個人情報漏洩などの事故をなくすために…

平成19年4月

社団法人
日本グラフィックサービス工業会
the Japan Graphic services industry association JaGra

社団法人
東京グラフィックサービス工業会
the Tokyo Graphic services industry association

■ 個人情報とは…

「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるものをいいます。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問いません。

なお、死者に関する情報が、同時に、遺族等の生存する個人に関する情報でもある場合には、当該生存する個人に関する情報となります。

また、法人その他の団体は「個人」に該当しないため、法人等の団体そのものに関する情報は含まれません。（ただし、役員、従業員等に関する情報は個人情報です。）

【個人情報に該当する事例】

①本人の氏名
②生年月日、連絡先（住所・居所・電話番号・メールアドレス）、会社における職位又は所属に関する情報について、それらと本人の氏名を組み合わせた情報
③防犯カメラに記録された情報等本人が判別できる映像情報
④特定の個人を識別できるメールアドレス情報
⑤特定個人を識別できる情報が記述されていなくても、周知の情報を補って認識することにより特定の個人を識別できる情報
⑥雇用管理情報（会社が従業員を評価した情報を含む）
⑦個人情報を取得後に当該情報に付加された個人に関する情報（取得時に生存する特定の個人を識別することができなかったとしても、取得後、新たな情報が付加され、又は照合された結果、生存する特定の個人を識別できた場合は、その時点で個人情報となります）
⑧官報、電話帳、職員録等で公にされている情報（本人の氏名等）

経済産業省のガイドライン

特に印刷業界としては、年賀状・暑中見舞いハガキ、名刺、名簿、アルバム、DM用宛名、印刷物やビデオ、Web等のデータ中に含まれる顔写真等、メールアドレスにつき個人情報の該当性に対する注意が必要と考えられます。

■ 法令・指針、その他の規範

平成17年４月に全面施行された個人情報の保護に関する法律（以下「個人情報保護法」という）、個人情報保護法施行令及び個人情報の保護に関する基本方針（閣議決定）は、個人情報保護に関する一般的なルールであり、法令遵守の観点から必ず確認しなくてはなりません。因みに、事業の用に供する個人情報データベース等を構成する個人情報によって識別される特定の個人の数の合計が、過去６ヶ月以内のいずれかの日においても、5,000を超えていた事業者は、原則として、「個人情報取扱事業者」として法の対象となります。加えて都道府県・市区町村も自治体個人情報保護条例や経済産業省及び厚生労働省のガイドライン、（社）日本グラフィックサービス工業会、（社）東京グラフィックサービス工業会及び（社）日本印刷産業連合会の各業界ガイドラインについても十分承知しておく必要があります。

社団法人　日本グラフィックサービス工業会
http://www.jagra.or.jp/

社団法人　東京グラフィックサービス工業会
http://www.tokyographics.or.jp/

社団法人　日本印刷産業連合会
http://www.jfpi.or.jp/

個人情報保護法（内閣府）
http://www5.cao.go.jp/seikatsu/

経済産業省ガイドライン
http://www.meti.go.jp/feedback/downloadfiles/i40615hj.pdf

厚生労働省指針
http://www.mhlw.go.jp/topics/2004/07/tp0701-1.html

（財）日本情報処理開発協会
http://www.jipdec.jp/

■ 利用目的の公表

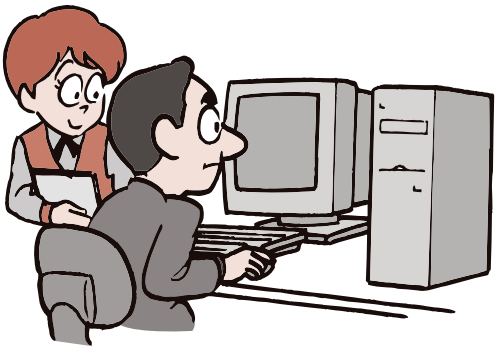
個人情報を取り扱うに当たっては、HP等でその利用の目的をできる限り特定しなければなりません。なお、利用目的の特定の際に、利用する個人情報の項目及び入手先の事業者名等を特定することまで求められるわけではありません。また多くの場合、業種の明示だけでは利用目的をできる限り具体的に特定したことにはなりません。また、単に「事業活動」を「お客様のサービスの向上」等のように抽象的、一般的な内容を利用目的とすることは、具体的に特定したことにはなりません。

なお、あらかじめ、個人情報を第三者に提供することを想定している場合には、利用目的において、その旨を特定しなければなりません。

【具体的に利用目的を特定している事例】

①「○○事業における商品の発送、関連するアフターサービス、新商品・サービスに関する情報のお知らせのために利用いたします」。
②「ご記入いただいた氏名、住所、電話番号は、名簿として販売することがあります」。
③例えば、情報処理サービスを行っている事業者の場合であれば「給与計算処理サービス、あて名印刷サービス、伝票の印刷・発送サービス等の情報処理サービスを業として行うために委託された個人情報を取り扱います」のようにすれば利用目的を特定したことになります。

経済産業省のガイドライン



■ 個人情報の特定

特定については、本人から直接書面で取得した情報（例. 自社の役員・従業員情報、顧客本人から直接受注した名刺・年賀状・各種名簿・発送リスト等、印刷、情報処理に係るもの）及び直接書面以外で印刷・情報処理等で取得した受託物、顧客からの支給品、個人データ、フイルム・刷版、DMデータ、印刷見本等を示します。

また、個人情報の一覧（台帳）を作ることを勧めます。そこには、カテゴリー毎に利用目的、入手経路、保管場所、保管期間、件数、廃棄方法を記載しておくと一覧性があって管理しやすいでしょう。同時に業務フローを作っておくことも必要です。加えて、開示対象個人情報の可否についても明記しておくと良いでしょう。

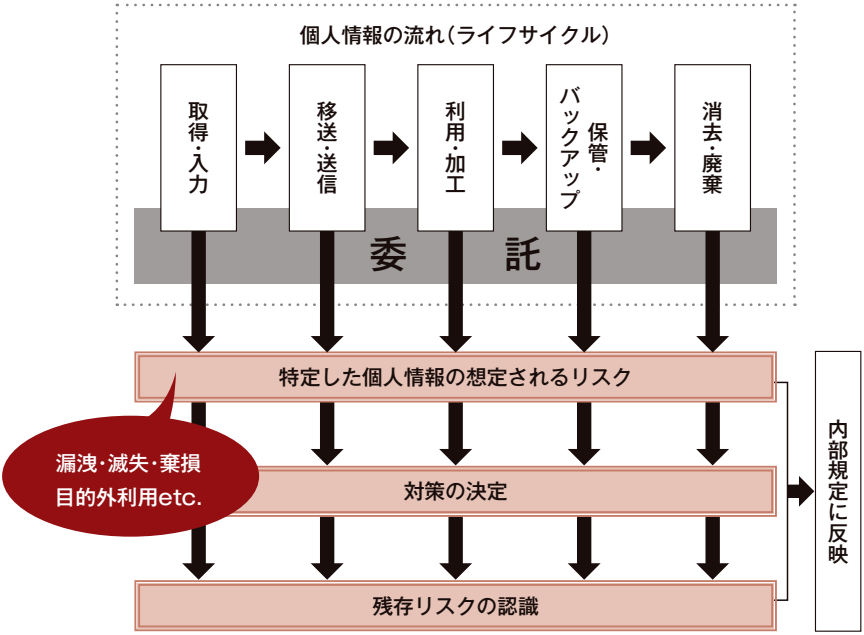
■ リスク分析

リスク分析は、取得、入力・編集、校正、移送・通信、利用（製版・印刷・製本、DM他）、保管（サーバー、完成製品見本、自社倉庫内在庫）・バックアップ、納品・運搬、消去・廃棄の各局面のライフサイクルに沿って行ないます。そのリスク分析に従い、評価し、対策を講じなければなりません。重要度の高いものから対策を立てますが、経済的理由等で対応できないものについては、「残存リスク」として把握しておくと良いでしょう。

個人情報管理台帳（例）

項目	個人情報名	項目			入手経路	件数	利用目的	保管場所	保管方法	アクセス権を有するもの	利用期限	廃棄方法	開示情報の可否
		データ	紙媒体	その他									

個人情報のリスク認識・分析・対策を検討する



※（財）日本情報処理開発協会テキストより転載

リスク分析とその対策（例）

（個人情報名：　　）

ライフサイクル	取得・入力	移送・送信	利用・加工	保管・バックアップ	消去・廃棄
部門					
想定されるリスク					
選択したリスク対策					
関連規定					
運用結果の記録					
残存リスク					
その他					

※（財）日本情報処理開発協会テキストより転載

■ 個人情報の取得と本人の同意

個人情報の取得は適正に行って下さい。

個人情報保護法では、「個人情報取扱事業者は、あらかじめ本人の同意を得ないで、特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。」とし、「個人情報取扱事業者は、(中略)、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。」と規定しています。

「本人の同意」とは、本人の個人情報が、個人情報取扱事業者によって示された取扱方法で取り扱われることを承諾する旨の当該本人の意思表示をいいます(当該本人であることを確認できていることが前提です)。

また「本人の同意を得る」とは、本人の承諾する旨の意思表示を当該個人情報取扱事業者が認識することをいい、事業の性質及び個人情報の取扱状況に応じ、本人が同意に係る判断を行うために必要と考えられる合理的かつ適切な方法によらなければなりません。

■ 直接書面等による取得について

個人情報取扱事業者は、本人との間で契約を締結することに伴って契約書その他の書面(電子的方式、磁気的方式、その他、人の知覚によっては認識することができない方式で作られる記録を含む)に記載された当該本人の個人情報を取得する場合、その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければなりません。例えば、個人情報取扱事業者は、書面等による記載やユーザー入力画面への打ち込み等により直接本人から個人情報を取得する場合がこれに該当します。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りではありません。

なお、口頭による個人情報の取得にまで、当該義務を課すものではありませんが、その場合は、あらかじめ利用目的を公表するか、速やかに、その利用目的を、本人に通知し、又は公表しなければなりません。

【あらかじめ、本人に対し、その利用目的を明示しなければならない場合】

①申込書・契約書に記載された個人情報を本人から直接取得する場合
②アンケートに記載された個人情報を直接本人から取得する場合
③懸賞の応募はがきに記載された個人情報を直接本人から取得する場合

経済産業省のガイドライン

なお、JIS Q15001では機微情報の取得、利用、提供も禁止しています。

＊機微情報とは、①思想、信条、宗教に関する事項　②人種、民族、門地、本籍地（所在都道府県情報は除く）、身体・精神障害、犯罪歴その他社会的差別の原因となる事項　③勤労者の団結権、団体交渉その他の団体行動行為に関する事項　④集団示威行為への参加、請願権の行使その他政治的権利の行使に関する事項　⑤保健医療、性生活事項

機微情報を取得する場合は、法令に特別な規定がある場合や司法手続上必要不可欠である場合を除き、本人の明示的同意が必要となります。

■ 直接書面以外による取得について

印刷業のみならず受注産業にとって注意を払う所です。直接書面以外で取得する顧客から処理を委託されるデータ、印刷物、DM発送等の発注に際して顧客（あるいは元請）から委託を受けるデータを含めた個人情報が、本人の同意を得たものか得ていないものか、委託される際に確認すべき事項であります。

■ データ内容の正確性の確保

個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つよう努めなければなりません。

印刷業の場合、印刷・データ処理に関してそれを業としているだけに、特に内容の正確性（誤字・誤植等）を保証する必要があります。顧客が「校正」を行なっていても、入力・プリプレス工程での内部チェックは必須の課題です。保存期間、データのバックアップの手順も定めておきます。

■ 緊急事態について

印刷業では、個人情報が漏洩、滅失又はき損をした場合に想定される経済的な不利益及び社会的な信用の失墜、本人への影響などのおそれを考慮し、その影響を最小限とするための手順を確立しなければなりません。

また、個人情報の漏洩、滅失又はき損が発生した場合に備えましょう。

①当該漏洩、滅失又はき損が発生した個人情報の内容を本人に速やかに通知し、又は本人が容易に知り得る状態に置きます。

②二次被害の防止、類似事案の発生回避などの観点から、可能な限り、事実関係、発生原因及び対応策を遅滞なく公表します。

③事実関係、発生原因及び対応策を関係機関（経済産業省、社団法人日本グラフィックサービス工業会、社団法人東京グラフィックサービス工業会等）に直ちに報告します。

DMの誤配送、FAX、メールの誤送信等これらはあってはならないことですが、ウッカリミスであっても事故に変わりはありません。漏洩、滅失、き損の緊急事態への対応は重要な対策です。事故発生にあっては何よりも本人への通知、二次被害の防止が優先します。直接取得でない場合は委託元との連絡、認定個人情報保護団体との連携、社内・外連絡網の作成、そして緊急事態への事前の対処方法の徹底が必要です。

■ 安全管理措置

個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければなりません。講ずるべき措置は、その内容によって、組織的、人的、物理的及び技術的な安全管理措置に分類することができます。

組織的安全管理措置

組織的安全管理措置とは、安全管理について従業者の責任と権限を明確に定め、安全管理に対する規程や手順書（以下「規程等」という）を整備運用し、その実施状況を確認することをいいます。

【組織的安全管理措置として講じなければならない事項】

①個人データの安全管理措置を講じるための組織体制の整備
②個人データの安全管理措置を定める規程等の整備と規程等に従った運用
③個人データの取扱状況を一覧できる手段の整備
④個人データの安全管理措置の評価、見直し及び改善
⑤事故又は違反への対処

経済産業省のガイドライン

人的安全管理措置

人的安全管理措置とは、従業者に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいいます。

【人的安全管理措置として講じなければならない事項】

①雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む）における委託者と受託者間での非開示契約の締結。
②従業者に対する内部規程等の周知・教育・訓練の実施

経済産業省のガイドライン

物理的安全管理措置

物理的安全管理措置とは、入退館（室）の管理、個人データの盗難の防止等の措置をいいます。

【物理的安全管理措置として講じなければならない事項】

①入退館（室）管理の実施
②盗難等の防止
③機器・装置等の物理的な保護

経済産業省のガイドライン

【各項目を実践するために講じることが望まれる手法の例示】

①「入退館（室）管理」を実践するために講じることが望まれる手法の例示

- 個人データを取り扱う業務の、入退館（室）管理を実施している物理的に保護された室内での実施
- 個人データを取り扱う情報システム等の、入退館（室）管理を実施している物理的に保護された室内等への設置

②「盗難等の防止」を実践するために講じることが望まれる手法の例示

- 個人データを記した書類、媒体、携帯可能なコンピュータ等の机上及び車内等への放置の禁止
- 離席時のパスワード付きスクリーンセイバ等の起動によるのぞき見等の防止
- 個人データを含む媒体の施錠保管
- 氏名、住所、メールアドレス等を記載した個人データとそれ以外の個人データの分離保管
- 個人データを取り扱う情報システムの操作マニュアルの机上等への放置の禁止

③「機器・装置等の物理的な保護」を実践するために講じることが望まれる手法の例示

- 個人データを取り扱う機器・装置等の、安全管理上の脅威（例えば、盗難、破壊、破損）や環境上の脅威（例えば、漏水、火災、停電）からの物理的な保護

技術的安全管理措置

技術的安全管理措置とは、個人データ及びそれを取り扱う情報システムへのアクセス制御、不正ソフトウェア対策、情報システムの監視等、個人データに対する技術的な安全管理措置をいいます。

【技術的安全管理措置として講じなければならない事項】

①個人データへのアクセスにおける識別と認証
②個人データへのアクセス制御
③個人データへのアクセス権限の管理
④個人データのアクセスの記録
⑤個人データを取り扱う情報システムについての不正ソフトウェア対策
⑥個人データの移送・送信時の対策
⑦個人データを取り扱う情報システムの動作確認時の対策
⑧個人データを取り扱う情報システムの監視

経済産業省のガイドライン

【各項目を実践するために講じることが望まれる手法の例示】

①「個人データへのアクセスにおける識別と認証」を実践するために講じることが望まれる手法の例示

・個人データに対する正当なアクセスであることを確認するために正当なアクセス権限を有する者であることの識別と認証（例えば、IDとパスワードによる認証、生体認証等）の実施

＊IDとパスワードを利用する場合には、パスワードの有効期限の設定、同一又は類似パスワードの再利用の制限、最低パスワード文字数の設定、一定回数以上ログインに失敗したIDを停止する等の措置を講じることが望ましい。

・個人データへのアクセス権限を有する者が使用できる端末又はアドレス等の識別と認証（例えば、MACアドレス認証、IPアドレス認証、電子証明書や秘密分散技術を用いた認証等）の実施

②「個人データへのアクセス制御」を実践するために講じることが望まれる手法の例示

・個人データへのアクセス権限を付与すべき者の最小化
・識別に基づいたアクセス制御（パスワード設定をしたファイルがだ

れでもアクセスできる状態は、アクセス制御はされているが、識別がされていないことになる。このような場合には、パスワードを知っている者が特定され、かつ、アクセスを許可する者に変更があるたびに、適切にパスワードを変更する必要がある）の実施。

・アクセス権限を有する者に付与する権限の最小化

・個人データを格納した情報システムへの同時利用者数の制限

・個人データを格納した情報システムの利用時間の制限（例えば、休業日や業務時間外等の時間帯には情報システムにアクセスできないようにする等）

・個人データを格納した情報システムへの無権限アクセスからの保護（例えば、ファイアウォール、ルータ等の設定）

・個人データにアクセス可能なアプリケーションの無権限利用の防止（例えば、アプリケーションシステムに認証システムを実装する、業務上必要となる者が利用するコンピュータのみに必要なアプリケーションシステムをインストールする、業務上必要な機能のみメニューに表示させる等）

＊情報システムの特権ユーザーであっても、情報システムの管理上個人データの内容を知らなくてもよいのであれば、個人データへ直接アクセスできないようにアクセス制御をすることが望ましい。

＊特権ユーザーに対するアクセス制御については、例えば、トラステッドOSやセキュアOS、アクセス制御機能を実現する製品等の利用が考えられる。

・個人データを取り扱う情報システムに導入したアクセス制御機能の有効性の検証（例えば、ウェブアプリケーションのぜい弱性有無の検証）

③「個人データへのアクセス権限の管理」を実践するために講じることが望まれる手法の例示

・個人データにアクセスできる者を許可する権限管理の適切かつ定期的な実施（例えば、定期的に個人データにアクセスする者の登録を行う作業担当者が適当であることを十分に審査し、その者だけが、登録等の作業を行えるようにする）。

・個人データを取り扱う情報システムへの必要最小限のアクセス制御の実施

④「個人データへのアクセスの記録」を実践するために講じることが望まれる手法の例示

・ 個人データへのアクセスや操作の成功と失敗の記録（例えば、個人データへのアクセスや操作を記録できない場合には、情報システムへのアクセスの成功と失敗の記録）

・採取した記録の漏えい、滅失及びき損からの適切な保護

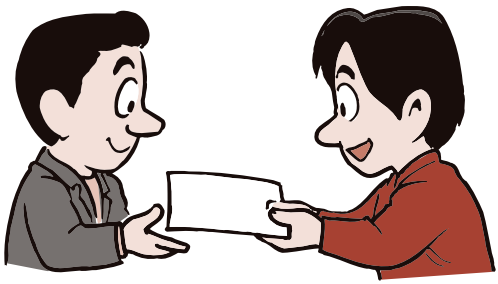
＊個人データを取り扱う情報システムの記録が個人情報に該当する場合があることに留意する。

⑤「個人データを取り扱う情報システムについて不正ソフトウェア対策」を実践するために講じることが望まれる手法の例示

・ウイルス対策ソフトウェアの導入

・ オペレーティングシステム（OS）、アプリケーション等に対するセキュリティ対策用修正ソフトウェア（いわゆる、セキュリティパッチ）の適用

・ 不正ソフトウェア対策の有効性・安定性の確認（例えば、パターンファイルや修正ソフトウェアの更新の確認）



⑥「個人データの移送（運搬、郵送、宅配便等）・送信時の対策」を実践するために講じることが望まれる手法の例示

・移送時における紛失・盗難が生じた際の対策（例えば、媒体に保管されている個人データの暗号化等の秘匿化）

・盗聴される可能性のあるネットワーク（例えば、インターネットや無線LAN等）で個人データを送信（例えば、本人及び従業者による入力やアクセス、メールに添付してファイルを送信する等を含むデータの転送等）する際の、個人データの暗号化等の秘匿化

⑦「個人データを取り扱う情報システムの動作確認時の対策」を実践するために講じることが望まれる手法の例示

・情報システムの動作確認時のテストデータとして個人データを利用することの禁止

・情報システムの変更時に、それらの変更によって情報システム又は運用環境のセキュリティが損なわれないことの検証

⑧「個人データを取り扱う情報システムの監視」を実践するために講じることが望まれる手法の例示

・個人データを取り扱う情報システムの使用状況の定期的な監視

・個人データへのアクセス状況（操作内容も含む）の監視

＊個人データを取り扱う情報システムを監視した結果の記録が個人情報に該当する場合があることに留意する必要があります。

■ 従業者の監督

個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人情報の安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければなりません。

その際、本人の個人データが漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人データの取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとします。従業者と会社間で個人情報の取扱いに関する各従業者の役割、責任を明確化し、従業者が個人情報保護の役割、責任を認識することが大切です。

なお「従業者」とは、個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、派遣社員等も含まれます。

■ 委託先の監督

個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければなりません。その際、本人の個人情報が漏えい、滅失又はき損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質及び個人情報の取扱状況等に起因するリスクに応じ、必要かつ適切な措置を講じるものとします。

「必要かつ適切な監督」には、委託契約において、当該個人データの取扱に関して、必要かつ適切な安全管理措置として、委託者、受託者双方が同意した内容を契約に盛り込むとともに、同内容が適切に遂行されていることを、あらかじめ定めた間隔で確認することも含まれます。

また、委託者が受託者について「必要かつ適切な監督」を行っていない場合で、受託者が再委託をした際に、再委託先が適切といえない取扱いを行ったことにより、何らかの問題が生じた場合は、元の委託者がその責めを負うことがあり得るので、再委託する場合は注意を要します。

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

①委託者及び受託者の責任の明確化
②個人データの安全管理に関する事項
・個人データの漏えい防止、盗用禁止に関する事項
・委託契約範囲外の加工、利用の禁止
・委託契約範囲外の複写、複製の禁止
・委託契約期間
・委託契約終了後の個人データの返還・消去・廃棄に関する事項
③再委託に関する事項
・再委託を行うに当たっての委託者への文書による報告
④個人データの取扱状況に関する委託者への報告の内容及び頻度
⑤契約内容が遵守されていることの確認（例えば、情報セキュリティ監査なども含まれます）
⑥契約内容が遵守されなかった場合の措置
⑦セキュリティ事件・事故が発生した場合の報告・連絡に関する事項

経済産業省のガイドライン

■ 苦情の処理

個人情報取扱事業者は、個人情報の取扱いに関する苦情の適切かつ迅速な処理に努めなければなりません。

また、苦情の適切かつ迅速な処理を行うに当たり、苦情処理窓口の設置や苦情処理の手順を定める等必要な体制の整備に努めなければなりません。

■ まとめ

個人情報保護法が全面施行されて２年が経過しました。社会全体での個人情報保護の意識も高まりを見せております。私たち印刷・グラフィックサービス業者にとっても情報と取扱とセキュリティ面の強化に努めなければなりません。残念なことに今年３月に大手印刷業者による大量の個人情報漏洩事故が発生しました。社団法人東京グラフィックサービス工業会では、３月19日に『声明』を発表し一層の注意喚起を図ったところでございます。

この小冊子は、経済産業省が３月末に「個人情報保護ガイドライン」を改定したことから、改めて事業者として遵守すべき事項を同ガイドラインに沿って編集いたしました。ご参考になさってください。そして、当業界から事故の再発を起こさないために全社で個人情報を大切に扱いましょう。

なお、私たち情報処理・加工に携わる業者として、以下の点はキチンと守りたいものです。

1.個人情報保護法，経済産業省「個人情報保護ガイドライン」をしっかりと遵守します。
2.全従業者に個人情報を扱う上での教育を必ず実施します。
3.委託先（協力企業）へ個人情報の処理・加工・発送等を委託する場合は、必ず契約を交わし、充分な監督を行ないます。
4.直接本人から受注する場合は、同意をとります。
5.顧客から個人情報を含んだ受注がある場合、顧客との契約のみならず受注する際に本人の同意を得ているか、再委託を行う同意を得ているかを確認します。
6.利用目的を逸脱する個人情報はお預かりしません。
7.事業の性質及び個人データの取扱い等に起因するリスクに応じ、必要かつ適切な組織的・人的・物理的・技術的安全管理措置を講じます。
8.情報漏洩等、緊急事態や苦情が発生した場合は、本人への被害を食い止める手順を定め、また関係官公庁及び認定個人情報保護団体である社団法人東京グラフィックサービス工業会へ連絡します。

「個人情報漏洩などの事故をなくすために…」

◇発行人：社団法人東京グラフィックサービス工業会　個人情報保護委員会
東京都中央区日本橋小伝馬町 7-16
電話 03-3667-3771　ＦＡＸ 03-3249-0377
ＵＲＬ：www.tokyographics.or.jp
◇発行日：平成１９年４月２５日
◇印　刷：㈱東京文久堂