

個人情報保護法完全施行から 1 年 (2006/4/7)

2005年4月1日に個人情報保護法が完全施行されてから1年が経過しました。現状とその問題点から、ここに要点をまとめます。

現在では、多くの企業が**個人情報保護基本方針**(プライバシーポリシー)を公表するようになりました。個人情報保護基本方針を公表することは、個人情報保護法上の義務として規定されているわけではありませんが、「個人情報の保護に関する基本方針」や、各省庁の出すガイドラインにおいても個人情報保護基本方針の作成・公表を要求するものがあること、個人情報保護法の要求する個人データの安全管理措置(個人情報保護法(以下、「法」)20条)の一環としての組織体制整備(「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」(以下、「ガイドライン」)24頁)の大前提であることから、必要であると判断されたのでしょう。Pマークを取得するには、これを公表する必要があるため、同ルールに従って公表しているという企業もあります。

個人情報の利用目的を公表している企業も多く見られます。個人情報保護法では、本人から直接に書面で個人情報を取得する場合には、原則として、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とされています(法18条2項)。また、直接書面取得以外の口頭での取得や、第三者からの間接的な取得の場合でも、あらかじめその利用目的を公表している場合を除き、原則として、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とされています(法18条1項)。業務受託などに伴って間接的に個人情報を受領する場合にも個人情報の利用目的の公表が必要です。

利用目的はできる限り特定しなければなりません(法15条1項)。総務省統計局が公表している日本標準産業分類の分類を参考にして具体的に記載するべきです。個人情報取扱事業者は、社会通念上、本人が想定することが困難でないと認められる範囲内での利用目的の変更の場合には利用目的の変更が可能です(法15条2項、ガイドライン15頁)、その際には、変更された利用目的について通知又は公表が必要とされています(法18条3項)。そして、この範囲を超えた利用目的の変更については、あらかじめ本人の同意を取る必要があります(法16条1項)。

個人情報保護法の浸透に伴い、個人情報の主体からクレームを申し立てられる恐れもありますから、企業は、個人情報に関する業務フローチャートを作成したうえで、収集する個人情報毎に利用目的を特定し、限定的に記載するように努めるべきです。

安全管理対策について、個人情報保護法は「個人情報取扱事業者は、その取り扱う個人

データの漏洩、滅失、又はき損の防止その他の個人情報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。」としか定めていません(法20条)が、ガイドライン23頁から32頁までに記載される、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、技術的安全管理措置が参考になります。

物理的安全管理対策や技術的安全管理対策については、各企業の中で何らかの対応が取られたケースが多いと思いますが、人的安全管理措置や、組織的安全管理措置については、対応が不十分な企業が多いようです。

個人情報漏洩事故の原因の多くが人為的なミスと内部犯罪や情報持ち出し、盗難であることを考慮すると(筆者著「個人情報保護の法律とリスクと対策がわかる」自由国民社106頁参照)、物理的安全管理措置や技術的安全管理措置と同等以上に、従業員の教育や個人情報取扱手順の規定化や、安全管理措置の評価、見直し及び改善が重要となるはずで

す。

派遣社員との誓約書などを作成する場合、派遣契約においては、派遣先と派遣社員との間に雇用関係が存在しないので、文面に注意しなければなりません。派遣社員に対して、自己の責任により漏洩事故があった場合に損害賠償義務などを確認することは法的に可能であると思われます。

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りません(法22条)。

そのため、個人情報を取り扱う業務を委託する企業は、受託企業に対して個人情報取扱いに関するチェックリストの提出をもとめて十分な保護水準にあることを確認したり、個人情報の取扱いに関する覚書の締結を求めたりすることが多くなりました。

個人情報の委託に関する契約に関して、従来の秘密保持契約書を流用している場合には、その文面が適切かどうかの確認が必要です。

契約書の内容は非常に重要ですから、個人情報保護に詳しい弁護士に相談するか、最低でも、次の4つのポイントを外していないかはチェックすべきです。

1. 利用目的が明確化され、かつ、目的の範囲内でのみ利用しなければならない。

2. 第三者に漏洩しないなどの善管注意義務。
3. 無承諾による再委託の禁止。
4. 開示者が要求した場合の返却又は廃棄。

保有個人データについて、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もので、6ヶ月を超えて保有する個人データ(保有個人データ 法2条5項、政令4条、なお政令3条にも例外あり)は、原則として、当該個人情報取扱事業者の氏名又は名称、利用目的、苦情の申出先、開示訂正等の手続について、本人の知りうる状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければなりません(法24条1項)。

また、保有個人データは、原則として、開示や利用目的の通知を求められた場合には本人に遅滞なく応じなければなりません(法24条2項、25条)。

さらに、利用目的達成に必要な範囲で、内容の訂正、追加又は削除に応じ(法26条)、目的外利用、不適正取得、無断第三者提供の場合には違反を是正するために必要な限度で利用停止又は消去を求めることができます(法27条1項)。

開示の手続については、情報主体に対して手数料を求められますが、正当な理由に基づく訂正や利用停止について費用を請求することはできません。

保有個人データの開示等の申請は、結果を原則として書面で通知する必要があります(法25条1項、政令6条)。また、訂正等を行った場合にもその結果通知が必要です(法26条2項)。そのため、従前から、電話などでこれらの対応を行ってきたクレジットカード会社や通販業者は、従前の簡易な方法をいわゆる「お問い合わせ」として取扱い、「保有個人データの開示等請求」とは区別しているようです。

企業の「お問い合わせ」に対する対応も、本人を名乗る第三者に対して個人情報を漏洩しないように本人確認を行うようになっていきます。具体的には、氏名のほかに住所、生年月日等の登録情報を本人確認のために相手方から聞き出したり、着信電話番号が非通知設定の場合には、コールバックによって登録された電話番号から相手方が電話しているのかを確認したりする対策が取られています。

企業の中には、PマークやTrusteなどのいわゆる**第三者認証**と呼ばれる制度を利用して、適切な個人情報保護を図る体制を作り、それをマーケティングにおける強みとする企業

も増えてきました。

これまで当事務所が扱った事例をみると、Pマークについては概ね申請してから5ヶ月後くらいに現地審査が実施されています。Pマークを取得することによって、組織的安全管理措置として個人情報の取扱いに関する規程の確立、運用、評価・見直し、改善が行えること、Pマークを取得すると同レベルの安全管理体制がある事業者としか個人情報にかかわる取引をすることができなくなること、個人情報にかかるコンプライアンスプログラムの導入によって、業務にもプラスの効果が生じることから、今後もこれらの第三者認証制度は利用が増加するものと思われます。

個人情報保護法完全施行後も、**個人情報漏洩**に関する事故を頻繁に耳にします。したがって、個人情報保護法完全施行によって、特に個人情報漏洩事故が減少したという劇的な効果はないように思います。

かつては、漏洩事故があると商品券などを送付していましたが、小額の弁償はかえって被害者の印象が悪いという統計の結果もあり、最近ではそのような対策ではなく、漏洩事故の事実と原因、今後の漏洩防止対策を説明して本人に謝罪するケースが多いようです。

ただし、平成14年の宇治市住民基本台帳データ漏洩事件の最高裁判決で、1人につき1万円の損害賠償が認められていることを考慮すると、個人情報の管理対策を適切にするとともに、個人情報漏洩保険に加入するなどのリスクヘッジは依然として重要であると思われます。

個人情報保護法の文言の解釈が確立されているとはいいがたく、依然として解釈には幅があります。たとえば名刺は、氏名、勤務先住所、勤務先電話番号などが記載されているので、間違いなく個人情報に該当します。

ガイドライン22頁では「ダイレクトメール等の目的に名刺を用いることは自明の利用目的に該当しない場合があるので注意を要する。」と規定するのみで、結局どのような場面ならば適法で、どのような場面なら違法なのか判然としません。

名刺にはEメールアドレスや役職も記載されるため、これをあいうえお順など検索しやすい順にデータベース化すると個人データに該当します。これを6ヶ月以上保有すれば保有個人データというべきです。個人情報保護法を杓子定規にとらえるならば、各従業員の名刺データベースを管理して、その記載内容をすべて報告することになりますが、これはあまりにも非現実的です。

個人情報保護法が**情報隠しに誤用**されているケースも見られます。個人情報保護法完全施行後は、苦情を申し出た際に担当者の名前を聞くと「個人情報ですのでお答えできません。」と言われたり、また、個人情報保護法は、政治活動、報道の自由との関係では適用ないはずですが、同様に情報を開示したくない場合の隠れ蓑として「個人情報保護法」を持ち出す場合があるようです。

個人情報保護法は、情報漏えいを行った**従業員に対する罰則**を課すべく、現在、政府で改正案が検討され、個人情報を漏えいした民間企業の社員らに対し、懲役1年以下または罰金50万円以下の罰則規定を新設するようです。

現行の個人情報保護法は、個人情報取扱事業者の義務として従業員の適切な監督を要求するのみで、従業員が個人情報保護法の罰則を受けるのは、主務大臣から個人情報の取扱いについて受けた是正命令に違反した場合のみです。

これについて、個人情報を漏洩した従業員自身に、直接に刑事罰を課しないと実効性を欠くのではないかといわれているため、法改正の検討に至ったものと思われます。

個人情報をはじめとする情報を保護しようとする潮流はますます強くなっていますが、情報漏えいのリスクも、より大きくなっていくことが考えられます。自衛のためにも、個人情報の保護について十分な対策を立てるとともに、安全管理の体制を常に見直していくことが求められています。