

Q1 企業において個人番号の収集が必要になる ケースにはどのようなものがありますか。

給与所得の源泉徴収票・給与支払報告書や健康保険関連の書類など法令や条例で定められた書類に個人番号を記載する必要があるため、パートやアルバイトなど非正規雇用の従業員も含め、番号の提供を受ける必要があります。収集した個人番号は雇用契約の終了後は速やかに削除する必要がありますが、「扶養控除等申告書」の提出を受けた事業者は7年間の申告書保存義務があるため、その期間中に再度雇用契約を結ぶ場合には、記録していた個人番号を再利用することができます。

人材派遣会社の場合、登録型派遣では、登録者の派遣先が決まり雇用契約を締結する時点で個人番号の提供を受けることが望ましいのですが、実務を効率よく行うために、給与支給条件等を決めるなどしている場合は、登録時点で個人番号を取得してよいという判断が示されています。

そのほか、研修の講師などに謝礼を支払う場合、「報酬、料金、契約金及び賞金の支払調書」の提出が必要となり、個人番号を記入する必要があります。成りすましを防ぐため、番号の提供を受ける際には、本人確認が必須とされています。全住民に配られる通知カードで番号を確認する場合には、運転免許証等の確認も法律で求められていますので、本人と対面する際に確認できるよう、事前に説明しておくといよいでしょう。また、「不動産の使用料等の支払調書」にも支払相手の番号を記入する必要がありますので、契約先が個人オーナーの場合には同様の確認作業が必要となる可能性があります。

従来提出している書類について、国税庁や厚生労働省から公表される新様式の情報を確認しておくといよいでしょう。扶養配偶者の番号確認まで必要となり負担の大きい健康保険・厚生年金保険関係は他の分野から

全ての企業にもたらされる マイナンバー制度のインパクト

マイナンバー制度への対応は行政機関だけでなく、企業においても必要となる。従業員から提供を受けた個人番号を安全に管理する義務が生じ、場合によってはセキュリティ対策の強化や業務フローの変更が求められる。マイナンバー制度がもたらす企業への影響について、みずほ情報総研のコンサルタントが解説する。

Q3 個人番号の収集・管理について、企業には どのような義務や規制が生じるのでしょうか。

マイナンバー法において、個人番号の適切な管理のために必要な措置を講じなければならないことが定められています。個人情報保護法では安全管理措置が義務付けられるのは個人情報取扱事業者ですが、マイナンバー法の場合は、番号を保有する全ての事業者が規制の対象となります。マイナンバー法で定められていない用途で個人番号を取得することは禁じられているため、個人番号の記入が不要な書類に番号が記入され提出された場合は、速やかに削除する必要があります。知らずに番号を収集・保管することへの罰則はありませんが、事業者が不正アクセス等により個人番号を取得したり不正な利益を図る目的で番号を収集したりした場合には、改善命令などの行政指導を経ずに直ちに処罰されます。

また細かいことですが、従業員の個人番号を記載した書類の提出を行う事務の法的位置づけについて、一度整理しておくことが望ましいでしょう。たとえば所得税については、企業は「特別徴収義務者」として従業員の給与から源泉徴収し国へ納付する義務がありますが、社会保障については従業員の代理として書類を提出している場合もあります。後者のような事務では、従業員から委任状をもらう必要がある可能性がありますが、厚生労働省から公表されるガイド等に従っていく必要があるでしょう。



1年遅れで実施する予定となっています。税と雇用保険関係から確認を始めるのがよいでしょう。

Q2 業務フローにはどのような変更が必要になりますか。

源泉徴収票の出力など個人番号を取り扱う事務を外部に委託している場合、委託先（再委託先、再々委託先等を含む）に対して、委託元は適切な監督を行う義務が生じます。具体的には、委託先に安全管理措置を遵守させるために必要な契約を締結するほか、特定個人情報に係る各種規定を盛り込む必要があります。再委託先が海外の事業者の場合でも、委託元には同様の義務が発生します。

企業内で個人番号を取り扱う事務を行う部署は主に経理部や人事・労務部になると思われませんが、支社や営業所においても、従業員と扶養家族の個人番号を取りまとめて本社の担当部に提出するなどの事務や、Q1で示したような報酬支払い時の番号収集・本人確認業務が発生することが考えられます。番号の管理や廃棄のルールを定め、社員に周知徹底することが必要です。情報セキュリティや個人情報保護に関する担当部門が中心となって社員教育を実施するとよいでしょう。



近藤 佳大

みずほ情報総研
経営・ITコンサルティング部
シニアマネジャー

Profile

1991年入社。情報通信分野の政策テーマに関するリサーチ、コンサルティング業務を担当。著書に『ITとビジネスをつなぐエンタープライズアーキテクチャ』（中央経済社、共著）、『図でわかる！マイナンバー法のすべてQ&A』（同）など。



Q4 漏洩リスクを防ぐにはどのようなポイントに注意すればよいでしょうか。

個人番号の漏洩や滅失、毀損を防止するには、個人番号を取り扱う事務に携わる従業員をできるだけ限定することが有効となります。たとえば、各支社や営業所に労務管理者がいるような企業では、本社で一括して番号を収集・管理するように業務フローの変更を行うことも考えられるでしょう。遠隔地で勤務する従業員からの番号提供は、ユーザーIDとパスワードで認証し通知カードのスキャンデータを送信してもらう方法でもよいことになりそうです。

セキュリティ対策については、情報漏洩が発生した場合のインパクトの大きさを考えて対策する必要があります。まずは大規模な漏洩リスクへの対策が重要であり、外部からのハッキングや記録媒体による外部への持ち出しなどに関する対策を最優先に行うべきでしょう。また、そうした大規模漏洩が生じる風土を生まないよう、社員一人ひとりに高いセキュリティ意識を醸成することが重要となります。従業員数が少ない企業では、担当者の座席を壁際にしてPC画面が後ろから見えないようにする、個人番号を記入したファイルにはパスワードをかけ特定の人しかアクセスできないようにするなど、できるところから取り組むとよいでしょう。経済産業省は2014年12月に「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」を改正し、スマートフォンなど記録機能を持つ媒体の持込禁止など新しい項目を加えています。具体例も掲載されていますので参考にするとよいでしょう。