

Y. その他サービス業（印刷・広告） Y社

事業概要	パンフレット、カタログ等印刷、デザイン、製本等		
従業員数	約 110 人	プライバシーマーク取得	あり
保有個人データ件数	なし（常時保有は従業者情報のみで主に一時的保管）		

1. 個人情報に関する概要

（1）保有する個人情報の件数、種類、利用目的

- ・保有している個人情報は従業者情報程度しかなく、個人情報は預託されている。
- ・生命保険番号やレセプト、資格関係などの機微情報を扱うこともある。

（2）個人情報保護担当部署

- ・システム管理室が担当している。

（3）個人情報保護管理者の有無・位置づけ

- ・個人情報保護管理者はシステム管理室長である。

（4）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

- ・プライバシーマークを平成 17 年に取得した。取得は、長い付き合いのある大きな取引先にプライバシーマークの取得が必要であると要請されたことがきっかけである。その後、社内でヒアリングを行い、社会的な要請を感じて取得に踏み切った。
- ・プライバシーマークの取得に当たっては、コンサルタントに委託した。
- ・得意先（特に新規）の取引先審査（信用度）に大変効果がある。
- ・更新審査は自社スタッフのみで対応した。
- ・平成 19 年 更新。

（5）個人情報保護に向けた取組経緯

- ・プライバシーマークの取得準備をきっかけに、取組を行った。

（6）個人情報の保有・管理・提供等に関する業界の特徴

- ・情報の保管管理を依頼されることがある。既存のデータに新たにデータを追加して印刷することが多く、保管データが上積みされていく。

2. 個人情報の適切な保護のための取組について

(1) 準備（規程・体制づくり）

- ・特徴的な取組はなし

(2) 個人情報の取得

- ・委託を受ける際は、授受記録（受注件名・内容・取得日・担当者名を記載）をとっている。
- ・提供者には当社の取扱基準を説明して、本人同意の上で取得している。
- ・従業員には会社が保有する情報（種類）を社内掲示し、開示・非開示の区別も明確にしている。

(3) 個人情報の利用（第三者提供を含む）

- ・個人情報は直接収集でないため、利用することはない。

(4) 個人情報の管理

①情報の管理態勢

（キャビネットは開閉を名簿管理）

- ・共有のキャビネットはいつ誰が開けて何を取り出したかを紙で記録するようにしている。スペアキーを持っている者をリスト化している。
- ・どの建物も警備会社と契約している。入退出の際、最初に入った人と最後に出た人は記録を採る。
- ・本社（人とデータ量が最も多い）では、カードキーを持っていない人は受付を通らないと中に入れなくなっている。
- ・社内のパソコンにはウイルス対策ソフトが入っており、サーバにも導入してある。
- ・パソコンには、ID やパスワードを設定している。
- ・フロッピーなどの媒体に関しては、ウイルス対策ソフトを作動させてからファイルを開くよう指導している。
- ・個人情報を、従業員個人のパソコンに保存することは禁止している。ノート PC を用いて社外で作業することはない。
- ・電子メールへのファイル等の添付は原則禁止している。送信の際にはパスワードを義務づけている。
- ・個人および企業情報を含んだ製品は、納品まで他製品とは別に施錠保管している。

②従業員への教育方法

（担当委員を中心に勉強会を開催）

- ・朝礼や部署ごとの勉強会を随時行っている。各部署の保護委員（情報保護担当：中間管理職レベルの職位）とセキュリティ委員（パソコン管理、事業者出入りの鍵の管理を担当）が中心となって勉強会をしている。保護委員は委員会を隔月で開催し、部署に持ち帰って勉強会に活かしている。社内の意識を高める効果がある。
- ・新入社員研修の初日に基礎教育として個人情報保護に関する教育をしている。アルバイトや派遣社員、パート社員に対しても講義を対面で行っている。
- ・社内の掲示板に個人情報保護に関する情報を掲示し、全員が閲覧するようにしている。
- ・集合研修を年に 1 回行っている。講師はシステム管理室が行い、毎回小テストをしている。テスト成績によっては各部署で補習をしている。
- ・個人情報に関するマニュアルの冊子を作り、全従業員に配布した。別添の問題集もある。
- ・一般とは別に、役員（常勤・非常勤）や管理職には階層別教育を行っている。

③盗難対策

- ・特徴的な取組はなし

④ノート PC の安全対策

- ・ノート PC は使っていない。

⑤外部委託先管理

（外部委託先は管理表で管理）

- ・業務が大量の場合は発送を委託することがある。委託先はプライバシーマークを取っている業者を優先している。
- ・委託先には、事前通知の上、実地見学を行っている。
- ・社内で設定した委託基準に達しない業者には発注しない。

⑥日常点検・確認の方策

- ・グループウェア上の掲示板に情報を載せている。

⑦初歩的ミスの防止策

- ・個人情報は FAX や電子メールでの送信禁止を前提としている。送る場合はファイルにパスワードの設定を義務付けている。

（5）個人情報の消去・破棄

- ・情報は、委託元との契約に応じて情報が不要になった時に廃棄する。廃棄証明をつけることを要求される場合は、そのようにする。

- ・紙の情報を溶解するため処分業者と契約しており、処分状況を顧客に報告することもある。紙媒体の情報は一般のゴミでは出さず、定期的に回収に来る処分業者に委託している。
- ・電子データは消去の記録をつけている。媒体に残っているものは消去ツールで中身を消してから粉碎処理を委託して行っている。フロッピーの再利用は禁止している。
- ・生産部としては、不要になった時点（生産後）から1ヶ月以内に処分する、というルールにしている。

(6) 個人情報の監査

- ・監査は年1回行っている。保護委員が自分の部署以外を監査し、個人情報の保護体制をメインにした監査を行っている

(7) 苦情処理・顧客対応

- ・お客様相談窓口を設置しており、各担当者レベルでは回答はしないようにしている。
- ・これまで個人情報に関する問い合わせや苦情はない。

(8) 事故発生時の対応

- ・漏えい事故は実際には起こっていないが、事故の際には被害の拡大を防止する措置をとり、関連する各団体・官公庁へ報告する。事故の規模によっては対策本部を臨時で設置して事故の状況把握と復旧対策を検討する。
- ・機密情報の契約を顧客と結んでいる。個々の対策、損害賠償は契約によって規定されているので、それに沿って行う。個人情報の漏えいに関しては、実際には収集・取得元が責任をとって、それからの派生的な当社のような委託先が損害賠償という形になると考えられる。

以 上