

お疲れ様です。コロナの感染状況はようやく下火になっていますが、ワクチン接種が進んだ諸外国では今の感染数が最大という国もあり、第6波到来の予測もある中で、まだまだ気が抜けない日々が続きますね。とにかく自分でできる感染対策を地道にやり続けるしかないですね。

さて、今回は「顧客情報管理」について解説いたします。顧客情報管理は大変に重要な体制整備の要件であるとともに代理店監査で最も指摘事項の多い項目のため、今回と次回の2回のテーマといたします。今回は代理店としての遵守事項、次回は代理店の従業者としての遵守事項について説明いたします。基本的なことを確実に、地道に、やり続けることが必要です。

《観点》

個人情報保護法等に則り、個人情報を適切に取り扱い、管理しているか。

《体制整備の実務面からの注意点》

1. プライバシーポリシーを公表する

プライバシーポリシーはお客様に見えやすい場所（事務所内、ホームページ等）に掲示しなければなりません。どこの代理店でも掲示はされていますが、「内容が更新されている」ことが重要です。例えば、取引保険会社名が旧社名のままになっていたり、法令の名称変更が反映されていない状況は不適切となります。また、センシティブ情報の項目が改正前の内容で記載されていることもあるので常に最新の内容で掲示されているかを点検する必要があります。これに限らず、「何のために公表しているのか」というルールの本質を踏まえて、形式的、おざなりの対応を脱することが大切です。

2. 個人データの安全管理に関する取扱規程を定めて、備え付ける。

保険代理店は個人情報の保護に関する規程および個人データの安全管理に関する取扱規程を全て備え付けておく必要があります。実査を行うと各種規程が個人情報保護法の旧規程のまま整備されていない状態が散見されます。また、募集人ヒヤリングでは規程の内容を理解できていないことが多く、特に個人情報と個人データの違いを知らない募集人が多いので研修等を通じて正しく理解することが重要です。

3. 個人データ管理責任者、個人データ管理者を設定する。

個人データ管理責任者（情報管理責任者）は取締役ないしは執行役と法令で定められています。役割分担図などを確認すると事務に精通したベテランの事務職員を責任者に任命している場合がありますが、これは法令違反となります。その方は個人データ管理者（担当者）としなければなりません。

4. 個人データ管理台帳を策定し、備え付けて定期的に更新する。

ほとんどの保険代理店では個人データ管理台帳を備え付けていますが、定期的な更新については様々な実態があります。数年間実施されていない、不定期で実施など、社内でルールが定まっていない、あるいは定まってもその通りに実施されていないのが現状です。個人データ管理台帳は社内のどこに、どのような個人データが所在しているかを特定する重要な管理台帳です。台帳に記載されているのに現物が見つからないことが検査で判明すると、個人情報漏えいと判定されてしまうので管理台帳を定期的に更新、棚卸して適正な状態に管理することが大変に重要な取り組みとなります。

5. 全ての従業者と個人データの非開示契約等を締結する。

非開示契約とは個人情報等の機密情報を許可なく第三者に開示しない旨を約束する契約です。入社時に取り付ける書類の一部ですが、在籍中や退職後に故意、過失問わず情報漏えいが判明した場合には非開示契約に基づき、懲戒処分や損害賠償請求をするための重要な契約書となりますので、契約内容は漏れが無きようしっかりと定める必要があります。

6. 機微（センシティブ）情報の取得・利用は業務上必要な範囲に限定する。

保険代理店の実査で執務室内のファイリングを確認すると、生保の告知書の写し、診断書の写しなどのセンシティブ情報を含む書類が保管されていることがあります。法令上、業務に必要でないセンシティブ情報を保管しておくことはできません。該当書類を保管する必要がある場合はセンシティブ情報をマスキングなどで確実に消去する必要があります。

また、金融庁検査の際には、上記のような実態の募集人に対しては徹底的なヒアリングが行われます。日頃から「基本に忠実」であることが非常に重要です。

7. 個人データの取り扱いを外部に委託する場合は保険会社に事前承認申請を行い、個人データが適切に管理されているか点検、監督する。

最近、クラウドサービスを導入してデジタル化を進める保険代理店が増えています。これは、自社のデータ管理を外部業者に委託することになるので、委託する全ての保険会社に事前承認申請を行い、代理店控えを保管しなければいけません。しかしながら、代理店実査で確認すると代申会社のみ申請を行っているケースが散見されます。委託保険会社全社の承認が必要となりますのでご注意ください。

8. パソコンのユーザーIDは個人ごとに設定する。

個人データ安全管理規程では、“ユーザーIDは利用者ごとに設定し、業務分担に応じてアクセス制御を行う”とされています。実査では全員共通のID・パスワードを使用している代理店もありますが、これでは、社内での情報漏えいがいつ発生してもおかしくない状態にあると言えます。全員のID・パスワードは個別に設定してデータ管理者が全員分を管理する体制にすることが必要です。

～次回に続く～

作成：日本創倫株式会社 専務取締役（SEO）オフィサー事業部長 風間利也
配信：日本代協 事務局