

守るべきことは？ 取るべき対応は？

4月1日 全面施行！ **個人情報保護法とその取組み方**



ご存じのとおり、4月1日より個人情報保護法が全面施行されましたが、まだまだ各社の取組み方には濃淡がみられ、完全に浸透しているとはいいいかねる状況です。そこで今月から2回にわたって、これをテーマに取りあげてみたいと思います。まず今月は法律自体の説明を、来月は雇用の分野との関わり合いについて触れてみます。

個人情報保護法で何が変わったか？

個人情報保護法(以下、保護法)とは、個人の権利、利益を保護するために、「個人情報取扱者」(=この意味は後述)に対し、個人情報を正しく取扱うよう義務付けた法律です。もっとも、個人情報を流出・漏洩させた企業は従来からも責任を問われてきたわけであり、「安全管理を徹底する」という意味では特に目新しいテーマではありません。では何が違うかという、少なくとも次の2点が挙げられます。

1つ目は、「利用目的の特定およびその通知もしくは公表または明示」および「本人からの開示の求めへの対応」が義務付けられたという点があります。逆に言えば個人が企業に対し、自己の個人情報について開示・訂正・削除等を請求する権利を法律が認めたということです。これは企業秘密の管理を考える場面では意識されなかった事項です。

2つ目は、企業秘密については、一般には公知情報(=既に知られている情報)は保護対象から外れますが、保護法の保護対象とするか否かを決めるに際しては公知性の有無は無関係という点です。

- 個人情報と企業秘密との違い -

したがって、安全管理対策さえ整えておけば足りるのであって、その点では従来の企業秘密の管理に大差はないというわけにはいきません。物理的、人的、組織的な体制を整えることは急務です。

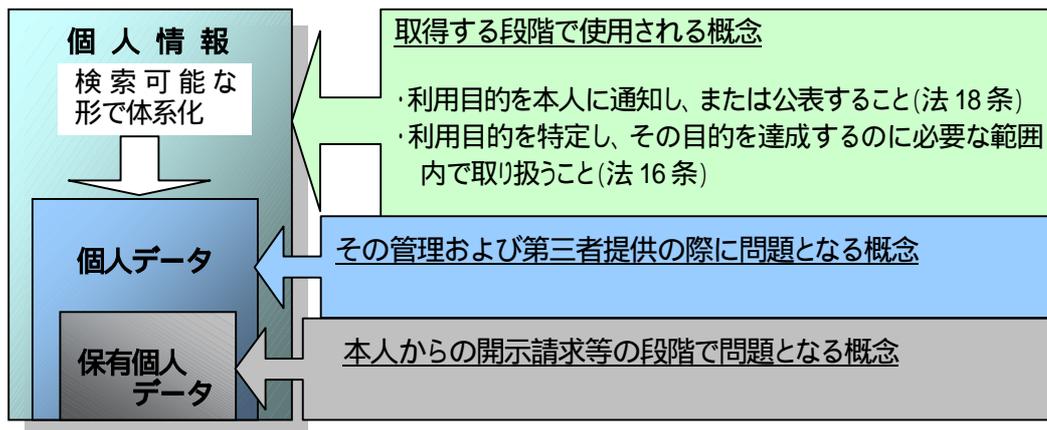
	保護法下の個人情報の取扱	企業秘密の取扱
対象となる情報	公知性の有無と無関係	非公知性の情報に限定
対象となる業者とそのリスク	個人情報取扱業者に限定	▶ 限定しない
	流出等に際しては損害賠償責任、社会的リスクを負う	
本人に対する義務、保護措置	利用目的の特定・通知等、及び開示等請求に対応する義務あり	▶ 左記の義務・規制はなし

個人情報、個人データ、保有個人データ

保護法では、保有している個人情報の情報が、「個人情報」、「個人データ」、「保有個人データ」のどれに該当するかによって義務付けの程度が違います。から の順で概念が狭くなり、なおかつ義務、規制も厳しくなります。

個人情報とは、特定の(生存している)個人を識別できるものをさします。個人データとは、断片的な個人情報を検索可能な状態に整理し、体系化したものをいいます。コンピューターでなくても、紙に記載され、容易に検索できるように整理されたものは、個人データに当たります。保有個人データとは、このうち個人情報取扱業者が開示、訂正等の権限を有し、なおかつ6か月を超えて保有し続けるものをいいます。

たとえば、返信されたアンケートの葉書そのものはまだ「個人情報」ですが、パソコンの中に格納された段階で「個人データ」となります。さらにそれを追加・削除等できる状態で、6か月が経過すると「保有個人データ」になります。保有個人データには、原則として本人からの開示、訂正、削除等請求に応じる義務が課せられます。したがって、不要な個人データはできる限り、6か月以内に消去することが望まれます。



個人情報と同意の要否

従来は、個人情報を取得するのに何の目的で集めるのか、をことわる必要などなかったのですが、今後は、少なくとも個人情報取扱業者であれば、利用目的の特定、明示及び本来の目的の範囲内での利用が義務づけられます。

なお、保護法では個人情報の取得に際して本人の同意を義務付けてはいません。同意を要するのは、本来の目的の範囲を超えて利用する場合です。一方、旧労働省の「行動指針」においては、本人の同意の下での収集が望ましいとされているため、定型化された個人情報については、利用目的と同意を確認する文書や規程を整備しておくに越したことはありません。また本年4月1日(以下、施行日)前に取得した個人情報については、不正な手段によって得たものでなければ、特定の利用目的を公表することで、利用できることになります。したがって、企業が施行日前に取得した個人情報は、施行後速やかに「何のために利用するか」を公表しなければならないということになります。これはホームページによる掲示でもかまいません。

個人データと第三者への提供制限

保護法では、事前に本人の同意を得ないで、個人データを第三者に提供することを禁止(法23条)しています。ここで問題となるのは、相手が提供制限を受ける「第三者」に該当するか否かという点です。整理すると下表のようになります。

第三者に該当 同意が必要	該当しない 同意は不要
・親会社と子会社間での情報交換 ・FC本部と加盟店間との情報交換 ・(ユニオンショップ協定に基づく)労働組合への社員の採用情報の提供 ・健保組合、厚生年金基金からの要請による情報提供 ・出向、転籍等に伴う先方への交渉段階での情報提供	法令に基づく場合、または国等が行う法令に定める事務に協力する場合 生命、財産の保護等のため、本人の同意を得ることが困難な場合 一定の要件下でのグループ内事業の協同利用 委託先への情報の提供 本社と支店間での情報交換 合併、転籍等に伴う情報移転

ただし、～ については当初の利用目的を超えて利用する場合には同意が必要(例えば、雇用管理上の情報を自社の販売部門の対象者名簿として加えるなど)

個人データと監督責任

個人データについては、委託先および従業者(法22条、法21条)に対する監督義務があります。委託先で個人情報が漏れた場合には委託元が責任を問われます。プライバシーマークを取得している業者に発注すれば免責されるわけではありませんが、委託先を選定する判断要素にはなり得ます。また従業者というのは、自社の従業員のみならず役員や派遣社員をさします。保護法の欠点の一つとして情報を持ち出した従業員に対する処罰規定(つまり、直接的な抑止効果)が無い点が挙げられています。そのため尻拭いの多くは支払い能力がある会社が負うことが予想されます。

保有個人データと開示等の例外

保有個人データについては、開示等の義務が課せられます。本人にDM等が送られて来て、自分の情報が悪用されているのではないかと感じた時、事業者に対し情報の開示を求め、訂正や追加、削除を求めること(法25条、法26条)が認められました。

ただし、この場合も例外があり、特に を巡る解釈が争点になりそうです。

本人または第三者の生命、財産等の権利・利益を害するおそれがある場合

当該個人情報取扱業者の業務の適正実施に著しい支障を及ぼすおそれがある場合

他に法令に違反することになる場合

また保有個人データの当否については、施行日から起算されますので、施行日前から保有する個人データについては少なくとも本年9月30日までは、開示等の義務はありません。

個人情報取扱業者の適否とリスク

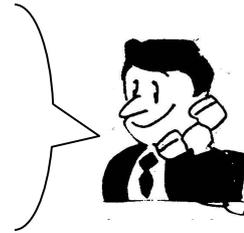
掛金5千件以下ならば、安心できるか？



保護法によって様々な義務や規制が設けられることはわかりましたが、当社のように過去6か月間いずれの月も5千人を超える個人データを持っていない小規模業者は、個人情報取扱業者(以下、取扱業者)に当たらないため、こうした保護法の影響は受けない、と解釈してもよろしいでしょうか？

法の施行に無関心な理由

おっしゃるとおり、この法律の適用を受けるのは、取扱業者に限られています。裏を返せばそれ以外のものは一連の義務や規制を受けないということです。いまだに何の対策を講じていない、無関心な企業、個人事業者が意外と多いというのは、このあたりに原因があるといわれています。ところが、取扱業者に該当するかしないかはあまり意味がないのです。

相手はそうとはとれない！

そもそも開示請求する本人からみて、相手が5千件の個人データを持っているか否かは知る術もなく、法の対象如何によらず、請求してくる可能性が大了。その場合「当社は取扱業者でないので、対応しません」で通用するとは思えません。

発注者もそうとはとれない！

仮に5千件の個人データを持っていなくても、発注者が取扱業者であれば、発注者から安全管理体制が求められるという点もあります。それは受託者に対し監督義務(法22条)があるからです。場合によっては未整備な業者には仕事をさせない、とか契約書に不当な損害賠償額を予定する条項を求めてくることもあり得ます。もっともその内容如何では、独占禁止法第19条の不正取引を禁止する一般指定条項(発注者の優越的地位の濫用)に抵触しかねないので、公正取引委員会も黙ってはいないでしょうし、今後の解釈の確定、裁判例の集積が待たれます。

罰則よりも恐ろしいものとは？

個人情報保護法には、取扱業者に対する罰則がありますが、これも直ちに下されるわけではありません。義務規定違反の疑いにより、監督官庁からの勧告、命令等を受けながらも、それに従わない場合に限ります。それよりも怖いのは、実際に生じた損害に対して賠償責任を負うことであり、顧客の信頼を失うことです。これについては従来の情報流出に伴うリスクと何ら変わりはありません。

今回の個人情報保護法にしる、前回の育児介護休業法にしる、直接的な営業利益に結びつかない対応は自発的に取り組むことが難しいだけに、こうした法律の施行がそのための好機となります。