

個人情報保護に関する法律についての 経済産業分野を対象とするガイドライン (概要)

平成16年10月

経済産業省

商務情報政策局情報経済課

1. 個人情報保護法の哲学 ～ 効果的な保護のあり方～

予防措置

～ あらかじめ利用目的を公表しておくこと、等

IT社会では、一旦流出した個人情報回収は不可能。
(一方で、情報は利用されなければ意味がない。)
被害の推定も困難。

事後規制ではなく、事前規制。

個人情報の性質を問わない

インターネット社会の特徴！ ~ データ化された個人情報は蓄積、流通、加工・編集が容易。

個人情報は相互に結びつけば(マッチングにより)いくらでもセンシティブになる！

医療情報、預貯金、犯罪歴など特定の情報さえ漏れなければOK、という認識は過去のもの！

IT社会においては、個人を特定できる情報は、全て「注意を払うべき個人情報」として取り扱う必要がある。

大量の個人情報は、コンピュータ等を用いてデータベース化されることによって、マッチングされる可能性(リスク)が飛躍的に高まる。

透明性と市場メカニズムの尊重

消費者が持つ「不安」をどのように解消するか。
今後益々高まっていく「個人情報の有用性」の芽を
規制によって摘まないためにどうするか。

< 透明性 >

利用目的の公表等で、個人(消費者)の予見可能性の向上。

< 市場メカニズムの尊重 >

利用目的の内容の是非は市場の判断に委ねる。

保護と利用のバランス

保護

利用目的の通知又は公表
セキュリティの確保
第三者提供の制限
本人関与・苦情処理

目的外利用を制限するとともに、十分なセキュリティの確保を義務付けることにより、消費者の不安を払拭する。

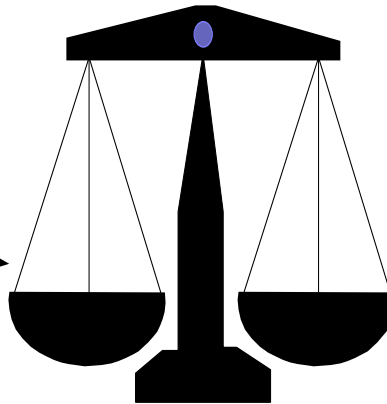
個人の権利利益を保護

利用

利用目的自体に制限無し
取得時は本人の同意不要

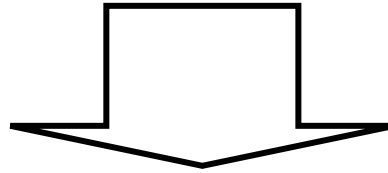
利用目的を対外的に明らかにすることにより不適切な利用を排除する。

個人情報 の有用性に配慮



自主的な取組の推進

法律では、あくまで必要最小限のルールを規定



事業の性質、個人情報取扱い状況等を踏まえ、業界団体及び各事業者はより適切な個人情報の保護が望まれる。

2. 個人情報保護法及びガイドラインの概要

基本方針を閣議決定

個人情報保護法の施行(平成17年4月1日)に向けて、同法第7条に基づく「個人情報の保護に関する基本方針」が閣議決定(4月2日)。

ただし、基本方針の性格は、各省共通に行うべき取り組み等について定めるものであり、個々の業界、事業者が具体的にどのような対応を行えばよいかについては、基本的な枠組みの提示にとどまっている。

具体的なマニュアルの必要性

企業が対応を行う際の参考となるような、分かりやすいマニュアルの作成が必要。

経済産業省では、当省の所管業種における個人情報保護法の適用をまとめた、「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」を策定。

- * ガイドラインの策定にあたっては、ガイドライン検討委員会(委員長・堀部政男 中央大学法科大学院教授)において、検討をいただいた。

1. 事業者の取組を支援するための具体的指針

基本方針及び個人情報保護法第8条に基づき、経済産業省所管の事業者等が個人情報の適正な取扱いを確保するために行う取組を支援するための具体的指針として策定。

2. 具体的な事例を掲載

個人情報保護法に関する対応を行うに際して具体的なイメージが持てるよう、参考事例を掲載。事例については、法のルールに適合している例と違反している例の双方について記述し、事業者が具体的にどのような対応を行えば良いのか分かるような工夫を行った。

3. 従業員の個人情報の取扱いについて

経済産業省所管の事業者等が、個人情報保護法に関する対応について全て理解できるようにするため、従業員の個人情報に関する部分も記述。従業員の個人情報の取扱いの部分については、厚生労働大臣と経済産業大臣の共同で作成を行った。

4. 行政の透明性の確保

「勧告」「命令」及び「緊急命令」については、個人情報取扱事業者が、本ガイドラインで、「しなければならない」と明記したものについて、必要な措置を講じたか否かを基に判断して行うこととし、行政の透明性の確保を図った。

法律で用いられている基本的な用語の定義とその具体的事例を示す。

1 - 1 個人情報 (ガイドライン2頁~)

法第2条第1項 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。

ガイドライン

氏名、性別、生年月日等に限られず、個人の身体、財産、職種、肩書き等の属性に関して、**事実、判断、評価を表す全ての情報**であり、評価情報、公刊物等によって**公にされているもの**や、**映像、音声も含まれ**、暗号化されているかどうかを問わない。
「生存する個人」は日本国民に限られず、外国人も含まれるが、法人その他の団体は「個人」に該当しないため、法人等の団体に関する情報は含まれない(ただし、役員、従業員等に関する情報は個人情報)。

【個人情報に該当する事例】

- ・防犯カメラに記録された情報など本人が判別できる映像情報
- ・特定の個人を識別できるメールアドレス情報(keizai_ichiro@meti.go.jpなどのようにメールアドレスだけの情報の場合であっても、日本の政府機関である経済産業省に所属するケイザイイチローのメールアドレスであることがわかるような場合等)。
- ・官報、電話帳、職員録等で公にされている情報(本人の氏名等)

【個人情報に該当しない事例】

- ・企業の財務情報等、法人等団体そのものに関する情報(団体情報)
- ・記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報(例えば、abc012345@ispisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。)
- ・特定の個人を識別することができない統計情報

法第2条第2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

ガイドライン

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物
コンピュータを用いなくても、カルテや指導要録など、紙面で処理した個人情報を一定の規則(例えば、五十音順、年月日順等)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

【個人情報データベース等に該当する事例】

- ・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、他の従業員等によっても検索できる状態にしている場合
- ・氏名、住所、企業別に分類整理されている市販の人名録

【個人情報データベース等に該当しない事例】

- ・従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いているが、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
- ・アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

法第2条第3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。

一～五 (略)

ガイドライン

国の機関、地方公共団体、独立行政法人以外で、取り扱う個人情報の量及び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者(1)を除いた、個人情報データベース等を事業の用に供している者。

- 1: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(2)の合計が過去6ヶ月以内のいずれの日においても5000人を超えない者。
- 2:事業の用に供する個人情報データベース等が、
他人の作成によるもので、
氏名、住所又は電話番号のみを含んでおり、
新たに個人情報を加えたり、他の個人情報を付加したりして、データベースそのものを変更するようなことをしない場合は、その個人情報データベース等に含まれる個人の数、上記 1の「特定の個人の数」には算入しない。

【特定の個人の数に算入しない事例】

- ・電話会社より提供された電話帳および市販の電話帳CD-ROM等に掲載されている氏名及び電話番号
- ・市販のカーナビゲーションシステム等のナビゲーションシステムに格納されている氏名、住所又は居所の所在場所を示すデータ

【事業の用に供しないため特定の個人の数に算入しない事例】

- ・倉庫業、データセンター(ハウジング、ホスティング)等の事業において当該情報が個人情報に該当するかどうかを認識することなく預かっている場合に、その情報中に含まれる個人情報

法第2条第4項 この法律において「個人データ」とは、個人情報データベース等を構成する個人情報をいう。

法第2条第5項 この法律において「保有個人データ」とは、個人情報取扱事業者が、開示、内容の訂正、追加又は削除、利用の停止、消去及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であって、その存否が明らかになることにより公益その他の利益が害されるものとして政令で定めるもの又は1年以内の政令で定める期間以内に消去することとなるもの以外のものをいう。

ガイドライン

「個人データ」とは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報という。

【個人データに該当する事例】

- ・個人情報データベース等から他の媒体に格納したバックアップ用の個人情報
- ・コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

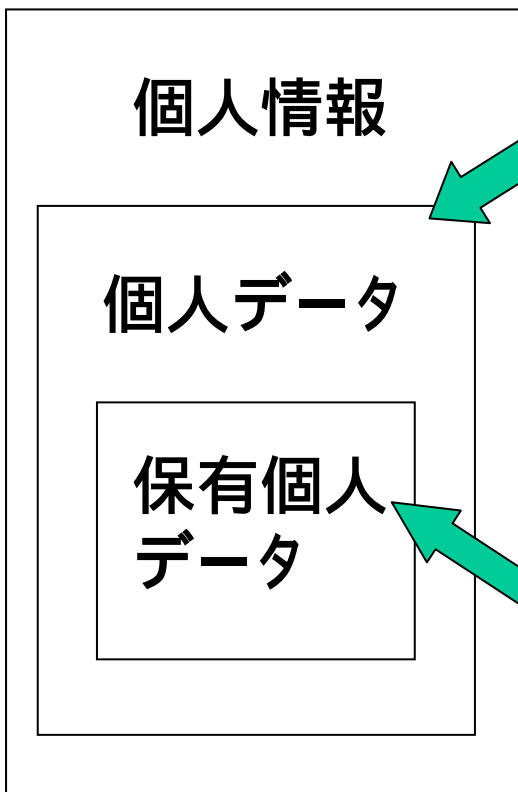
【個人データに該当しない事例】

- ・個人情報データベース等を構成する前の入力帳票に記載されている個人情報

ガイドライン

「保有個人データ」とは、個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する「個人データ」をいう。

個人情報取扱事業者が個人データを受託処理している場合で、その個人データについて、何ら取決めがなく、自らの判断では本人に開示等を行うことができないときは、本人に開示等の権限を有しているのは委託者であって、受託者ではない。



2. 個人情報取扱事業者の義務

法第15条から法第36条に個人情報取扱事業者の義務が定められている。事業者が具体的に対応を行う際に、事業者が分かりやすいように、本ガイドラインで、具体的な事例とともに示す。

1. 利用目的による制限等

利用目的をできる限り特定しなければならない。(第15条)

利用目的の達成に必要な範囲を超えて取り扱ってはならない。(第16条)

2. 適正な取得、正確性の確保、安全管理措置等

偽りその他不正の手段により取得してはならない。(第17条)

取得したときは利用目的を通知又は公表しなければならない。(第18条)

正確かつ最新の内容に保つよう努めなければならない。(第19条)

安全管理のために必要な措置を講じなければならない。(第20条)

漏えい時の被害・事業の性質・リスクに応じた、必要かつ適切な措置であること
従業員・委託先に対し必要な監督を行わなければならない。(第21、22条)

3. 第三者提供の制限

本人の同意を得ずに第三者に提供してはならない。(第23条)

例外：オプトアウト(本人の求めに応じて提供を停止できることとしている場合)

4. 本人の関与

利用目的等を本人の知り得る状態に置かなければならない。(第24条)

本人の求めに応じて保有個人データを開示・訂正・利用停止等を行わなければならない。(第25条～第27条)

5. 苦情の処理

苦情の適切かつ迅速な処理に努めなければならない。(第31条)

個人情報全般
が対象

個人情報のうち
「個人データ」
(データベース化
された情報)
が対象

保有個人データ
が対象

* 各義務規定には適宜除外事由あり

法第15条第1項 個人情報取扱事業者は、**個人情報を取り扱うに当たっては、その利用の目的(以下「利用目的」という。)をできる限り特定**しなければならない。

第2項 個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると合理的に認められる範囲を超えて行ってはならない。

ガイドライン

利用目的の特定に当たっては、利用目的を単に抽象的、一般的に特定するのではなく、個人情報取扱事業者において**最終的にどのような目的で個人情報を利用するかを可能な限り具体的に特定**する必要がある。

「 事業()における商品の発送、新商品情報のお知らせ、関連するアフターサービス」等を利用目的とすることが挙げられる。単に「当社の事業活動」、「お客様のサービスの向上」等を利用目的とすることは、できる限り特定したことにはならない。

「 事業」の特定に当たっては、社会通念上、本人から見て合理的に予想できる程度に特定することが望ましい。例えば、日本標準産業分類の中分類から小分類程度の分類が参考になる。

【具体的に利用目的を特定している事例】

- ・「 事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします。」
- ・「ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります。」
- ・情報処理サービスを行っている事業者の場合であれば、「給与計算処理サービス、あて名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために、委託された個人情報を取り扱います。」のようにすれば利用目的を特定したことになる。

【具体的に利用目的を特定していない事例】

- ・「事業活動に用いるため」、「提供するサービスの向上のため」、「マーケティング活動に用いるため」

法第18条第1項 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、**本人に通知し、又は公表**しなければならない。

第2項 個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面(中略)に記載された当該本人の個人情報を取得する場合その他**本人から直接書面に記載された当該本人の個人情報を取得する場合**は、あらかじめ、本人に対し、その利用目的を明示しなければならない。(以下略)

ガイドライン

個人情報取扱事業者は、個人情報を取得する場合は、**あらかじめその利用目的を公表**していることが望ましい。公表していない場合は、**取得後速やかに、その利用目的を、本人に通知するか、又は公表**しなければならない。

【本人に通知又は公表が必要な事例】

- ・インターネット、官報、職員録等から個人情報を取得する場合
- ・個人情報の第三者提供を受ける場合

個人情報取扱事業者は、書面等による記載、ユーザー入力画面への打ち込み等により、**直接本人から個人情報を取得する場合**には、あらかじめ、本人に対し、その利用目的を明示しなければならない。なお、口頭による個人情報の取得にまで、当該義務を課すものではない。

【あらかじめ、本人に対し、その利用目的を明示しなければならない場合】

- ・申込書・契約書に記載された個人情報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
- ・懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

法第20条 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、滅失又はき損の防止その他の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。

ガイドライン

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、滅失又はき損の防止その他の個人データの安全管理のため、**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、及び技術的な安全管理措置**を講じなければならない。

その際、本人の個人データが漏えい、滅失又はき損等をした場合に**本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ**、必要かつ適切な措置を講じる。(本ガイドラインでは、各安全管理措置を講じる際に望まれる事項を具体的に示した。)

組織的安全管理措置

安全管理について従業者(法第21条参照)の責任と権限を明確に定め、安全管理に対する規程や手順書(以下規程等という)を整備運用し、その実施状況を確認すること。

具体的には、組織体制の整備、規程等の整備と規程等に従った運用、個人データ取扱台帳の整備、評価、見直し及び改善、事故又は違反への対処など。

人的安全管理措置

従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や、教育・訓練などの措置。

物理的安全管理措置

入退館(室)の管理、個人データの盗難の防止対策、機器・装置等の物理的な保護などの措置。

技術的安全管理措置

個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視など、個人データに対する技術的な安全管理措置。

具体的には、アクセスにおける識別と認証、アクセス権限の管理、アクセスの記録、情報システムに対する不正ソフトウェア対策、移送・通信時の対策、情報システムの動作確認、情報システムの監視など。

法第21条 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

ガイドライン

個人情報取扱事業者は、法第20条に基づく安全管理措置を遵守させるよう、従業者に対し必要かつ適切な監督をしなければならない。

「**従業者**」とは、個人情報取扱事業者の組織内において**直接間接に事業者の指揮監督を受けて事業主の業務に従事している者**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。

安全管理措置の一環として従業者をビデオ及びオンラインによるモニタリングを実施する場合についての留意点についても記述。

【従業者に対して必要かつ適切な監督を行っていない場合】

- ・従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合
- ・内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

【従業者のモニタリングを実施する上での留意点】

個人データの取り扱いに関する従業者及び委託先の監督、その他安全管理措置の一環として従業者を対象とするビデオ及びオンラインによるモニタリング(以下「モニタリング」という)を実施する場合は、次の点に留意する。等

- ・モニタリングの目的、即ち取得する個人情報の利用目的をあらかじめ特定し、社内規程に定めるとともに、従業者に明示すること。
- ・モニタリングの実施に関する責任者とその権限を定めること。
- ・モニタリングを実施する場合には、あらかじめモニタリングの実施について定めた社内規程案を策定するものとし、事前に社内に徹底すること。
- ・モニタリングの実施状況については、適正に行われているか監査、又は確認を行うこと。

法第22条 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

ガイドライン

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合、法第20条に基づく安全管理措置を遵守させるよう、受託者に対し必要かつ適切な監督をしなければならない。

「必要かつ適切な監督」には、委託契約において、当該個人データの取扱いに関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を**契約に盛り込む**とともに、**同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認**することも含まれる。なお、**優先的地位にある者**が委託者の場合、受託者に**不当な負担を課すことがあってはならない**。

委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意する。

【受託者に必要かつ適切な監督を行っていない場合】

- ・個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者に委託した場合で、受託者が個人データを漏えいした場合。
- ・個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合。
- ・再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱い状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合。

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

- 委託者及び受託者の責任の明確化
- 個人データの安全管理に関する事項
 - ・個人データの漏えい防止、盗用禁止に関する事項
 - ・委託契約範囲外の加工、利用の禁止
 - ・委託契約範囲外の複写、複製の禁止
 - ・委託契約期間
 - ・委託契約終了後の個人データの返還・消去・廃棄に関する事項
- 再委託に関する事項
 - ・再委託を行うに当たっての委託者への文書による報告
- 個人データの取扱い状況に関する委託者への報告の内容及び頻度
- 契約内容が遵守されていることの確認(例えば、情報セキュリティ監査なども含まれる。)
- 契約内容が遵守されなかった場合の措置
- セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

第23条第1項 個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。 一～四(略)

第2項 個人情報取扱事業者は、第三者に提供される個人データについて、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、次に掲げる事項について、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ときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。 一～四(略)

ガイドライン

個人情報取扱事業者は、あらかじめ、**本人の同意**を得ないで、個人データを第三者に提供してはならない。同意の取得に当たっては、事業の性質及び個人データの取扱い状況に応じ、本人が同意に係る判断を下すために必要と考えられる合理的かつ適切な範囲の内容を明確に示すこと。

【第三者提供とされる事例】

- ・親子兄弟会社、グループ会社の間で個人データを交換する場合
- ・フランチャイズ組織の本部と加盟店の間で個人データを交換する場合
- ・同業者間で、特定の個人データを交換する場合
- ・外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】

- ・同一事業者内で他部門へ個人データを提供すること。

個人情報取扱事業者は、第三者提供におけるオプトアウトを行っている場合には、本人の同意なく、個人データを第三者に提供することができる。

「**第三者提供におけるオプトアウト**」とは、提供にあたりあらかじめ、以下の . . . の情報を、本人に通知し、又は本人が容易に知り得る状態に置いておくとともに、本人の求めに応じて第三者への提供を停止することをいう。

- ・第三者への提供を利用目的とすること。
- ・第三者に提供される個人データの項目
- ・第三者への提供の手段又は方法
- ・本人の求めに応じて第三者への提供を停止すること。

【オプトアウトの事例】

- ・住宅地図業者(表札や郵便受けを調べて住宅地図を作成し、販売(不特定多数への第三者提供))
- ・データベース事業者(ダイレクトメール用の名簿等を作成し、販売)

法第23条第4項 次に掲げる場合において、当該個人データの提供を受ける者は、前3項の規定の適用については、第三者に該当しないものとする。

第1号 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託する場合。

第3号 個人データを特定の者との間で共同して利用する場合であって、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とき。

ガイドライン

委託

個人データの取扱いに関する業務の全部又は一部を委託する場合は、第三者に該当しない。個人情報取扱事業者には、委託先に対する監督責任が課される(法第22条関連)。

【業務の委託の事例】

- ・データの打ち込み等、情報処理を委託するために個人データを渡す場合
- ・百貨店が注文を受けた商品の配送のために、宅配業者に個人データを渡す場合

共同利用

個人データを特定の者との間で共同して利用する場合、以下のア)～エ)の情報を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おくとともに、共同して利用することを明らかにしている場合は、第三者に該当しない。

ア)共同して利用される個人データの項目

イ)共同利用者の範囲(本人からみてその範囲が明確であることを要するが、範囲が明確である限りは、必ずしも個別列挙が必要ない場合もある。)

ウ)利用する者の利用目的(共同して利用する個人データのすべての利用目的)

エ)開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等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

【共同利用を行うことがある事例】

- ・グループ企業で総合的なサービスを提供するために利用目的の範囲内で情報を共同利用する場合

法第24条第1項 個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、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。個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。一～四(略)

法第25条第1項 個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの開示(当該本人が識別される保有個人データが存在しないときにその旨を知らせることを含む。以下同じ。)を求められたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。(以下略)

法第26条第1項 個人情報取扱事業者は、本人から、当該本人が識別される保有個人データの内容が事実でないという理由によって当該保有個人データの内容の訂正、追加又は削除(以下この条において「訂正等」という。)を求められた場合には、(中略)利用目的の達成に必要な範囲内において、遅滞なく必要な調査を行い、その結果に基づき、当該保有個人データの内容の訂正等を行わなければならない。

法第27条第1項 個人情報取扱事業者は、本人から、当該本人が識別される保有個人データが第16条の規定に違反して取り扱われているという理由又は第17条の規定に違反して取得されたものであるという理由によって、当該保有個人データの利用の停止又は消去(以下この条において「利用停止等」という。)を求められた場合であって、その求めに理由があることが判明したときは、違反を是正するために必要な限度で、遅滞なく、当該保有個人データの利用停止等を行わなければならない。

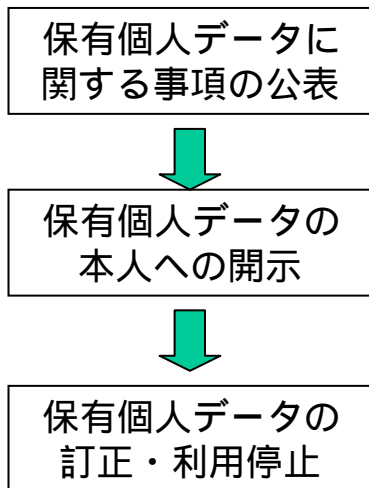
ガイドライン

個人情報取扱事業者は、保有個人データについて、一定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。

個人情報取扱事業者は、**本人から、自己が識別される保有個人データの開示(存在しないときにはその旨を知らせることを含む。)**を求められたときは、本人に対し、書面の交付による方法(開示の求めを行った者が同意した方法があるときはその方法)により、遅滞なく、当該保有個人データを開示しなければならない。

個人情報取扱事業者は、本人から、**保有個人データに誤りがあり、事実でないという理由によって訂正等を求められた場合**には、原則として、訂正等を行い、訂正等を行った場合には、その内容を本人に対し、遅滞なく通知しなければならない。

個人情報取扱事業者は、本人から、**手続違反の理由により保有個人データの利用停止等が求められた場合**には、原則として、当該措置を行わなければならない。なお、利用の停止等を行った場合には、遅滞なく、その旨を本人に通知しなければならない。



3 - 1 経過措置 (53頁)

ガイドライン

法施行前から保有している個人情報については、法施行時に個人情報の取得行為がなく、法第18条(取得に際しての利用目的の通知等)の規定は適用されない。

保有個人データに関する事項の本人への周知については、法施行時に法第24条第1項の措置(前ページ参照)を講ずる必要がある。

3 - 2 ガイドラインの見直し (56頁)

ガイドライン

個人情報の保護についての考え方は、社会情勢の変化、国民の認識の変化、技術の進歩等に応じて変わり得るものであり、本ガイドラインは、法の施行後の状況等諸環境の変化を踏まえて毎年見直しを行うよう努めるものとする。

3 - 3 参考となる事項・規格 (56頁～)

ガイドライン

個人情報取扱事業者は、その事業規模及び活動に応じて、個人情報の保護のためのコンプライアンス・プログラムを策定し、実施し、維持し及び改善を行うことが望ましい。

なお、その体制の整備に当たっては、日本工業規格 JISQ15001「個人情報保護に関するコンプライアンス・プログラムの要求事項」を、個人データの安全管理措置の実施に当たっては、日本工業規格 JISX5070「セキュリティ技術 - 情報技術セキュリティの評価基準」及び日本工業規格 JISX5080「情報セキュリティマネジメントの実践のための規範」等を参考にすることができる。

また、個人情報取扱事業者は、「個人情報保護に関する考え方や方針に関する宣言(いわゆる、プライバシーポリシー、プライバシーステートメント等)」を策定し、ウェブ画面への掲載等により公表することが望ましい。

(参考) 諸外国及び我が国の取組み

< OECDプライバシーガイドライン8原則 (1980年) >

収集制限の原則

適法・公正な手段により、必要な場合には情報主体に通知又は同意を得て収集されるべき。

データ内容の原則

利用目的に沿ったもので、かつ、正確、完全、最新であるべき。

目的明確化の原則

収集目的を明確にし、データ利用は収集目的に合致するべき。

利用制限の原則

データ主体の同意がある場合、法律の規定による場合以外は目的外に利用してはならない。

安全保護の原則

合理的安全保護措置により、紛失・破壊・不正な使用・改竄・漏洩等から保護するべき。

公開の原則

データ収集の実施方針等を公開し、データの存在、利用目的、管理者等を明示するべき。

個人参加の原則

自己に関するデータの所在及び内容を確認させ、又は異議申立を保障するべき。

責任の原則

管理者は諸原則実施の責任を有する。

EU諸国は官民を対象とする包括的な個人情報保護法を保有。

個人情報保護に係るEU指令(1998年発効)

EU加盟国に対し、EU指令に基づき国内法を改正することを義務付けた。

個人情報の取得には本人からの明示の同意が必要。

企業はその取り扱う個人情報のリストを個人情報保護機関に登録しなければならない。

直罰によって担保

欧州型の理念的な法律は実施困難。
まともに適用すれば大半の企業が違法状態になる！

第三国条項(EU指令第25条)

EU加盟国と同等の個人情報保護が図られていない国には、個人データの移転を禁止することができる。

プライバシー法(1974年：公的分野のみを対象)

その他、こどものオンラインプライバシー保護法、公正信用報告法などの個別分野での法の整備
(1980年～1990年代)

- ・民間分野の包括的な保護法制は存在しない。
- ・事業者の自主的な取組を重視。

米国型のパッチワーク方式では、現在生じつつある問題に適切に対処することが出来ない！

(1) 行政機関個人情報保護法制定(昭和63年)

(2) 民間部門の自主的取り組み

通産省ガイドラインの策定(平成元年告示、9年改訂)
プライバシーマーク制度の導入(平成10年) - - - (財)日本情報処理開発協会
日本工業規格(JISQ15001)の制定(平成11年)

(3) 住民基本台帳法改正(平成11年)

改正時に、与党3党合意、小渕元首相国会答弁
(「民間部門も含めて個人情報の保護を図る」)

(4) IT戦略本部で個人情報の保護について議論

個人情報保護検討部会(平成11年)・個人情報保護法制化専門委員会(平成12年)

(5) 個人情報保護法案の作成(平成13年3月)

第151通常国会に提出されるが、継続審議扱いの後、第155臨時国会において廃案。

(6) 個人情報保護法の成立(平成15年5月)

同法案を修正し、第156通常国会に再提出・成立。

個人情報保護法関連資料については、
以下をご参照下さい。

(内閣府)

<http://www5.cao.go.jp/seikatsu/kojin/index.html>

(経済産業省)

http://www.meti.go.jp/policy/it_policy/privacy/privacy.htm