

大阪府からの受託業務に係る個人情報の適正管理のポイント

(目 次)

● はじめに

1 個人情報取扱特記事項等の遵守

- 一般的注意事項

2 受託者内部における個人情報の適正な取扱いに係る責任体制

- 責任体制の確立
- 再委託の原則禁止

3 個人情報の管理

(1) 個人情報管理の基本

- 業務実施場所の特定
- 業務実施場所での個人情報の管理
- 個人情報の所在等の把握

(2) 電子化された個人情報の管理

- 電子データとして保存された個人情報の管理
- 受託業務に係る個人情報を取り扱うことができるパソコン等
- パソコン等のパスワード管理
- パソコン等の安全管理
- 外部記憶媒体に保存された個人情報の管理

(3) 個人情報の送信等

- 個人情報を電子メールで送信する場合
- 個人情報をファックスで送信する場合
- 個人情報を郵送で送付する場合

(4) 個人情報の外部持出し

- 外部持出の原則禁止
- 外部持出中の行為
- 外部持出終了後の処理

(5) 個人情報のホームページでの登載等

- 受託者のホームページにおける受託業務に係る個人情報の登載の原則禁止
- 例外的にホームページに登載する場合

(6) その他

- 会議・打合せ中の個人情報
- コピー紙の再利用等
- 職場における会話

4 個人情報の廃棄

● はじめに

この適正管理のポイントは、大阪府からの委託契約に基づく受託者が、受託業務を処理するに当たり、個人情報を適正に管理していただく上で留意していただくべき事項をまとめたものです。

受託者の皆さんにおかれましては、ここに掲げている事項を踏まえて、受託業務を実施していただきますようお願いいたします。

1 個人情報取扱特記事項等の遵守

■ 一般的注意事項

◎ 府との委託契約に基づく受託者（以下「受託者」という。）は、委託契約及びこれに添付された個人情報取扱特記事項等の規定並びに委託業務の実施に係る府の指示及び指導（この「受託者に係る適正管理のポイント」を含む。）に従い、個人情報を適正に取り扱ってください。

- 府が個人情報の保護のため、立入検査その他府が必要と考える調査を行う場合は、調査の実施に協力しなければなりません。
- 個人情報保護法、同法に基づき事業所管省庁が策定した個人情報の適正な取扱いのためのガイドライン法令等を遵守しなければなりません。

2 受託者内部における個人情報の適正な取扱いに係る責任体制

■ 責任体制の確立

◎ 府からの受託業務の履行に係る個人情報の適正な取扱いを確保するため、内部における責任体制を確立し、その体制を維持しなければなりません。

◎ この契約による個人情報の取扱いの責任者（作業責任者）及び業務の従事者（作業従事者）を定めてください。

- 個人情報の適正な取扱いを確保するため、作業責任者及び作業従事者それぞれに対して、この「個人情報の適正管理のポイント」の内容を十分に周知してください。
- 作業責任者には、作業従事者が個人情報を適正に取り扱うよう、必要な監督を行わせるとともに、作業従事者には、作業責任者の指示に従い、個人情報を適正に取り扱わせなければなりません。
- 作業責任者には、受託業務の責任者である受託者の管理職を充てることとし、責任体制が不明確にならないようにするため、作業従事者と兼務することは避けてください。

3 個人情報の管理

(1) 個人情報管理の基本

■ 業務実施場所の特定

◎ 業務の実施に当たっては、受託業務のうち個人情報を取り扱う業務を実施する場所（業務実施場所）を明確に定めてください。

- 個人情報の漏えい、滅失又は損傷を防止する観点から、受託者は、あらかじめ施錠等のセキュリティ管理が可能な場所を業務実施場所に定めてください。
- ここでいう個人情報を取り扱う業務には、府から引き渡された資料等を取り扱う場合だけでなく、受託業務の実施のため受託者が収集した個人情報を取り扱う場合も含まれます。

■ 業務実施場所での個人情報の管理

◎ 個人情報を含んだ資料等（紙文書のほか電子データを含む。以下、「個人情報」という。）は、業務実施場所内で、組織的に管理し、施錠できるロッカー等で管理してください。

◎ 業務実施のため利用した個人情報は、業務終了時には、必ず元の管理場所に戻してください。

◎ 個人情報の複製（バックアップ用）は、原則として1つに留めるなど、必要最小限の範囲に止めてください。

- 施錠できるロッカー等が不足する場合は、扉付きのロッカーで保管する、施錠できるロッカーに集約して管理するなどの工夫を行ってください。
- 鍵の管理者は、作業責任者又はその者から権限を付与された者等責任者を明確にしてください。
- 個人情報は、作業責任者、作業従事者の机等の引き出しなど、従業員等が個人的に管理を行っている場所に保管しないでください。
- 個人情報を利用している業務の途中で、机等を離れる場合は、紛失や他人に内容を見られることを防ぐため、個人情報を机上等に放置しないでください。また、一時的であってもダンボール箱、紙袋等に入れて、フロアに放置しないでください。

■ 個人情報の所在等の把握

◎ 受託業務に係る個人情報を適正に管理するため、個人情報の所在、種類、内容をきちんと把握してください。

- 個人情報の適正な管理を行うとともに、万一個人情報の漏えい、き損又は滅失という事故が発生した場合に迅速に対応できるようにするためには、所在等の把握は重要です。

(2) 電子化された個人情報の管理

■ 電子データとして保存された個人情報の管理

◎ 電子データは、容易に大量の複写、持出し等ができるため、慎重な管理を行ってください。

- 個人情報が一覧で表示されるような名簿類については、アクセス権(パスワード)を設定し、たとえ、作業従事者に指定された者であっても、当該業務の担当者以外の者が閲覧できないように取り扱ってください。

(注) 例えば、ワード・エクセルについても、ファイルごとにもパスワードを設定することができます。

■ 受託業務に係る個人情報を取り扱うことができるパソコン等

◎ 受託業務に係る個人情報を取り扱うパソコン・外部記憶媒体等は、業務実施場所において管理される、あらかじめ作業責任者が承認したものに限定してください。

◎ 作業責任者は、受託業務に係る個人情報を取り扱うパソコン・外部記憶媒体等に、個人情報の流出等につながる恐れがあるソフトウェア(又はアプリケーション)がインストールされないよう、指導監督してください。

- 作業責任者は、業務従事者等の従業員が私的な理由で、受託業務の実施に使用されるべきパソコン・外部記憶媒体等を使用することがないように指導監督してください。
- パソコン等を業務上、止む無く持ち出す場合は、後述の「(4) 個人情報の外部持出」の注意事項に従ってください。

■ パソコン等のパスワード管理

◎ 受託業務に係る個人情報を取り扱うパソコン等には、パスワードを設定してください。

- パスワードの設定は、出来る限り、簡単に想像できる組み合わせは避けてください。
- パスワードの設定の際は、十分な長さとし、ありふれた文字の連続などではなく、英数字を混在させるなど、想像しにくい組み合わせにしてください。
- パスワードは定期的に変更してください。
- パスワードを記載したメモをパソコン等の近く等他人に知られる場所に貼り付けておかない、職場の会話の中で周囲に漏れない、など、パスワードが漏れることがないように注意してください。

■ パソコン等の安全管理

- ◎ 作業従事者の離席時には、個人情報等の重要な情報が表示されているパソコンの画面を開いたままにならないよう、指導監督してください。
- ◎ 受託業務の実施に使用されるべきパソコン・外部記憶媒体等が盗難等に遭うことがないように、引き出し、ロッカー等に収納する等の安全管理措置をとるよう、作業従事者を指導監督してください。

- 作業責任者は、作業従事者に対して、離席時には、スクリーンセーバーが実行される設定を行い、パスワードによる保護をかけるよう、指導監督してください。

■ 外部記憶媒体に保存された個人情報の管理

- ◎ 外部記憶媒体の使用は必要最小限としてください。止むを得ず、作業従事者に使用させる場合は管理簿に登録した上で、組織管理を徹底し、紛失等が発生しないようにしてください。
- ◎ 使用しなくなった外部記憶媒体は、媒体内の個人情報を必ず消去してください。

- 外部記憶媒体を使用する場合は、管理簿に登録してください。
- 業務責任者は管理簿を管理し、業務従事者に外部記憶媒体を使用させる場合には、遅滞なくこれを管理簿に登録してください。
- 業務責任者は、業務従事者等の従業員が個人で購入した外部記憶媒体が、業務実施場所内に持ち込まれ、受託業務の処理に使用されることがないように指導監督してください。
- 業務責任者は、業務従事者等の従業員が私的な理由で、受託業務の実施に使用されるべき外部記憶媒体を使用することがないように指導し、又は監督してください。
- 紛失には十分注意してください。
- 業務実施場所の外に持ち出す場合は、後述の「(4) 個人情報の外部持出」の注意事項に従ってください。

(3) 個人情報の送信等

■ 個人情報を電子メールで送信する場合

- ◎ 作業従事者が電子メールで個人情報を送信する場合は、原則として作業責任者又は上司の許可を得てください。
- ◎ 複数の宛先へ電子メールを送信する場合は、メールアドレスを第三者に知られることがないように、**BCC** 送信機能を使ってください。

- 電子メールを転送する場合は、内容を吟味して個人情報や機密情報を削除するとともに、相手先を厳選してください。
- 電子メールの自動転送は原則禁止です。
自動転送が認められる場合
 - ・不在時等にやむを得ずメールを受信する必要がある、携帯電話や信頼できるプロバイダの自分のメールアドレスに限って転送する場合
 - ・受託者の社内メールのメールアドレスに到着したメールを担当者に転送する場合
- 電子メールの件名には、個人情報を含めないようにしてください。
- 電子メールを送信する場合は、誤送信を防ぐため、送信前に必ず宛先のアドレス及び原稿を確認してください。(Outlook の場合、「宛先」、「CC」、「BCC」を意識して使い分けること。)
- 電子メールにファイルを添付して送信する場合は、ファイルの内容を必ず確認してください。(特に、別の文書を編集加工したファイルの場合、元の文書にあった個人情報を間違えて送信する危険があります。)
- 重要データを電子メールで送信する場合、添付ファイルにパスワードを設定するなどの保護をしてください。

■ 個人情報をファックスで送信する場合

- ◎ 作業従事者がファックス等で個人情報を送信する場合は、原則として作業責任者又は上司の許可を得てください。
- ◎ ファックスによる文書の送信は、必ず、送信先やファックス番号を確認してください。

- ファックスを送信する場合は、誤送信を防ぐため、送信前に必ず宛先のファックス番号を確認してください。
- ファックス送信時の原稿や、受信時に出力された用紙は放置しないでください。

■ 個人情報を郵送で送付する場合

- ◎ 作業従事者が郵送で個人情報を送信する場合は、宛先と内容が間違いないかの確認を徹底するよう指導してください。

(4) 個人情報の外部持出

■ 外部持出の原則禁止

- ◎ 受託業務に係る個人情報は、府が個別又は業務の性格上包括的に承諾した場合（業務の性格上当然に承諾したものと見られる場合を含む。）を除き、業務実施場所から持ち出されることがないように、従業員等に周知徹底してください。
- ◎ 作業責任者は、府が個人情報の持出しを承諾している事案について、作業従事者が個人情報の持出しを行おうとする場合には、事案ごとに、あらかじめ、府の承諾の範囲内であるか、当該事案における持出しの必要性を確認した上で、その可否を判断してください。
- ◎ 作業従事者は、あらかじめ作業責任者の了解を得た場合を除き、個人情報を持ち出してはいけません。
- ◎ 作業責任者は、従業員等が個人所有のパソコンに、受託業務に係る個人情報のデータを送信することがないように、指導監督してください。

- 個人情報の業務実施場所外への持ち出しは上述の場合を除き、禁止です。
- 上述のとおり、作業従事者が作業責任者の了解を得て、個人情報を例外的に持ち出しうる場合の取扱いは次のとおりです。
 - （作業従事者が了解を得る際の手続）
 - ・ 個別事情により個人情報を持ち出すものについては、その都度、作業責任者が作成、管理する持出し管理簿に使用目的等を記載し、上司の許可を得る。
 - （作業従事者が了解を得る場合の留意点）
 - ・ 持出しの了解を受ける際には、万一の紛失に備え、持出した個人文書を特定又は容易に推定できるようにしてください。
 - ・ 了解を受ける文書は、やむを得ない場合を除き、原本ではなく、写しとしてください。
- 作業責任者は、作業従事者に次のような持出しに伴う個人情報の流出事例（例：日頃のマスコミ等で報道されている事例）を周知し、事故防止に向けた意識付けに取り組んでください。
 - ・ **USB** メモリ等により、個人情報の無断に持ち出した結果、紛失又は盗難に遭った事例
 - ・ 自宅での作業のために、自宅のパソコンに個人情報を持出し、そのパソコンがウイルスに感染していることに気が付かず作業したところ、「ファイル共有ソフト」を通じて情報が流出した事例

■ 外部持出中の行為

◎ 作業責任者は、作業従事者等に対し、個人情報の持出し時は、盗難・紛失などの情報漏えいのリスクを常に意識し、手元から離さないように注意喚起してください。

- 個人情報流出事件の多くが、個人情報を持ち出した際に起きており、車上荒らしなどの盗難被害、電車内の網棚等での置き忘れ、紛失等の過失によって流出したケースが多数発生しています。
- 止むを得ず自宅に持ち帰る場合は、帰宅途中の買い物、飲酒等は流出リスクを高めることとなりますので、これを控えるよう、作業従事者に対し、注意喚起してください。
- 万一の紛失に備え、個人情報を含む電子機器や電子媒体には、第三者がアクセスできないよう、パスワードを設定する等の情報セキュリティ対策を実施してください。

■ 外部持出終了後の処理

◎ 作業責任者は、作業従事者に対し、帰社後すぐに、持ち出した個人情報がかつて揃っているかどうかを確認させてください。

- 職員の個人情報の持出し終了後は、不足がないかを直接現物を確認してください。

(5) 個人情報のホームページでの登載等

■ 受託者のホームページにおける受託業務に係る個人情報の登載の原則禁止

◎ ホームページには、原則、個人情報を登載しないようにしてください。

- ホームページに個人情報（個人の肖像も個人情報です。）を登載する場合は、あらかじめ本人に対し、提供する情報の内容、提供の目的、当該情報がインターネットを通じて広く発信されること等を十分に説明した上で提供についての明確な同意を確実に得るようにしてください。
- ホームページで提供した個人情報について、本人から訂正、提供の停止の求めがあったときは、速やかに対応してください。

■ 例外的にホームページに登載する場合

- ◎ ホームページで公表する場合には、作業責任者は、必ず内容を確認してください。
- ◎ 受託業務に係るホームページの掲載については、事前に府（委託業務担当課）と調整してください。

(6) その他

■ 会議・打合せ中の個人情報

- ◎ 個人情報が掲載された会議・打合せ資料は、会議終了後、できるだけ回収に努めてください。業務執行上の必要性があるため、これを回収しない場合は、会議等の参加者に取扱注意の個人情報であることを確認したうえで解散してください。
- ◎ 個人情報が掲載された会議・打合せ資料については、会議終了後、会議室等に放置しないようにしてください。

■ コピー紙の再利用等

コピー紙の再利用等

- ◎ 再利用しようとするコピー紙・メモ紙の裏面に個人情報が記載されていないことを確認してください。

- コピー、FAX、プリンタ使用時は、出力された資料・原稿の放置や複数混入に気をつけてください。

■ 職場における会話

- ◎ 職場における会話の中で、個人情報を周囲に漏らさないようにしてください。

- エレベータ内や廊下においても、来訪者等が近くにいる場合もあるため、重要な個人情報を含む会話は控えてください。
- 業務上必要な会話においても、必要最小限の情報提供に留意してください。

4 個人情報の廃棄

◎ 受託業務終了後又は受託業務中であっても保有する必要のなくなった個人情報については、確実かつ速やかに廃棄若しくは消去又は返却してください。

- 「保有する必要のなくなった」とは、受託業務を進める上で、個人情報を保有する必要がなくなったことをいいます。
- 廃棄又は消去の方法
 - ・ 紙文書
シュレッダーにより裁断するか処理業者に廃棄を委託してください。
この場合、作業責任者又は作業従事者が廃棄に立ち会うか、処理業者に廃棄した旨の報告をもとめるなど確実に廃棄されたことを確認してください。
 - ・ パソコン等及び外部記憶媒体
個人情報を入力した電子ファイルが不要になった場合は、直ちに消去してください。
パソコン等及び外部記憶媒体自体を廃棄する場合は、物理的に破壊するなど解読不可能な状態にしてください。
- 府が、廃棄又は消去の作業への立会いを求めた場合には、これに協力してください。