

2017年個人情報保護法改正 ～改正の概要及び改正に伴う態勢整備～



井上 博登

長島・大野・常松法律事務所
弁護士

2017年5月30日をもって、個人情報の保護に関する法律(以下「個人情報保護法」といい、改正前のものを「現行法」、改正後のものを「改正法」という。)が大幅に改正される。これまでは、保有する個人情報によって識別される個人の数が5,000人以下の小規模事業者^{注1}については個人情報取扱事業者にあたらないものとされ、個人情報保護法の各種規制の適用対象から除外されていたが、2017年5月30日以降は全ての事業者に適用が広げられる。不動産証券化関連業務に携わる事業者は規模の大小様々であろうが、これまで適用の除外を受けてきた事業者は新たに個人情報保護法に対する対応が求められ、また、既に個人情報保護法の適用を受けて対応済みであった事業者も改正による対応が必要となる。改正の概要、改正後の個人情報保護法の枠組みを概観し、改正法の下での要対応事項についてご紹介したい。

1. 改正の概要

個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律(平成27年9月9日法律第65号)が2015年9月9日に公布され、2017年5月30日に施行されることとなった。これにより、個人情報保護法が大幅に改正される。

個人情報の取扱いについて懸念が広がっていることから、個人情報の流通経路を辿ることができるようにし、不正な個人情報の流通を防止する一方、ビッグデータの活用が求められる中、個人情報として取り扱うべき範囲が曖昧であるために、活用が進まないという指摘を受け、個人情報の定義を明確化し、匿名化された情報については活用ができるようにすること等が挙げられている。

改正の背景としては、名簿の流出などにより、個

主要な改正事項は以下の通りである。

注1

改正前の個人情報の保護に関する法律施行令第2条

法第二条第三項第五号の政令で定める者は、その事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数(中略)の合計が過去六月以内のいずれの日においても五千を超えない者とする。

(後略)

(1) 個人情報の定義の明確化

現行法では、「個人情報」とは、「生存する個人に関する情報であつて、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。)」をいうものとされているが、改正法では、下記のように「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。)」に加えて、「個人識別符号が含まれるもの」を個人情報として定義し、指紋データや顔認識データ、パスポート番号、運転免許証番号等が個人情報に含まれることが明確化された。

改正法第2条

1 この法律において「個人情報」とは、生存する個人に関する情報であつて、次の各号のいずれかに該当するものをいう。

一 当該情報に含まれる氏名、生年月日その他の記述等(文書、図画若しくは電磁的記録(電磁的方式(電子的方式、磁気的方式その他の知覚によっては認識することができない方式をいう。次項第2号において同じ。))で作られる記録をいう。第18条第2項において同じ。)に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項(個人識別符号を除く。)をいう。以下同じ。)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。)

二 個人識別符号が含まれるもの

2 この法律において「個人識別符号」とは、次の各号のいずれかに該当する文字、番号、記号

その他の符号のうち、政令で定めるものをいう。

一 特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であつて、当該特定の個人を識別することができるもの

二 個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であつて、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

(2) 要配慮個人情報

人種、信条、病歴等が含まれる個人情報については、要配慮個人情報として、原則として本人の同意を得た場合に限り取得できるものとし、また、本人の同意を得ないオプトアウトによる第三者提供^{注2}も認められないものとした。

改正法第2条第3項

この法律において「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、犯罪により害を被った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その取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

(3) 匿名加工情報

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たものを匿名加工情報と定義し、その加工方法・加工基準を定めることにより、匿名化された情報の利活用を促進する枠組みが導入された。

注2

下記2.(3)参照

(4) トレーサビリティの確保

個人データの提供者は、受領者の氏名等を記録する義務を負うものとされ、また、受領者も提供者の氏名やデータ取得経緯等を確認し、記録する義務を負うものとされた。

(5) オプトアウトによる第三者提供の厳格化

オプトアウトによる個人データの第三者提供をしようとする場合、データの項目等を個人情報保護委員会へ届け出るものとされ、また、個人情報保護委員会は、その内容を公表するものとされた。

(6) 小規模取扱事業者への対応

これまでは保有する個人情報によって識別される個人の数が5,000人以下の小規模事業者については個人情報取扱事業者には該当しないものとされ、実質的に個人情報保護法の適用が除外されてきたが、そのような事業者についても個人情報取扱事業者には該当することとなり、個人情報保護法への対応が求められることとなった。

2. 個人情報取扱事業者となる者が負うこととなる義務の概要

個人情報データベース等^{注3}を事業に用いることとした場合、個人情報取扱事業者^{注4}として個人情報保護法の適用を受けることとなる。「個人情報データベース等」は、改正法第2条第4項に定義されてい

るが、個人情報保護委員会作成「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)」(平成28年11月版)(以下「ガイドライン」という。)は、これにつき、「『個人情報データベース等』とは、特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した、個人情報を含む情報の集合体をいう。また、コンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則(例えば、五十音順等)に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものも該当する。」と説明しており、さらに、個人情報データベース等に該当する事例として、①電子メールソフトに保管されているメールアドレス帳(メールアドレスと氏名を組み合わせた情報を入力している場合)、②インターネットサービスにおいて、ユーザーが利用したサービスに係るログ情報がユーザーIDによって整理され保管されている電子ファイル(ユーザーIDと個人情報を容易に照合することができる場合)、③従業員が、名刺の情報を業務用パソコン(所有者を問わない。)の表計算ソフト等を用いて入力・整理している場合、④人材派遣会社が登録カードを、氏名の五十音順に整理し、五十音順のインデックスを付してファイルしている場合を例として挙げており、従業員、取引先担当者の情報をコンピュータを用いて管理したり、個人テナントの情報をレントロール等で管理したりしている場合には通常該当することとなる。

注3

改正法第2条第4項

この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの(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。)をいう。

- 一 特定の個人情報を電子計算機を用いて検索することができるように体系的に構成したもの
- 二 前号に掲げるもののほか、特定の個人情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの

注4

改正法第2条第5項

この法律において「個人情報取扱事業者」とは、個人情報データベース等を事業の用に供している者をいう。ただし、次に掲げる者を除く。

- 一 国の機関
- 二 地方公共団体
- 三 独立行政法人等(独立行政法人等の保有する個人情報の保護に関する法律(平成15年法律第59号)第2条1項に規定する独立行政法人等をいう。以下同じ。)
- 四 地方独立行政法人(地方独立行政法人法(平成15年法律第118号)第2条第1項に規定する地方独立行政法人をいう。以下同じ。)

個人情報取扱事業者となった場合、大要以下のよ
うな義務を負うこととなる。

(1) 個人情報の取得に関連する対応

個人情報取扱事業者は、個人情報の利用目的を
できる限り特定し(改正法第15条)、個人情報の取
得にあたっては原則として利用目的を本人に通知
し、又は公表しなければならない(改正法第18条第
1項)。また、本人から直接書面等で個人情報を取
得する場合には、原則としてその利用目的を明示し
なければならず(改正法第18条第2項)、利用目的
の範囲を超えた利用を行うには、原則として事前の
本人の同意が必要とされる(改正法第16条第1項)。
個人情報取扱事業者は、偽りその他不正な手段によ
り個人情報を取得してはならず(改正法第17条第1
項)、また、要配慮個人情報については原則として
事前の本人の同意なくして取得してはならないもの
とされる(改正法第17条第2項)。

(2) 個人情報の管理に関連する対応

個人情報取扱事業者は、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じなければならず
(改正法第20条)、その従業者及び委託先に対して
必要かつ適切な監督を行わなければならない(改正
法第21条及び第22条)。また、利用目的の達成に
必要な範囲内において、個人データを正確かつ最新
の内容に保つとともに、利用する必要がなくなったと
きは、当該個人データを遅滞なく消去するよう努め
なければならないものとされる(改正法第19条)。

(3) 個人情報の第三者に対する提供に関連する 対応

個人情報取扱事業者が個人データを第三者に提
供するには、原則として、事前の本人の同意が必要
とされる(改正法第23条第1項)。但し、第三者に
提供される個人データ(要配慮個人情報を除く。)に
ついて、本人の求めに応じて当該本人が識別される
個人データの第三者への提供を停止することとして
いる場合であって、一定の事項につき、あらかじめ、

本人に通知し、又は本人が容易に知り得る状態に置
くとともに、個人情報保護委員会に届け出たときは、
個人データを第三者に提供することができるものと
される(改正法第23条第2項。いわゆるオプトアウト
による第三者提供)。

また、委託、合併等、共同利用に伴う提供につい
ては第三者提供にあたらぬものとされている(改正
法第23条第5項)。

また、個人データを第三者に提供した個人情報取
扱事業者は、原則として、受領した者の氏名等を記
録する義務を負うものとされ、また、受領した個人
情報取扱事業者も提供者の氏名やデータ取得経緯
等を確認し、記録する義務を負う(改正法第25条及
び第26条)。

(4) 保有個人データへの本人の関与に対する対応

個人情報取扱事業者は、本人から求められたとき
は、原則として、保有個人データの利用目的を通知
しなければならない(改正法第27条第2項)。また、本
人から請求を受けたときは、原則として、本人に対
し、保有個人データを開示しなければならない(改正
法第28条)。また、保有個人データの内容が事実で
ないときは、原則として、本人からの請求に従い、内
容の訂正等を行わなければならない(改正法第29
条)。また、利用目的による制限(改正法第16条)、
適正な取得(改正法第17条)、第三者提供の制限(第
23条第1項及び第24条)に違反していることが判明
したときは、原則として、本人からの請求に従い、利
用停止等を行わなければならない(改正法第30条)。

3. 具体的な対応事項

個人情報取扱事業者に該当することとなった場合
の対応事項としては以下のようなものが考えられる。

(1) 個人情報の利用目的の通知態勢の確立又は 利用目的の公表

まず、個人情報取扱事業者としては、個人情報の

利用目的を定め、個人情報を取得した場合に個別に通知できる態勢を整えるか、利用目的を公表する必要がある。

ガイドラインによれば、ここでいう「公表」とは、広く一般に自己の意思を知らせること(不特定多数の人々が知ることができるように発表すること)をいい、公表に当たっては、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならない。

ガイドラインは「公表」にあたる事例として①自社のホームページのトップページから1回程度の操作で到達できる場所への掲載、②自社の店舗や事務所等、顧客が訪れることが想定される場所におけるポスター等の掲示、パンフレット等の備置き・配布、③(通信販売の場合)通信販売用のパンフレット・カタログ等への掲載を挙げている。

個人情報の利用目的の範囲を超えた利用を行うには、原則として事前の本人の同意が必要とされることから、利用目的はできる限り特定しつつも、予想される利用目的を広く想定しながら策定する必要がある。新規に作成するのであれば、各種不動産関連事業者の利用目的がホームページで公開されているため、参考とすることができるであろう。

また、書面により本人から個人情報を取得する場合にはあらかじめその利用目的を明示しなければならないため、そのような形で個人情報を取得する場面が想定される場合には、利用目的を明記した書面を本人に手渡すなどの対応が取れるよう準備しておく必要がある。

(2) 安全管理措置

前述の通り、個人情報取扱事業者は、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じな

ければならない(改正法第20条)が、具体的な対応についてはガイドラインに詳細な記載がある。

ガイドラインでは、中小規模の事業者が大規模な事業者と同様の対応を行うことに苦慮する可能性があることに配慮し、全ての事業者一律に同程度の対応を求めることをせず、中小規模事業者が取るべき措置とその他の事業者の事業者が取るべき措置の双方を提示している。

(ア) 基本方針の策定

ガイドラインでは、基本方針の策定が重要であるとされている。具体的に定める項目の例としては、「事業者の名称」、「関係法令・ガイドライン等の遵守」、「安全管理措置に関する事項」、「質問及び苦情処理の窓口」等が考えられるとされている。いわゆるプライバシーポリシーを策定済であれば、それを基本方針とすることができると考えられるが、未策定の場合には新たに策定が必要となる。

(イ) 個人データの取扱いに係る規律の整備

ガイドラインでは、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等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならないとされており、個人データの取扱いに係る内規の策定が必要となる。既に個人情報保護規程等の規程を策定済の事業者においても、法令の改正に合わせた変更が必要となると考えられる。

(ウ) 各種安全管理措置

ガイドラインでは、組織的安全管理措置、人的安全管理措置、物理的安全管理措置及び技術的安全管理措置として、次頁表記載の措置を講じなければならないものとしている。

講じなければならない措置	手法の例示	中小規模事業者における手法の例示
Ⅲ組織的安全管理措置		
①組織体制の整備	<p>(組織体制として整備する項目の例)</p> <ul style="list-style-type: none"> 個人データの取扱いに関する責任者の設置および責任の明確化 個人データを取り扱う従業員およびその役割の明確化 上記の従業員が取り扱う個人データの範囲の明確化 法や個人情報取扱事業者において整備されている個人データの取扱いに係る規律に違反している事実または兆候を把握した場合の責任者への報告連絡体制 個人データの漏えい等の事案の発生または兆候を把握した場合の責任者への報告連絡体制 個人データを複数の部署で取り扱う場合の各部署の役割分担および責任の明確化 	個人データを取り扱う従業員が複数いる場合、責任ある立場の者とその他の者を区分する。
②個人データの取扱いに係る規律に従った運用	<p>個人データの取扱いに係る規律に従った運用を確保するため、例えば次のような項目に関して、システムログその他の個人データの取扱いに係る記録の整備や業務日誌の作成等を通じて、個人データの取扱いの検証を可能とすることが考えられる。</p> <ul style="list-style-type: none"> 個人情報データベース等の利用・出力状況 個人データが記載または記録された書類・媒体等の持ち運び等の状況 個人情報データベース等の削除・廃棄の状況(委託した場合の消去・廃棄を証明する記録を含む。) 個人情報データベース等を情報システムで取り扱う場合、担当者の情報システムの利用状況(ログイン実績、アクセスログ等) 	あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。
③個人データの取扱状況を確認する手段の整備	<p>例えば次のような項目をあらかじめ明確化しておくことにより、個人データの取扱状況を把握可能とすることが考えられる。</p> <ul style="list-style-type: none"> 個人情報データベース等の種類、名称 個人データの項目 責任者・取扱部署 利用目的 アクセス権を有する者等 	あらかじめ整備された基本的な取扱方法に従って個人データが取り扱われていることを、責任ある立場の者が確認する。
④漏えい等の事案に対応する体制の整備	<p>漏えい等の事案の発生時に例えば次のような対応を行うための、体制を整備することが考えられる。</p> <ul style="list-style-type: none"> 事実関係の調査および原因の究明 影響を受ける可能性のある本人への連絡 委員会等への報告 再発防止策の検討および決定 事実関係および再発防止策等の公表等 	漏えい等の事案の発生時に備え、従業員から責任ある立場の者に対する報告連絡体制等をあらかじめ確認する。
⑤取扱状況の把握および安全管理措置の見直し	<ul style="list-style-type: none"> 個人データの取扱状況について、定期的に自ら行う点検または他部署等による監査を実施する。 外部の主体による監査活動と合わせて、監査を実施する。 	責任ある立場の者が、個人データの取扱状況について、定期的に点検を行う。
Ⅳ人的安全管理措置 従業員の教育	<ul style="list-style-type: none"> 個人データの取扱いに関する留意事項について、従業員に定期的な研修等を行う。 個人データについての秘密保持に関する事項を就業規則等に盛り込む。 	同左

V 物理的安全管理措置		
①個人データを取り扱う区域の管理	<p>(管理区域の管理手法の例)</p> <ul style="list-style-type: none"> ・ 入退室管理および持ち込む機器等の制限等 ・ なお、入退室管理の方法としては、ICカード、ナンバーキー等による入退室管理システムの設置等が考えられる。 <p>(取扱区域の管理手法の例)</p> <ul style="list-style-type: none"> ・ 壁または間仕切り等の設置、座席配置の工夫、のぞき込みを防止する措置の実施等による、権限を有しない者による個人データの閲覧等の防止 	個人データを取り扱うことのできる従業者および本人以外が容易に個人データを閲覧等できないような措置を講ずる。
②機器および電子媒体等の盗難等の防止	<ul style="list-style-type: none"> ・ 個人データを取り扱う機器、個人データが記録された電子媒体または個人データが記載された書類等を、施錠できるキャビネット・書庫等に保管する。 ・ 個人データを取り扱う情報システムが機器のみで運用されている場合は、当該機器をセキュリティワイヤー等により固定する。 	同左
③電子媒体等を持ち運ぶ場合の漏えい等の防止	<ul style="list-style-type: none"> ・ 持ち運ぶ個人データの暗号化、パスワードによる保護等を行った上で電子媒体に保存する。 ・ 封緘、目隠しシールの貼付けを行う。 ・ 施錠できる搬送容器を利用する。 	個人データが記録された電子媒体または個人データが記載された書類等を持ち運ぶ場合、パスワードの設定、封筒に封入し鞆に入れて搬送する等、紛失・盗難等を防ぐための安全な方策を講ずる。
④個人データの削除および機器、電子媒体等の廃棄	<p>(個人データが記載された書類等を廃棄する方法の例)</p> <ul style="list-style-type: none"> ・ 焼却、溶解、適切なシュレッダー処理等の復元不可能な手段を採用する。 <p>(個人データを削除し、または、個人データが記録された機器、電子媒体等を廃棄する方法の例)</p> <ul style="list-style-type: none"> ・ 情報システム(パソコン等の機器を含む。)において、個人データを削除する場合、容易に復元できない手段を採用する。 ・ 個人データが記録された機器、電子媒体等を廃棄する場合、専用のデータ削除ソフトウェアの利用または物理的な破壊等の手段を採用する。 	個人データを削除し、または、個人データが記録された機器、電子媒体等を廃棄したことを、責任ある立場の者が確認する。
VI 技術的安全管理措置		
①アクセス制御	<ul style="list-style-type: none"> ・ 個人情報データベース等を取り扱うことのできる情報システムを限定する。 ・ 情報システムによってアクセスすることのできる個人情報データベース等を限定する。 ・ ユーザーIDに付与するアクセス権により、個人情報データベース等を取り扱う情報システムを使用できる従業者を限定する。 	個人データを取り扱うことのできる機器および当該機器を取り扱う従業者を明確化し、個人データへの不要なアクセスを防止する。
②アクセス者の識別と認証	<p>(情報システムを使用する従業者の識別・認証手法の例)</p> <ul style="list-style-type: none"> ・ ユーザーID、パスワード、磁気・ICカード等 	機器に標準装備されているユーザー制御機能(ユーザーアカウント制御)により、個人情報データベース等を取り扱う情報システムを使用する従業者を識別・認証する。

③外部からの不正アクセス等の防止	<ul style="list-style-type: none"> ・情報システムと外部ネットワークとの接続箇所にファイアウォール等を設置し、不正アクセスを遮断する。 ・情報システムおよび機器にセキュリティ対策ソフトウェア等（ウイルス対策ソフトウェア等）を導入する。 ・機器やソフトウェア等に標準装備されている自動更新機能等の活用により、ソフトウェア等を最新状態とする。 ・ログ等の定期的な分析により、不正アクセス等を検知する。 	<ul style="list-style-type: none"> ・個人データを取り扱う機器等のオペレーティングシステムを最新の状態に保持する。 ・個人データを取り扱う機器等にセキュリティ対策ソフトウェア等を導入し、自動更新機能等の活用により、これを最新状態とする。
④情報システムの使用に伴う漏えい等の防止	<ul style="list-style-type: none"> ・情報システムの設計時に安全性を確保し、継続的に見直す（情報システムのぜい弱性を突いた攻撃への対策を講ずることも含む）。 ・個人データを含む通信の経路または内容を暗号化する。 ・移送する個人データについて、パスワード等による保護を行う。 	<ul style="list-style-type: none"> ・メール等により個人データの含まれるファイルを送信する場合には、当該ファイルへのパスワードを設定する。

(3) 従業者及び委託先の監督措置

前述の通り、個人情報取扱事業者は、個人データの安全管理のためにその従業者及び委託先に対して必要かつ適切な監督を行わなければならない(改正法第21条及び第22条)。

(ア) 従業者

ガイドラインでは、個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況(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、個人データを取り扱う従業者に対する教育、研修等の内容及び頻度を充実させるなど、必要かつ適切な措置を講ずることが望ましいとしており、個人データの安全管理に関し従業者に対する研修等を実施すると共に、従業者による内部規程の遵守状況につき随時監査・確認を行うなどの対応が必要となる。

なお、「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者等をいい、雇用関係にある従業員(正社員、契約社員、嘱託社員、パート社員、アルバイト社員等)のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれるものとされている。

(イ) 委託先

ガイドラインでは、委託先については、委託先において当該個人データについて安全管理措置が適切に講じられるよう、委託先に対し必要かつ適切な監督をしなければならないものとし、具体的には、個人情報取扱事業者は、改正法第20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講じられるよう、監督を行うものとしている。また、委託する業務内容に対して必要のない個人データを提供しないようにすると共に、取扱いを委託する個人データの内容を踏まえ、個人データが漏えい等をした場合に本人が被る権利利益の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、以下に掲げる措置を講じなければならないものとしている。

(A) 適切な委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法及びガイドラインで委託元に求められるものと同等であることを確認するため、安全管理措置の各項目(上記3.(2)参照)が委託する業務内容に沿って確実に実施されることについて、あらかじめ確認しなければならないものとしている。

(B) 委託契約の締結

また、委託契約には、当該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として委託元、委託先双方が同意した内容とともに、委託先における委託された個人データの取扱状況を委託元が合理的に把握することを盛り込むことが望ましいものとしている。

(C) 委託先における個人データ取扱状況の把握

また、委託先における委託された個人データの取扱状況を把握するために、定期的に監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、委託の内容等の見直しを検討することを含め、適切に評価することが望ましいものとしている。

従って、個人情報取扱事業者としては、委託先の選定の際に確認すべき項目についてのルールを定めた上で、それに従い委託先を選定すると共に、委託先との契約上、一定の状況把握が可能となる条項を織り込み、それに基づき委託先における個人データの取扱い状況を把握し、問題があれば改善の対応が行える態勢を整える必要がある。

(4) 第三者提供関連の対応

(ア) 共同利用

前述の通り、個人情報取扱事業者が個人データを第三者に提供するには、原則として、事前の本人

の同意が必要とされる(改正法第23条第1項)ところ、委託、合併等、共同利用に伴う提供については第三者提供にあたらないものとされている(改正法第23条第5項)。このうち共同利用(改正法第23条第5項第3号)^{注5}については、特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いている必要があるものとされている。従って、個人データの共同利用が想定される場合には、共同利用の範囲について検討した上で、共同利用の範囲等が本人に通知又は本人が容易に知り得るようにする必要がある。

(イ) 利用目的における第三者提供に関する記載

あらかじめ、個人情報を第三者に提供することが想定される場合には、利用目的において、その旨を特定しなければならない。従って、グループ会社間で個人データを提供することが想定される場合などについては、上記3.(1)で定めた利用目的において、その旨を定めなければならない。

(ウ) オプトアウトによる第三者提供

前述のオプトアウトによる第三者提供を行う事業者については、あらかじめ、一定の事項につき、本

注5

共同利用の具体的な例として、ガイドラインでは、①グループ企業で総合的なサービスを提供するために取得時の利用目的の範囲内で情報を共同利用する場合、②親子兄弟会社の間で取得時の利用目的の範囲内で個人データを共同利用する場合、③使用者と労働組合又は労働者の過半数を代表する者との間で取得時の利用目的の範囲内で従業員の個人データを共同利用する場合を挙げている。

注6

ここで「本人が容易に知り得る状態」とは、事業所の窓口等への書面の掲示・備付けやホームページへの掲載その他の継続的方法により、本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態をいい、事業の性質及び個人情報の取扱状況に応じ、本人が確実に認識できる適切かつ合理的な方法によらなければならない(改正後に適用となる個人情報の保護に関する施行規則第7条第1項第2号)とされ、ガイドラインではその具体例として、①本人が閲覧することが合理的に予測される個人情報取扱事業者のホームページにおいて、本人が分かりやすい場所(例:ホームページのトップページから1回程度の操作で到達できる場所等)に法に定められた事項を分かりやすく継続的に掲載する場合、②本人が来訪することが合理的に予測される事務所の窓口等への掲示、備付け等が継続的に行われている場合、③本人に頒布されている定期刊行物への定期的掲載を行っている場合、④電子商取引において、商品を紹介するホームページにリンク先を継続的に表示する場合を挙げている。「本人が容易に知り得る状態」について具体的な定めが置かれているのはオプトアウトによる第三者提供の場面のみであるが、他の場面で本人が容易に知り得る状態に置くことが求められている場合についてもこれに準ずる形で対応することとなる。

人に通知し、又は本人が容易に知り得る状態^{注6}に置く態勢を整えるとともに、個人情報保護委員会に届け出る必要がある。

(エ) 第三者提供に関する記録の整備

また、第三者提供を行う事業者、第三者提供を受ける事業者については、前述の第三者提供に関する記録の整備が必要となる。

(6) 保有個人データに関する対応態勢整備

前述の通り、個人情報取扱事業者は、本人から求められたときに、保有個人データの利用目的を通知し、本人に対し保有個人データを開示し、また、内容の訂正、利用停止等を行うなどの対応が必要になる。保有個人データに関する対応についての担当部署を定め、対応手順についてのルールを定めておく必要がある。

また、個人情報取扱事業者は、保有個人データについて、以下の情報を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とされているため、これに対する対

応が必要となろう。

- ①個人情報取扱事業者の氏名又は名称
- ②全ての保有個人データの利用目的
- ③保有個人データの利用目的の通知の求め又は開示等の請求に応じる手続及びこれらに係る手数料の額(定めた場合に限る。)
- ④保有個人データの取扱いに関する苦情の申出先

4. 最後に

今回の改正において最も影響が大きいのが、これまで個人情報取扱事業者に該当しないものとして実質的に個人情報保護法の適用外となってきた中小規模事業者に対する適用の拡大である。今般新たに設立された個人情報保護委員会でも、中小規模事業者への広報活動を広く進めており、中小規模事業者向けの説明資料も公開されている(http://www.ppc.go.jp/personal/pr/28_national-briefing_chusho/)。これらの資料も参考しつつ、2017年5月30日の施行までに対応の準備を進められたい。

いのうえ ひろと

1998年東京大学法学部卒業、2000年長島・大野・常松法律事務所入所。2005年Columbia Law Schoolに留学し、LL.M.を取得、2006年London School of Economics and Political ScienceにてLLM Banking Law and Financial Regulationを取得、2006年に帰国。2010年から2013年まで東京大学法学部非常勤講師。

不動産、不動産ファンド、不動産ファイナンス、不動産証券化、J-REIT等の案件を中心として取扱い、ジョイントベンチャー、M&Aについても幅広い経験を有し、日本国内外を問わず、多様な業種のクライアントを代理している。