JIPDEC・日本商工会議所共催「中小企業向け改正個人情報保護法実務対応セミナー」講演要旨

2017 年 1 月 27 日開催

「改正個人情報保護法への実務対応」

牛島総合法律事務所　弁護士　影島 広泰氏

■改正個人情報保護法とは

今回の改正個人情報保護法（以下、「改正法」という。）の全面施行によりすべての事業者に対し、①取得、②利用、③保管、④提供、⑤開示等について、法的規制がかかることとなった（図 1）。

改正法の主な変更点としては、これまで適用除外であった小規模事業者（取り扱う個人情報の数が 5,000 人以下）にも法的規制がかかるようになったことが挙げられる。

また、現行法で業界ごとに所管する各省庁の主務大臣が持っていた監督権限が、改正法により設立された個人情報保護委員会に権限が一元化され、所管省庁策定の 27 分野、39 ガイドラインも原則として委員会に一元化されることとなった。この個人情報保護委員会はいわゆる三条委員会と呼ばれる、政府から独立性の高い公正取引委員会に匹敵する委員会として位置づけられ、事業者への立入検査権を有している。

改正法により新たに導入された罰則行為として、

・個人情報データベース提供罪（第 83 条）

・検査拒否等の罰則（第 85 条 1 条）

が挙げられるが、特に「個人情報データベース提供罪」は社員による名簿売買行為に対する罰則となるため、従業者への教育のポイントとなる。また、立入検査を拒否した場合に罰則が科せられることがあるため、注意が必要である。

なお、2013 年に策定されたマイナンバー法は個人情報保護法の「特別法」と位置づけられており、マイナンバーを取り扱う際には改正個人情報保護法とマイナンバー法の両方が適用される。

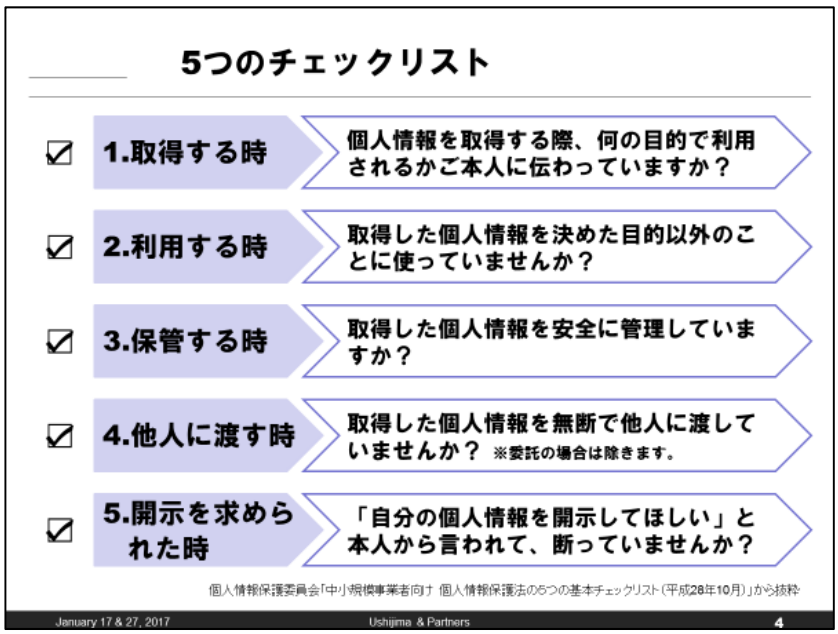


図 1.5 つのポイント

■「個人情報」の定義

改正法により「個人情報」の概念が大きく変わり、従前からあった「個人情報」「個人情報データベース等」「個人データ」「保有個人データ」のほか、「個人識別符号」「要配慮個人情報」が新設されたことから、事業者は何が個人情報に当たるかの把握が最も重要なこととなる。

（1）個人情報の定義

個人情報	生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により**特定の個人を識別することができるもの**（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。 例）・会社における職位又は所属情報であって氏名と組み合わせたもの ・防犯カメラに記録された情報等、本人が判別できる映像情報 ・メールアドレスだけでも特定の個人が識別できる場合は個人情報に該当する ・官報、電話帳、職員録、法定開示書類（有価証券報告書等）、新聞、ホームページ、SNS 等で公にされている特定の個人を識別できる情報 ・日本国民に限らず、外国人も「個人」に含まれる なお、企業の財務情報等、法人等団体そのものの情報や、死者に関する情報は個人情報に該当しない。 注）「容易に照合することができ」るとは、通常の業務において**一般的な方法で他の情報と容易に照合できる**状態をさす。
個人情報データベース等	個人情報を含む情報の集合物であって、検索できるように構成したもの。**利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。** 【除外されるものの例】 市販の電話帳、住宅地図。これらの情報は安全管理措置、第三者提供の対象外となる。例えば、第三者提供の際に掲載されている本人の同意は不要である。
個人データ	個人情報データベース等を構成する個人情報をいう。 注）個人情報と個人データの違いは、単体で存在しているのが個人情報であるのに対し、データベース化された情報が個人データである。
保有個人データ	個人情報取扱事業者が、開示、内容の訂正、追加または削除、利用の停止、消去および第三者への提供の停止を行うことのできる権限を有する個人データ 【保有個人データに該当しないものの例】 クラウド事業者 A 社が B 社から預かっている個人データは、通常、本人から A 社に開示請求があっても、B 社との守秘義務契約により開示できないため、A 社の保有個人データにはならない。

上記の概念を図示化したのが図 2 である。

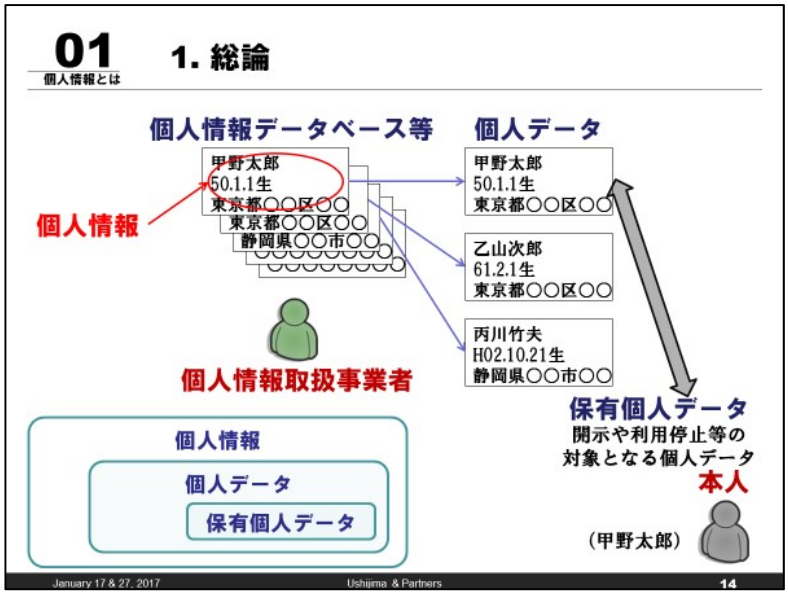
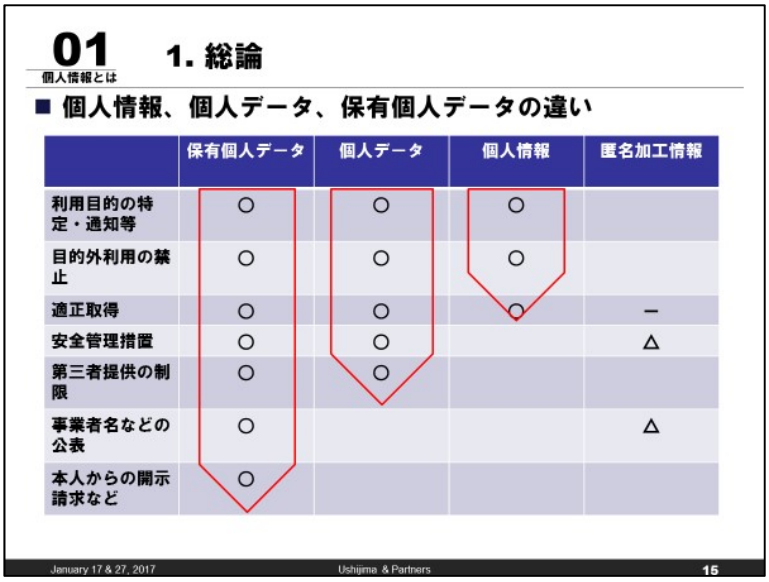


図 2.個人情報の定義

個人情報、個人データ、保有個人データはそれぞれ取り扱う局面により規制対象が異なっており、個人情報は「安全管理措置」と「第三者提供制限」の法的規制がかからない。例えば、第三者提供時に同意が必要となるのは「個人データ」のみである（図 3）。



	保有個人データ	個人データ	個人情報	匿名加工情報
利用目的の特定・通知等	○	○	○	
目的外利用の禁止	○	○	○	
適正取得	○	○	○	－
安全管理措置	○	○		△
第三者提供の制限	○	○		
事業者名などの公表	○			△
本人からの開示請求など	○			

図 3.法的規制対象

（2）個人識別符号の新設

IT 技術の発達に伴い、個人情報と個人情報ではないものの区別があいまいになった。特定の個人を識別できるもの、たとえば、顔認識データの場合、目と目と鼻の間隔を示す 3 つの数字をコンピュータ処理することで特定の個人を識別できるため、個人情報として保護すべきである、との意見が出された。また端末 ID 等の場合、個人／法人所有での整理の必要性があるなどの考えから、改正法では「個人識別符号」が新設され、個人情報の定義に追加された。

政令第 1 条第 1 項第 1 号および 1 条 1 項 2～7 号で個人識別符号が定められている。

1 号）特定の個人の身体の一部の特徴を電子計算機で使用するために変換した符号

（DNA、顔の骨格、虹彩、声紋、歩行態様、静脈の形状、指紋又は掌紋等）

2 号）対象者ごとに異なるものとなるように役務の利用、商品の購入又は書類に付される符号
（パスポート番号、基礎年金番号、運転免許証番号、住民票コード及び個人番号等）

なお、携帯端末 ID、携帯電話番号、メールアドレス、クレジットカード番号等は「個人識別符号」として政令に列挙されていないから、通常は単体では個人情報ではない。しかし、他の情報（氏名等）と１つのデータセットとして保有していたり、容易照合性により、個人情報(１号の符号)に該当することもありえる。また、メールアドレスは、前に述べたとおり、氏名がアドレスに使われている場合などには単体で個人情報に当たることがあるから注意が必要である。

（3）要配慮個人情報の新設

要配慮個人情報とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪被害の事実、その他本人に対する不当な差別、偏見その他の不利益が生じないように、取扱いに配慮を要するものとして政令で定めた 11 個の情報を指す。中小企業の実務では、特に「病歴」と「健康診断等の結果」が要配慮個人情報に該当することに注意が必要となる。

要配慮個人情報の取得にあたっては、あらかじめ本人の同意が必要となり、オプトアウトによる第三者提供もできない。ただし、法令に基づく取得、たとえば企業が労働安全衛生法に基づき、社員の健康診断結果を健診実施機関から取得する場合や、本人が SNS やブログ等で公開している情報の取得にあたっては、本人同意は不要となる。このほか、コンビニ等店舗の監視カメラに外形上明らかに身体の障害が映っている場合などには「同意」は不要である。

また、本人が要配慮個人情報に該当する情報を提供している場合、例えば、採用時に履歴書に本人の要配慮個人情報を記載しているような場合には、本人が提供しているという事実をもって同意があると考えて良いのが一般的であろう。

■個人情報取得の実務

（1）利用目的の特定

個人情報の取得にあたっては、利用目的を特定し通知等する必要がある。利用目的の特定にあたっては、改正法第 15 条で「できる限り特定」しなければならない、と定められており、利用目的を詳しく、具体的に通知する必要がある。

（2）利用目的の通知等

特定した利用目的の通知・公表・明示は必要だが、本人に利用目的を通知・公表していれば、法律上同意は必要ない。明示が必要な場面としては、本人の個人情報が記載された申込書・契約書等を本人から直接取得する場合、アンケートに記載された個人情報を直接本人から取得する場合、キャンペーン参加希望者が企業のウェブサイトの入力画面に入力した個人情報を直接本人から取得する場合が挙げられる。明示と通知・公表の違いについて図 4 に示す。通知・公表、明示の方法はガイドラインで紹介されている。

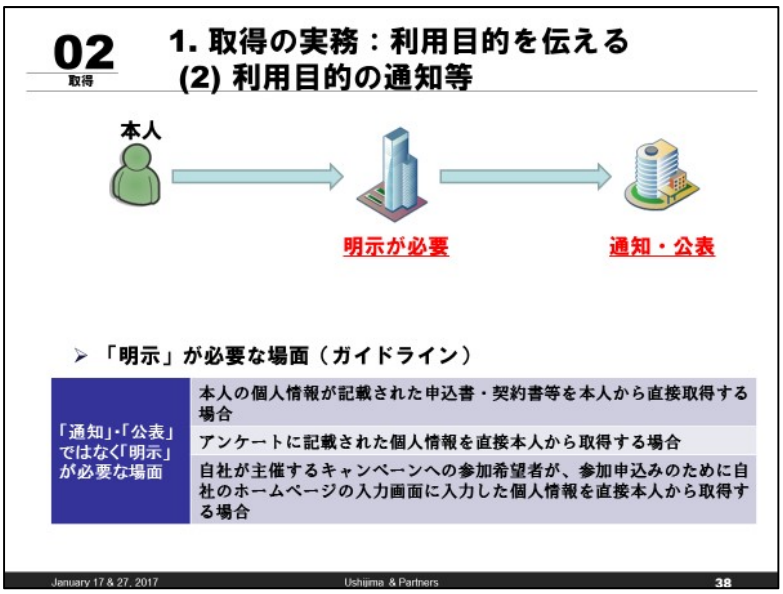


図 4.利用目的の通知・公表・明示

なお、利用目的を本人に通知・公表することで当該個人情報取扱事業者の権利または正当な利益を害するおそれがある場合、たとえば反社会勢力情報や業務妨害を行う悪質者情報等を取得したことが明らかになることで当該事業者に害が及ぶ場合や、名刺交換などの取得状況から利用目的が明らかと認められる場合は、利用目的の通知は不要である。

■個人情報利用の実務

（1）利用範囲

事業者は、利用目的の達成のために必要な範囲以外で個人情報を利用してはならないが、法令に基づく場合や、人・法人の生命・身体・財産などの具体的な権利利益の保護のために必要で、本人の同意を得ることが困難な場合等には目的外利用が可能となる。たとえば、従業員が急病になり、医者に本人や家族の連絡先等を伝えなければならないが本人同意が困難な場合などが該当する。

（2）利用目的の変更

利用目的を後で変更する場合、原則本人同意が必要であるが、元の利用目的と関連性がある場合は変更された利用目的を通知または公表すれば同意は不要である。現行法では「相当の」関連性がなければならなかったが、改正法では社会通念上、本人が通常予期しえる限度と客観的に認められる範囲内であることとして、規制が緩和されている。

■個人データの保管・管理

個人データの保管にあたっては、以下に述べるとおり（1）安全管理措置、（2）従業者への監督義務、（3）委託先に対する監督義務等が課せられている。

個人情報保護委員会から経済産業分野ガイドラインをベースとした「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。）が公表され、必要かつ適切な措置について解説されている。なお、マイナンバー法ガイドラインと基本的な枠組みはほぼ同じである。

（1）データの安全管理措置：個人データの漏えい、滅失またはき損の防止等のために「必要かつ適切な措置」を講じる義務

（2）従業者への監督：従業者に対する「必要かつ適切な監督」を講じる義務

（3）委託先の監督：委託先に対する「必要かつ適切な監督」を講じる義務

なお、上記の安全管理措置をはじめとする個人情報保護法に違反した場合、まず個人情報保護委員会から勧告が出され、守らなければ「命令」が出され、命令に違反すると「刑罰」が科せられることとなっている。

■安全管理措置

（1）データの安全管理措置

事業者が行う安全管理措置について、ガイドラインでは以下 6 つの措置が定められている。なお、これまで適用除外であった小規模事業者に対しては軽減措置が設けられている。

1）基本方針の策定

2）個人データの取扱いに係る規律の整備

3）組織的安全管理措置

4）人的安全管理措置

5）物理的安全管理措置

6）技術的安全管理措置

なお、従業員 100 人以下の事業者は「中小規模事業者」と呼ばれ、措置についての軽減された例示がなされている（ただし、取り扱う個人情報の本人の数が 5,000 人を超える事業者、または委託を受けて個人データを取り扱う事業者は、中小規模事業者に該当しない）。

以下、安全管理措置の概要を紹介する。

1）基本方針の策定

個人データの適正な取扱いの確保について、組織として取り組むために基本方針を策定することが重要であるとされている。なお、基本方針の策定は義務であるとはされていない。

2）個人データの取扱いに係る規律の整備

個人データの取扱いに関する社内規程を策定することになる。なお、中小規模事業者は社内規程を策定せず、個人データの取得、利用、保存等を行う場合の基本的な取扱い方法を整備しておけばよい。

3）組織的安全管理措置

事業者は安全管理措置を講ずるための組織体制を整備しなければならないが、中小規模事業者の場合、個人データを取り扱う事業者が複数いる場合は責任ある立場の者とその他の者を区別すればよい。

あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。

個人データの取扱い状況を確認するための手段を整備しなければならない。手法としては、一般的には「個人データ取扱台帳」を作成し、個人データベース等の種類、名称、個人データの項目、責任者・取扱い部署、アクセス権限者を一覧表化して常時把握できるようにする。中小規模事業者については、あらかじめ整備された取扱い方法に従って取り扱われているかを責任者が確認すればよい。

漏えい等の事案の発生または兆候を把握した場合は、適切かつ迅速に対応するための体制を整備しなければならない。なお、漏えい時対応に関しては、別途個人情報保護委員会より発表される予定である（注：講演後に「個人データの漏えい等の事案が発生した場合等の対応について」が発表された）。

個人データの取扱状況を把握し、安全管理措置の評価、見直しおよび改善に取り組まなければならない。安全管理措置についても PDCA（Plan-Do-check-Act）サイクルを回す必要があるということである。

4）人的安全管理措置

従業員に対する教育をきちんと行うということである。これは従前の経済産業分野ガイドラインでも挙げられて

いる内容で、新たな対応が必要ということではない。

5）物理的安全管理措置

経済産業分野ガイドラインよりも区域の管理および持ち運び規制が強化されている。

区域の管理では、これまでは入退室管理だけが求められていたが、サーバや情報システムを管理する区域（管理区域）や個人データを取り扱う事務を行う区域（取扱区域）等、マイナンバー導入の際に求められた措置が新たに加わっている。

また、盗難防止だけでなく、新たに持ち運び時の対策も求められるようになったため、移送の際の個人データの暗号化や目隠しシールの貼付、施錠できる搬送容器の利用等の対応が必要となる。特に実務的には、従業員のスマホに入った個人情報への対策に注意が必要である。削除・廃棄に際しては、シュレッダー処理等復元できないようにすることが求められている。

6）技術的安全管理措置

特に新たな上乗せ措置はなく、従来どおりアクセス制御、ID・パスワード等でのアクセス者の識別と認証、ウイルス対策ソフト等を導入した外部からの不正アクセス防止、システム利用時の漏えい防止（メール添付ファイルへのパスワード設定等）を行うことが求められている。

（2）委託先の監督

以上は自社内で行う措置となるが、もう 1 つ重要な対策として「委託先の監督」が挙げられる。たとえば宛名ラベルの印字を依頼する際は個人データ取扱いの委託にあたる。このように、個人情報を委託すること自体はまったく問題がなく、本人の同意も必要がないが、マイナンバー導入時と同様に、委託にあたっては、①委託先の選定、②委託契約の締結、③委託先における個人データ取扱い状況の把握、が必要となる。

実務的には、委託先の監督をどこまで厳密に行うかが問題となってくる。ガイドラインでは、「本人が被る権利利益侵害の大きさを考慮し、委託する事業の規模及び性質、個人データの取扱い状況（取り扱う個人データの性質及び量を含む）等に起因するリスクに応じて」行うとなっている。つまり、たとえば取引先一覧と顧客のセンシティブ情報では本人に与える影響が大きく異なる、また企業の規模によって監督の義務も異なってくると明示されているので、杓子定規に考える必要はなく、自社の規模・委託内容に基づき柔軟に対応することができる。

委託先の選定にあたっては「自分の会社が果たすべき義務」を委託先も果たしているかが選定の視点となる。また、委託先の取扱い状況の把握に関しては、定期的な報告を求めるような条項を締結する契約内容に盛り込み、把握していくことが実務的に行われている。

委託に関して質問が多い内容として、委託とそれ以外の切り分けをどこで行うのか（クラウドは委託か？等）という問題がある。この件については、ガイドラインのパブコメ意見に対し「委託契約の条項により受託者が個人データを取り扱わない旨が定められており、適切なアクセス制御を行っている場合は委託にあたらない」という回答が個人情報保護委員会から出されている。宛名ラベルの印刷では、個人データの中身を使った個人情報取扱い事務を依頼しているので委託に当たる。一方、クラウドのストレージサービス等、中身を触らないというサービスは委託に当たらない、と整理することができる。

このほか、個人データの取扱いで「不要となった個人データ消去の努力義務」が新たに法律上で明確に定められた。

■個人データの第三者提供

第三者提供については、今回の改正で規制が強化されており、実務的にも重要なポイントとなる。

第三者提供の際の原則論は、本人の事前同意が必要というものである。同意のとり方については特に規制がないので、どのような形ででも構わない。ただし、同意が不要な例外として、①法令に基づく場合、生命・財産等の保護の

場合（急病の従業員に関する情報を病院に伝える等）、②「委託」「事業継承」「共同利用」の場合（第三者に当たらない）、③「オプトアウト」を用いる場合（本人が「嫌だ」と言った場合に第三者提供をやめることになっている場合）、が定められている。

（1）オプトアウト

これまでは実務で「オプトアウト」方式が幅広く使われていたが、一部、乱用されているという指摘もあった。たとえば名簿業者は「オプトアウトに際し本人に通知する内容」を事務所に掲示し、企業の顧客情報等の名簿を業者間で転々流通させている。しかし、実際にはわれわれはどこに名簿業者の事務所があるのか、どの名簿業者が自分のデータを持っているのかを把握できず、「第三者提供停止」を伝える機会も持てない。このため、今回の改正では以下のように規制が強化されているため、これまでオプトアウト方式を取っていた企業は見直しが必要となる。

① 要配慮個人情報はオプトアウト不可（必ず本人の事前同意が必要）
② オプトアウトに関して本人に通知・または容易に知りえる状態に置く内容に「本人の求めを受け付ける方法」を追加
③ オプトアウトによる第三者提供を行う際に「委員会」への届出が必要。委員会がオプトアウト方式を取っている企業一覧を掲載）。3 月 1 日から受付開始。現在該当する企業は 5 月 30 日までに届出が必要となる。
④ オプトアウトについて本人に通知または本人が容易に知りえる状態に置く場合の措置の強化（必要な期間を置く、確実に認識できる適切かつ合理的な方法によること）

（2）トレーサビリティ

今後、個人データを第三者提供する場合は、提供する側も提供を受ける側も「いつどこに提供したか」「いつどこから提供を受けたか」を記録する義務が生じる。ただし、国・地方公共団体等に提供する際、法令や生命・財産に関わる場合等、委託・事業継承・共同利用の場合は記録義務がない。また、解釈として、本人が SNS 等を利用して提供している情報や、修理の取次ぎ等本人に代わって提供している場合は提供者には当たらないと解釈できるため、記録義務の対象とはならない。

また、本人と一体と評価できる関係にある者に提供する場合や最終的に本人に提供することが意図されている状況等も記録義務の対象外と考えられる。

提供する側の記録に際しては、以下の項目が求められる。

	提供年月日	第三者の 氏名等	本人の 氏名等	個人データの 項目	本人の同意
オプトアウトによる第三者提供	○	○	○	○	
本人の同意に基づく第三者提供		○	○	○	○

本人の氏名等については、人数ではなく「誰のデータか」（本人の氏名等）まで必要となるので、実務としては提供データそのものを保管しておくことが合理的と思われる。記録の保管期間は原則として 3 年となる。

提供を受ける側はこれまで規制がなかったが、今後は提供にあたって確認・記録が必要となる。確認項目は、①提供者の氏名、②提供データの取得経緯（誰からどうやって入手したか）が法律で定められており、提供者の個人情報保護法遵守状況を確認することも「望ましい」とされている。

また、実務で提供を受ける場合の重要ポイントとして、個人データの中の 1 件のみを受け取る場合（＝個人情報の受領）や、システムのテストデータとして氏名等を除去した個人データを受け取る場合等、提供者にとっては個人データであっても、受領者にとっては個人データに該当しない場合は確認・記録の義務は発生しない。

確認する際のポイントとしては、氏名や所在地は口頭での確認も認められるが、取得の経緯については売買契約書等、エビデンスに基づく確認が求められる。

受領する側の記録事項は以下のとおり。

	提供を受けた年月日	第三者の氏名等	取得の経緯	本人の氏名等	個人データの項目	委員会による公表	本人の同意
個人情報取扱事業者からオプトアウトによる第三者提供	○	○	○	○	○	○	
個人情報取扱事業者から本人の同意に基づく第三者提供		○	○	○	○		○
個人情報取扱事業者ではない者（私人など）からの第三者提供		○	○	○	○		

提供する側と同様、記録にあたっては提供を受けたデータそのものを保管しておくことが実務上合理的と思われる。

■外国にある第三者への提供

外国への個人データ移転に関してはこれまで法律上の規制はなく、新たな規制導入となる。

改正後、外国へのデータ移転に際しては、たとえ従業員に関するものでも原則として事前に本人の同意が必要となる。ただし、例外として今後公表される委員会規則で定める「日本と同等の水準にある外国への提供」や「基準に適合する体制を整備している者（移転先企業）への提供」に関しては事前同意が不要としている。この規制は、委託や共同利用の場合にも適用されるため、注意が必要となる。

実務的には、本人から同意をとるか、移転先企業の体制整備を確認することになる。体制整備に関しては、移転先企業との契約書・覚書等で日本の個人情報保護法の義務の実施が確保されている、または国際的な枠組みに基づく認定を受けていることを以て条件が満たされていることになる。国際的な枠組みに基づく認定の具体例としてはAPEC CBPR 認証が挙げられる。また、委託については委託元が CBPR 認証を受けることで、海外へのデータ移転の際の本人同意が不要となる旨がガイドラインで謳われているので、実務で委託による移転がある場合は対応策として検討する価値がある。

なお、「外国にある」とは外国で法人格を取得している法人のことであり、個人データを管理するサーバの所在地ではない。また、その外国法人が日本国内で個人データを事業の用に供しており、日本の個人情報取扱事業者に該当する場合は「外国にある第三者」には該当しない。さらに、クラウドに関しては、日本国内における委託と同様の考え方ができるため、純粋に外国にある第三者への提供という場面は非常に限定的なケースとなる可能性が高い。

■保有個人データ開示等に関する実務

保有個人データに関しては以下の事項を公表する義務があるため、プライバシーポリシー等に明記する必要がある。

① 個人情報取扱事業者の氏名又は名称
② すべての保有個人データの利用目的
③ 本人からの求めに応じる手続（手数料を徴収する場合は、その額も含む）
④ 保有個人データの取扱いに関する苦情の申出先

また、以前より本人から開示請求や訂正、利用停止の申出があった場合は対応が義務づけられていたが、今回の法改正で本人に裁判上の開示請求権があることが明確化された。これは企業法務から考えると、本人からの開示

請求を拒否すると裁判リスクが伴うことになるため、注意が必要である。

■匿名加工情報

匿名加工情報とは、ビッグデータ解析によるマーケティング等への円滑な利活用を目的として設けられたものであり、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あって、個人情報を復元することができないもののことを指している。加工にあたっては個人情報保護委員会規則で定める基準を満たすことが求められているが、加工の基準が抽象的であるため、経済産業省では 2016 年に「匿名加工情報作成マニュアル」を公表している。今後は個人情報保護委員会からも「匿名加工情報に関する事務局レポート」が出されることになっている。（注）

匿名加工情報の取扱いに関しては、安全管理措置や作成した情報の項目の公表などの義務はあるが、一番のポイントは本人の同意は不要となっており、取扱いのルールを遵守すれば利用目的も関係なく自由にデータ利活用ができる点である。

ただし、これまで特定の個人を識別できないように加工し、「非個人情報」として制限なく取り扱っていた情報のうち、「匿名加工情報」と位置づけられることにより規制が強化されている部分があることに注意が必要である。

もっとも、匿名加工情報はあくまでも「ある誰か」に関する情報を指すものであり、統計情報等「個人に関する情報」ではない形にしたものは匿名加工情報に当たらない。さらに、ガイドラインでは利用目的も考慮の対象となっており、匿名加工情報として取り扱うために加工したものが匿名加工情報であり、安全管理措置の一環として個人名等を削除したものは該当しない（安全管理措置を講じた個人データまたは個人情報に該当）。

（注）個人情報保護委員会「匿名加工に関する事務局レポート」は 2017 年 2 月 27 日に発行されている。

まとめ

今回の改正で特に対応が必要な点は、以下のとおりとなる。

- 要配慮個人情報
- 安全管理措置・委託先の監督
- 第三者提供の際の説明・記録義務
- 外国にある第三者への提供（特に委託）
- オプトアウトによる第三者提供

また、今後の個人情報取扱いに関しては、個人情報保護委員会が作成した「中小規模事業者向け　個人情報保護法の 5 つの基本チェックリスト」を参考にしてほしい。