資料３－１

2019年9月26日

特定個人情報保護評価(全項目評価書を作成する事務)の意見について

(個人市民税に関する事務、固定資産税・都市計画税に関する事務、介護保険に関する事務共通)

特定個人情報を保護するためには、システムインフラ(ハード)とソフト(人による人的なリスク)の把握が必要と思われますが、各事務の取扱いの流れを確認したいと思いましたが、公表されている資料(税の種類・事務の違いに関わらず)では、特定個人情報の取扱いの手段・流れが明確になっていないため、リスクを具体的に把握することが出来ません。

共通の手法(取得、利用・加工、委託、移送、保管、返却・消去)により考えられるリスクについて以下のとおり記述し意見といたします。

1.特定個人情報の取得のリスクにつて

(1)情報の取得

①法令に違反するリスク(利用目的を通知しているか)

②取得の方法・手段によってリスクが異なります。

・例えば窓口における取得か

・FAX、郵送による取得か

・メール添付による取得か

(2)利用・加工

①システムへの取り込み⇒納品されたデータをアップするだけか、他の手段で行うのか不明であるが、担当者を限定する必要があります。(アクセス者をID、パスワードにより限定が必要です。)

②システムへの照会・取得⇒入力する場合は誤入力チェックが行われているか?

複数による誤入力チェックが望ましい。

(3)移送・送信

①移送の手段によってリスクが異なります。(公共交通機関利用、社用車か)

②送信の手段によってリスクが異なります。(専用線、メール添付送信、ストレージの利用)

2.委託におけるリスク

委託する場合は、委託元に監督責任が発生します。

(1)取得した情報の委託⇒委託先への情報の移送・送信の手段によってリスクが異なります。

①情報を委託先へどんな手段で移送するのか

持参か、公用車か、メール添付か、ストレージ等の利用か

(2)委託先の選定・評価⇒①委託先は、特定個人情報のリスク管理ができているか、委託先を評価し選定する必要があります。(必要な安全措置がとられているか)

②委託契約書には、監査、報告、漏えい事故が発生した場合の報告や再委託の承認等の条項が盛り込まれているか?

(3)委託先におけるデータの取扱い

委託した業務が終了した場合のデータ等の取扱い(消去、返還等)について

3. システムインフラについて

(1)端末はディスクトップかノートPCかによりリスク対策が異なります。

ノートPCの場合盗難防止措置(ワイヤーロックや使用しない場合は施錠保管等)

(2)漏えい対策

システムの使用しているサーバやPC端末は、OSは何を使用し脆弱性対策はとられているか?

また、ウイルス対策はとられ、最新のパターンファイルに更新が行われているか?

(3)サーバは、システム環境が保たれた場所に設置されているか、(サーバ室、施錠されたラック)

(4)バックアップの措置が取られているか

(5)停電や漏水等の対策がとられているか

(6)ファイル交換ソフト等の使用制限