも求められませんでした。

他方、近年、データ保護関連法制が世界に広がる中で、一部の国において国家管理的規制がみられるなど、個人データの越境移転に係るリスクが変化しつつあります。自らの個人データが外国においてどのように取り扱われているか十分に知らされていない点について、消費者の不安の意見がありました。

個人データの越境移転が広がる状況において、国や地域における制度の相違は、個人やデータを取り扱う事業者の予見可能性を不安定なものとし、個人の権利利益の保護の観点からの懸念も生じます。

このような観点から、今回の改正において、個人情報取扱事業者が日本国外へ個人データを移転できる場合を一定の場合に制限する改正法 24 条について、事業者の負担にも考慮しつつ、移転先の事業者やその事業者が置かれている外国の状況について、本人への情報提供を通じた必要最低限の留意を求めることとされました[2]。

(2) 個人データの日本国外への移転に関するルール

改正法 24 条 2 項及び 3 項は、個人データの日本国外への移転について、以下の通り、規定しています。

> 24 条 2 項：
> 個人情報取扱事業者は、前項の規定により本人の同意を得ようとする場合には、個人情報保護委員会規則で定めるところにより、あらかじめ、当該外国における個人情報の保護に関する制度、当該第三者が講ずる個人情報の保護のための措置その他当該本人に参考となるべき情報を当該本人に提供しなければならない。
>
> 24 条 3 項：
> 個人情報取扱事業者は、個人データを外国にある第三者（第 1 項に規定する体制を整備している者に限る。）に提供した場合には、個人情報保護委員会規則で定めるところにより、当該第三者による相当措置の継続的な実施を確保するために必要な措置を講ずるとともに、本人の求めに応じて当該必要な措置に関する情報を当該本人に提供しなければならない。

この新しい条文により示されている通り、個人データを日本国外へ移転させるときには、「同意を根拠とする場合」（以下の「ア」の場合）、個人情報保護法規則（以下「改正規則」という。）で定められる情報を提供する必要があります。また、「外国にある第三者が体制を整備している場合」（以下の「イ」の場合）、改正規則で定められる措置を講ずる必要があります。

ア　「同意を根拠とする場合」提供する必要がある情報（改正規則 11 条の 3 第 2 項）

> ①外国の名称
> ②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
> ③外国にある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

この情報提供義務に関しては、特に上記②について、企業がどのように外国の個人情報保護制度を把握するかが課題となります。

イ　「外国にある第三者が体制を整備している場合」必要な措置（改正規則 11 条の 4 第 1 項）

> ①提供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提供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
> ②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

---

[2] 佐脇紀代志「一問一答　令和 2 年改正個人情報保護法」（以下「一問一答」といいます。）p52 参照

この措置に関しては、特に海外の企業（提供先）の個人データの取扱状況をどのように継続的に確認するかが課題となります。

ウ　対応のポイント

①　個人データを日本国外へ移転しているかどうかの改めての事実確認

まず、自社が個人データを日本国外へ移転しているかどうかを確認する必要があります。日本国内のみでビジネスを行っている場合でも、海外の会社のサービスを利用して、個人データを日本国外へ移転させている場合がありますので注意が必要です。

②　プライバシーポリシーの改訂

同意を根拠として個人データを日本国外へ移転させている場合、プライバシーポリシーを改訂し、外国の名称や外国における個人情報の保護に関する制度を記載することを検討する必要があります。

③　外国企業との契約内容の確認

「外国にある第三者が一定の体制を整備している」企業に個人データを提供した場合、継続的に個人データの取扱状況を確認する必要があります。継続的に外国企業のデータの取扱状況を確認するため、当該外国企業との間の契約を検討する必要があります。

（3）よくあるご相談：サーバの所在する国と改正法 24 条との関係

サーバの所在する国と改正法 24 条の関係について、ご相談いただくことがあります。この点について、立法担当官は以下の通り整理しています（一問一答 p58）。

まず、クラウドサービス等のサーバの運営事業者が、当該サーバに保存された個人データを取り扱わないこととなっている場合には、外国にある第三者への提供（第 24 条）には該当しません。

仮に、サーバの運営事業者が「外国にある第三者」に該当する場合であっても、本人に提供すべき「外国の制度に関する情報」の外国とは、サーバの位置ではなく、当該運営事業者の法人格として登記された外国となります。

サーバが所在する国（あるいはサーバが所在する国の候補）が分かる場合には、本人への説明責任・透明性確保の観点から、当該国の制度に関する情報等についても、本人に情報提供することが望ましいものと考えられます。

サーバの運営事業者が複数あるなどして、具体的な所在国を特定できない場合には、可能性のある外国の制度に関する情報等を、本人に提供しなければなりません。

（4）個人データの国外移転に関する情報提供義務ついて、GDPR の観点からフランクフルト提携オフィスのコメント

GDPR also requires data controllers to provide data subjects with certain information about the transfer of their personal data outside the EEA. According to Article 13(1)(f) and 14(1)(f), GDPR, no matter if the transfer of data is justified by the data subjects' consent or by another lawful basis, the data subjects must be informed about the following factors:

- "the existence or absence of an adequacy decision by the Commission", i.e. whether the non-EEA recipient country is recognized by the EU Commission for having a data protection level adequate to that of the EU. So far, there have been 12 countries, including Japan, which have been granted an Adequacy Decision by the EU Commission (full list of countries[2] with Adequacy Decisions); and
- if the non-EEA recipient country does not have an adequate level of data protection, which safeguards allowed under GDPR the data controller is using in order to protect the transferred personal data. Among the others (e.g. binding corporate rules or codes of conduct), the most commonly used safeguard at the moment is the standard contractual clauses approved by the EU Commission; and
- the means by which the data subjects can obtain a copy of the safeguards used or where they have been made available.

The above-mentioned information should be provided to data subjects when their data is collected. When the data is not collected directly from the data subjects, the information must be given at the latest before the controller transfers the data.

4. 個人関連情報

（1）個人関連情報の概念が設けられた理由

近年、「個人情報」には該当しない利用者のインターネットの閲覧履歴などを収集し、その情報を第三者に提供し、第三者が他の情報と合わせて個人を識別できる情報（個人情報）として、その第三者のビジネスに利用することが行われています。これは利用者の観点からは、自分の興味・関心がある情報にアクセスすることが容易となるという側面もあり、また、現在では、世界的に普及しているビジネス形態といえます。

---

[3] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en

他方、本人の知らないところで、閲覧履歴などを、企業に把握され、利用された場合、その権利利益が大きく侵害される場合もあります。このような権利利益の侵害を防止するために、令和 2 年改正により「個人関連情報」という概念が導入され、「個人データの第三者提供」に準じる形の新しいルールが規定されました[4]。

(2) 個人関連情報とは

「個人関連情報」とは、「生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの」と定義されています（改正法 26 条の 2 第 1 項柱書）。

具体例：氏名と結びついていないインターネットの閲覧履歴、位置情報、cookie

(3) 個人関連情報に関するルールの確認

改正法 26 条の 2 第 1 項は、個人関連情報について、以下の通り規定しています。

> 個人関連情報取扱事業者・・・は、第三者が個人関連情報を個人データとして取得することが想定されるときは、第23条第1項各号に掲げる場合を除くほか、次に掲げる事項について、あらかじめ個人情報保護委員会規則で定めるところにより確認することをしないで、当該個人関連情報を当該第三者に提供してはならない。
> 一・・・本人の同意・・・
> 二 （略）

この規定により、ある企業が、個人を識別できない情報を、別の企業に提供し、その別の企業が、個人を識別できる形で利用することが想定される場合（「第三者が個人関連情報を個人データとして取得することが想定されるとき」）、本人の同意を得ていることを確認する必要があります。

「第三者が個人関連情報を個人データとして取得することが想定されるとき」に該当する場合、同意の取得が問題となりますので、実務上、「第三者が個人関連情報を個人データとして取得することが想定されるとき」をどのように判断するかが重要となります。

(4)「第三者が個人関連情報を個人データとして取得することが想定されるとき」の判定について

ア　提供先が明示している場合（争いなし）

個人関連情報の提供前に、提供先の会社が提供元の会社に「提供先において、個人関連情報を取得した後に他の情報を照合して個人を識別する」ことを明示している場合、「第三者が個人関連情報を個人データとして取得することが想定されるとき」に該当することは明らかです。

イ　提供先が明示していない場合（判定が難しい場合）

他方、上記のように、提供先の会社が明示していない場合、「第三者が個人関連情報を個人データとして取得することが想定されるとき」に該当するかどうかが問題となります。

この点について、立法担当者は、「取引状況等の客観的事情に照らし、一般人の認識を基準とすれば、当該第三者によって個人データとして取得されることを通常想定できる場合」、「第三者が個人関連情報を個人データとして取得することが想定されるとき」に該当するという基準を示しています。また、具体例として、「第三者に個人関連情報を提供する際、当該第三者において当該個人関連情報を氏名等と紐付けて利用することを念頭に、そのために用いる固有 ID 等も併せて提供する場合」を挙げています（一問一答 p65）。

ウ　提供元と提供先との契約において「提供先は、個人データとして取得しない」ことが規定されている場合

提供元と提供先との契約において「提供先は、個人データとして取得しない」ことが規定されている場合、通常、提供元の個人関連情報取扱事業者は、当該第三者が個人関連情報を個人データとして取得することを想定していません。したがって、改正法 26 条の 2 第 1 項は原則として適用されないように思われます。

他方、立法担当官は、提供先が大規模通販事業者である場合、不特定多数の顧客情報を保有しており、「一般人の認識を基準とした場合、提供した個人関連情報が顧客情報と照合されて個人データとして取得される蓋然性が高い場合も考えられます」としていることには注意が必要です（一問一答 p66）。

この見解によれば、契約により「個人データとして使用しないこと」を明確に規定していたとしても、必ずしも改正法 26 条の 2 第 1 項の規定が適用されないことにはなりません。将来、個人情報保護委員会からの行政指導がなされないよう、念のために、同項規定の「確認」をしておいた方がよい場合もあると思われます。

(5) 他の検討課題

上記において述べたこと以外にも、以下の点が検討課題となります。

①同意の取得方法
②同意を取得していることの確認の記録
③個人関連情報を海外に移転させる場合の対応
④個人関連情報を委託する場合の対応

---
[4] 一問一答 p60 参照

（6）個人関連情報について、GDPR の観点からフランクフルト提携オフィスのコメント

1. Definition of personal data under GDPR

Under Article 4(1) GDPR, "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". GDPR does not have a separate definition for "personal-related information" like the Japanese data protection law. Even though one piece of data alone may not identify a natural person, after being combined with other pieces, they can identify an individual and therefore still constitute personal data. In other words, data such as Internet browsing history, location information, cookies, which is considered "personal-related information" under Japanese data protection act, is also defined as "personal data" under GDPR and is protected as any other personal data categories such as name, ID number or email address.

Data only stops being considered "personal" under GDPR when it is made irreversibly anonymous, and the data subject can no longer be identified by any means. Anonymized data is therefore not protected by GDPR. Data that has been encrypted or pseudonymized is still considered "personal data" as it can potentially be used to re-identify a person when being decoded or combined with more data.

2. Controllers' obligations towards personal data

As long as the data is considered "personal data", it is protected under GDPR and data controllers and processors have to fulfil their obligations towards such data. Each data controller and processor shall be independently responsible for complying with its obligations under GDPR, unless:

(i) when they are joint controllers. In this case, the joint controllers can have some forms of agreement among themselves about who shall be responsible for which obligations, including the obligations to obtain data subjects' consent when required (Article 26(1) GDPR); or

(ii) in a controller- processor relation in which the processor shall only process personal data under the controller's instruction, it is the controller's sole obligation to make sure data subjects have given valid consent, if required. However, Article 11 GDPR provides an exemption that "if the purposes for which a controller processes personal data do not or do no longer require the identification of a data subject by the controller, the controller shall not be obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with this Regulation". That means, if the controller shares with its processor personal data, which the controller cannot use to identify the data subjects, it does not have to collect more information to identify them only to obtain their consent. Even if the processor can potentially use the personal data from the controller to identify the data subjects, it may not be allowed under the controller's instruction to do so. And if the processor nevertheless tries to identify the data subjects for its own purposes, the processor will be considered an independent controller in respect of that personal data and must then be independently responsible for, among others, ensuring a lawful basis for its processing activities e.g. obtaining consent (Article 28(10) GDPR).

When an independent controller A shares personal data, which it cannot use to identify the data subjects, to another independent controller B who might be able to use such data to identify the data subjects, GDPR does not require controller A to make sure that controller B has obtained the data subjects' consent. In respect of controller B's independent processing activities after receiving the data from controller A, it is controller B's sole obligation to inform the data subjects how it processes their data and ask for their consent (if consent is required). If controller B fails to comply with this obligation, it must be liable to the data subjects on its own, without controller A being involved.

However, if controller B is not located in an EEA country or a country with Adequacy Decision (Article 45 GDPR), controller A must ensure that controller B will comply with GDPR basic principles by applying one of the appropriate safeguards under Article 46(2) GDPR. Standard contractual clauses by the EU Commission, as the most commonly used safeguard, requires the data exporter (i.e. controller A) to use reasonable efforts to determine that the data importer (i.e. controller B) is able to satisfy its legal obligations under those clauses. In this case, controller A might be held liable to data subjects if it shares personal data with controller B despite being aware of the fact that controller B is actually not able to ensure GDPR principles (e.g. not able to obtain data subjects' consent where required). The rule for international transfer of data is one of the rare GDPR rules requiring a data sender to have some control over its data recipient, which is to an extent similar to the "personal -related information" rules in Japanese data protection act.

In short, GDPR does not distinguish personal data-related information and there are thus no special rules for personal-related information under this Regulation. Data controllers and processors shall be independently responsible for complying with their obligations under GDPR or under equivalent applicable law, unless in case of joint controllership or when the data importer is not located in an EEA country or a country with Adequacy Decision.

5. 個人データの漏えい時の義務（Data Breach）

（1）漏えい時の義務が設けられた理由

令和 2 年改正前においては、個人データが漏えいした場合に法律上の義務は定められておらず、「告示」により、個人情報保護委員会へ報告するよう定められていました。法律上の義務が定められていなかったことから、報告をしない事案もあったため、令和 2 年改正により、法律上の義務が定められることとなりました[5]。

（2）漏えい時の義務に関するルールの確認

改正法 22 条の 2 第 1 項は、漏えい時の個人情報保護委員会への報告義務について、以下の通り規定しています。

> 個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失、毀損その他の個人データの安全の確保に係る自体であって個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を個人情報保護委員会に報告しなければならない。

また、改正法 22 条の 2 第 2 項本文は、漏えい時の本人への通知義務について、以下の通り規定しています。

> 前項に規定する場合には、個人情報取扱事業者・・・は、本人に対し、個人情報保護委員会規則で定めるところにより、当該事態が生じた旨を通知しなければならない。

したがって、令和 2 年改正法施行後は、一定の個人データの漏えいがあった場合、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負います。

（3）個人情報保護委員会への報告義務（どのような漏えいの場合、いつまでに）

実務上、個人情報保護委員会への報告義務が生じるのは、「どのような漏えいの場合か」（以下の「ア」）、また、「いつまでに」（以下の「イ」）報告する必要があるのかが重要となります。

ア 「どのような漏えいの場合」に報告義務が生じるのか

改正規則 6 条の 2 は、以下の場合に報告義務が生じると規定しています。

> ①要配慮個人情報が含まれる場合
> 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
> 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
> 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

イ 「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

（4）データ漏えい時の法的義務についての対応のポイント

ア データの漏えいの発生から個人情報保護委員会への報告に至るまでの具体的な社内手続きを整備

社内手続きが整備されていない場合、データの漏えいが発生したとしても、上記の期限までに報告できないこととなります。したがって、少なくとも以下のような事項を準備しておく必要があります。

①インシデントレポート
②データ漏えいに対応する責任部署
③データ漏えいに対応するための分かりやすいフロー図

イ 従業員の認識（研修）

会社の様々な部署の方が個人データを取扱っていますので、データの漏えいは、会社の様々な部署で発生する可能性があります。ある部署の方が、上記の期限を知らず、個人情報保護委員会への報告が遅れた場合、会社として、個人情報保護法に違反するおそれがあります。

そこで、会社の様々な部署の方に対して、広く研修などを行い、上記の個人データ漏えい時の対応について、周知を行う必要があります。

ウ 委託先などとの契約書

個人データを委託先に移転している場合、委託先におけるデータ漏えいに対応する必要があります。委託先からデータ漏えいの報告を速やかに得て、データ漏えいの原因究明などの対応が可能となるよう、委託先との契約書を見直す必要があります。

エ 外国居住者の個人データを保有している場合

外国居住者の個人データを保有している場合、当該外国法に基づく当局への報告・本人への通知を検討する必要があります。

---
[5] 一問一答 p37 参照

（5）漏えい時の義務について、GDPR の観点からフランクフルト提携オフィスのコメント

Article 33(1) GDPR sets out a general notification requirement in case of data breach. In particular, a controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of a data breach, notify the breach to the competent supervisory authority, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons. If the notification to the supervisory authority is not made within 72 hours, the controller must provide reasons for the delay.

With the exemption given in Article 33(1) GDPR when there is no risk to natural persons, it is vitally important that the controller should not only seek to contain the data incident, but it should also assess the risk that could result from the breach immediately upon becoming aware of it.

There is no precise definition of when a data breach results in a risk to the rights and freedoms of data subjects. In its guidelines, the EDPB suggests several factors for controllers to consider when assessing a data breach's risks, in particular:

- the type of breach (e.g data leakage or data lost);
- the nature, sensitivity, and volume of personal data;
- the ease of identification of individuals;
- the severity of consequences for individuals;
- the special characteristics of the individual and the data controller.

Recital 75 GDPR gives some examples of risks to rights and freedoms and suggests that risks should be broadly interpreted to include physical, material as well as non-material damage such as discrimination, identity theft, fraud, financial loss, reputation damage or unauthorized reversal of pseudonymization, etc. In practice, data controllers are likely to notify data breaches in most cases, rather than take the risk of not notifying and then being found later to be in violation.

In case the breach poses high risks to the natural persons (e.g. when sensitive data is involved), the controller will have to notify not only the supervisory authority, but also the affected data subjects (Article 34(1) GDPR).

On the other hand, the EDPB's guideline states that if e.g. the breached data is publicly available or properly encrypted to be unintelligible to unauthorized parties, it is considered "no-risk" situations and the controller will be exempted from the notification obligation.

Regarding the data breach notification procedure, it is not compulsory but it can be recommended as best practice for data controllers and processors to have in place trainings as well as internal policies for their employees on how to react in case of data breach.

Besides, Article 33(5) GDPR also requires controllers to keep reports of all data breaches (not only the one that imposes risks on natural persons), including the facts relating to the breach, its effects, and the remedy taken. The competent supervisory authority may ask for this data breach reports at anytime to check the controllers' accountability.

Fines for non-compliance with the data breach notification and documentation obligation under Article 33 GDPR can be up to 10 million Euro or up to 2% of the controller's worldwide turnover of the preceding year, whichever is higher (Article 83 (4)(a) GDPR).

6. 仮名加工情報

（1）「仮名加工情報」のルールが設けられた理由

平成 27 年改正法において、ビックデータの適正な利活用に資する環境整備のために「匿名加工情報」が創設されました。匿名加工情報は、特定の個人を識別することができないよう、また、作成元の個人情報を復元することができないように加工されたものであり、本人の同意なく、目的外利用や第三者提供を行うことができます。

他方、安全管理措置の一環として、匿名加工情報の作成には及ばない程度の加工（氏名の削除など）を施し、加工後のデータ単体からは特定の個人を識別できないようにする事例（仮名化）も存在しました。

「仮名化」された個人情報は、比較的簡便な加工により一定の安全性を確保するとともに、データとしての有用性を保ち得るものとして、利活用されることが想定されています[6]。

（2）「仮名加工情報」とは

「仮名加工情報」とは、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報です。

仮名加工情報は、以下の特徴があります。

①事業者内部における分析に限定
②本人の請求への対応義務を緩和
③漏えい時の報告義務を緩和

---
[6] 一問一答 p11 参照

（3）「仮名加工情報」の利用が想定されている領域

立法担当官によれば、以下のようなケースが仮名加工情報の利用が想定されています（一問一答 p16）。

①当初の利用目的には該当しない目的や、該当するか判断が難しい新たな目的での内部分析を行うケース（データセット中の特異な値が重要とされる、医療・製薬分野における研究用データセットとして用いるケースや、不正検知等の機械学習モデルの学習用データセットとして用いるケース等）
②利用目的達成した個人情報について、将来的に統計分析に利用する可能性があるため、仮名加工情報として加工した上で保管するケース

（4）仮名加工情報について、GDPR の観点からフランクフルト提携オフィスのコメント

Article 4(5) GDPR defines “pseudonymization” as “the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person”. A common method of pseudonymization is to replace one attribute such as name, social security number, data of birth etc. in a dataset by e.g. a randomly assigned code. After this process, as pseudonymized data can still be used to indirectly identify the data subject, it remains being personal data protected under GDPR. The additional information which can be used to re-identified data subjects must be kept separately from the data it relates to by means of technical or organizational measures. Under GDPR, pseudonymization is not only encouraged as a mean of data security (Article 32(1)(a) GDPR). The technique is also linked to the more generalized duty of “data protection by design” (Article 25(1) GDPR) and to data minimization safeguards connected to processing for archiving purposes, scientific or historical research purposes or statistical purposes (Article 89(1) GDPR).

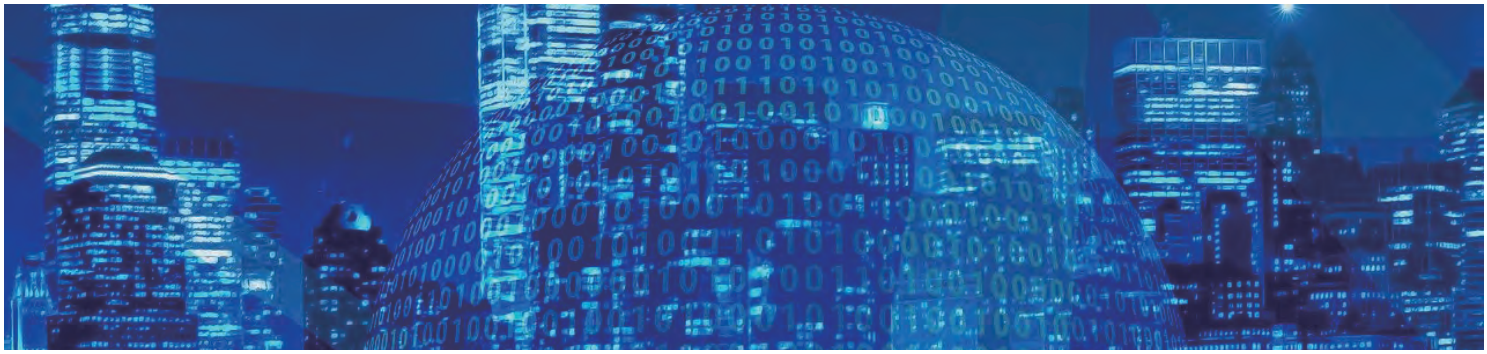
Pseudonymization is not made a compulsory duty, but rather a recommended technique according to the GDPR wordings. However, some EU Member States’ laws still impose strict pseudonymization requirements. For example, Article 71(1) of the German Protection Act stipulates that “personal data shall be rendered anonymous or pseudonymized as early as possible, as far as possible in accordance with the purpose of processing”. It is nevertheless controversial whether the EU Member State are allowed under GDPR to make pseudonymization a compulsory measures for data security in its national rules.

7. 今後の連載予定について

今後、「カメラ画像情報の国際的共有」、「位置情報のビジネス的な利用」、「医療製薬分野（仮名加工情報）」、「金融分野」、「中国法」をテーマとするニューズレターを連載する予定です。

他プラクティスグループのニューズレターも配信しております。
配信を希望される方は下記メールアドレス宛にご連絡ください。
広報部宛　prcorestaff@aplaw.jp
※お名前、部署、役職をご明記ください。
　また、下記の一覧よりご興味ある分野をお選びください。

【日本語】
□ジェネラル／様々な分野の旬な法律トピックス
□ベトナムビジネス
□インドビジネス
□ロシアビジネス
□再生可能エネルギー
□農林水産
□イノベーション／テクノロジー
□その他（ご興味のある分野をご教示ください。）
【英語】
□ジェネラル／様々な分野の旬な法律トピックス



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 福原 聡
アソシエイト / 第二東京弁護士会

E: satoshi.fukuhara@aplaw.jp

> View Profile

弁護士 設樂 承平
アソシエイト / 第二東京弁護士会

E: shohei.shidara@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