

結婚情報サービス協議会における
個人情報保護指針

結婚情報サービス協議会
制定：2006（平成18）年2月23日

【目 次】

第1章	総 則	1
第2章	定 義	1
第3章	個人情報の取得等	9
第4章	個人データの管理	12
第5章	第三者への提供	24
第6章	保有個人データに関する事項の公表、 保有個人データの開示・訂正・利用停止等	25
第7章	内部規程・方針、管理体制等	28
第8章	そ の 他	29
	附 則	30

結婚情報サービス協議会における個人情報保護指針

第1章 総則

(目的)

第1条 この個人情報保護指針（以下「本指針」という。）は、個人情報の保護に関する法律（以下「法」という。）及び経済産業省の「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」その他の関係法令等に基づき、結婚情報サービス協議会（以下「協議会」という。）が、加盟会社が行う結婚相手紹介サービス事業（以下「当事業」という。）における個人情報の保護と適切な取扱いの確保に関する活動を支援する具体的な指針として定めたものであり、他の業種に類を見ない詳細かつ機密性の高い個人情報を取扱う当事業の特性に鑑み、個人情報の有用性に配慮するとともに、個人の権利利益を保護することにより、当事業の健全な発展に寄与することを目的とする。

(適用範囲)

第2条 本指針は、当事業において個人情報を取り扱う協議会の加盟会社に適用される。
2 前項に該当しない当事業において個人情報を取り扱う事業者においても、個人情報を取り扱う際の基準又は個人情報保護に関する規程を策定する際の参考として本指針を用いることができる。

なお、本指針中に事例として記述した部分は、理解を助けることを目的として、該当する事例及び該当しない事例のそれぞれにつき、典型的な例を示すものである。

第2章 定義

(定義)

第3条 本指針において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。

(1)「個人情報」

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、他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。

◎「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、暗号化されているかどうかを問わない。

◎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る。

◎また、「生存する個人」には日本国民に限られず、外国人も含まれるが、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ない（ただし、役員、従業員等に関する情報は個人情報）。

【個人情報に該当する事例】

- 事例1) 本人の氏名
- 事例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
- 事例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
- 事例4) 特定の個人を識別できるメールアドレス情報(kekkon-tarou@misc.or.jp 等のようにメールアドレスだけの情報の場合であっても、結婚情報サービス協議会に所属するケッコントロウのメールアドレスであることがわかるような場合等)
- 事例5) 特定個人を識別できる情報が記述されていない場合でも、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
- 事例6) 雇用管理情報（会社が従業員を評価した情報を含む。）
- 事例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る。）
- 事例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）

【個人情報に該当しない事例】

- 事例1) 企業の財務情報等、法人等の団体そのものに関する情報（団体情報）
- 事例2) 記号や数字等の文字列だけから特定個人の情報であるか否かの区別がつかないメールアドレス情報（例えば、abc012345@ispisp.jp。ただし、他の情報と容易に照合することによって特定の個人を識別できる場合は、個人情報となる。）
- 事例3) 特定の個人を識別することができない統計情報

(2) 「個人情報データベース等」

特定の個人情報をコンピュータを用いて検索することができるように体系的に構成した個

人情報を含む情報の集合物をいう。コンピュータを用いていない場合であっても、紙面で処理した個人情報を一定の規則（例えば、五十音順、年月日順等）に従って整理・分類し、特定の個人情報を容易に検索することができるよう、目次、索引、符号等を付し、他人によっても容易に検索可能な状態に置いているものも該当する。

【個人情報データベース等に該当する事例】

- 事例1) 電子メールソフトに保管されているメールアドレス帳（メールアドレスと氏名を組み合わせた情報を入力している場合）
- 事例2) ユーザーIDとユーザーが利用した取引についてのログ情報が保管されている電子ファイル（ユーザーIDを個人情報と関連付けて管理している場合）
- 事例3) 従業員が、名刺の情報を業務用パソコン（所有者を問わない。）の表計算ソフト等を用いて入力・整理し、他の従業員等によっても検索できる状態にしている場合
- 事例4) 氏名、住所、企業別に分類整理されている市販の人名録

【個人情報データベース等に該当しない事例】

- 事例1) 従業員が、自己の名刺入れについて他人が自由に検索できる状況に置いても、他人には容易に検索できない独自の分類方法により名刺を分類した状態である場合
- 事例2) アンケートの戻りはがきで、氏名、住所等で分類整理されていない状態である場合

(3) 「個人情報取扱事業者」

個人情報取扱事業者とは、その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないものを除いた、個人情報データベース等を当事業の用に供している者をいう。ここでいう、「その取り扱う個人情報の量及び利用方法からみて個人の権利利益を害するおそれが少ないもの」とは、その事業の用に供する個人情報データベース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月以内のいずれの日においても5000人を超えない者とする。

◎当事業は、他の業種に類を見ない詳細かつ機密性の高い個人情報を取扱う事業であることに鑑み、5000人を下回る場合であっても加盟会社に個人情報取扱事業者の義務等を遵守することを義務づけているが、非加盟会社にあっても個人情報取扱事業者の義務等を遵守することが望ましい。

(4) 「個人データ」

個人データとは、個人情報取扱事業者が管理する「個人情報データベース等」を構成する個人情報をいう。

【個人データに該当する事例】

事例1) 個人情報データベース等から他の媒体に格納したバックアップ用の個人情報

事例2) コンピュータ処理による個人情報データベース等から出力された帳票等に印字された個人情報

【個人データに該当しない事例】

事例) 個人情報データベース等を構成する前の入力帳票に記載されている個人情報

※電話帳、カーナビゲーションシステム等の取扱いについて

個人情報データベース等が、以下の要件のすべてに該当する場合であっても、その個人情報データベース等を構成する個人情報については、個人データとなる可能性も否定できない。しかしながら、その利用方法からみて個人の権利利益を侵害するおそれが少ないことから、個人情報取扱事業者の義務を課されないものと解釈する。

- ①個人情報データベース等の全部又は一部が他人の作成によるものである。
- ②その個人情報データベース等を構成する個人情報として氏名、住所（居所を含み、地図上又はコンピュータの映像面上において住所又は居所の所在場所を示す表示を含む。）又は電話番号のみを含んでいる。
- ③その個人情報データベース等を事業の用に供するに当たり、新たに個人情報を加え、識別される特定の個人を増やしたり、他の個人情報を付加したりして、個人情報データベース等そのものを変更するようなことをしていない。

(5) 「保有個人データ」

個人情報取扱事業者が、本人又はその代理人から求められる開示、内容の訂正、追加又は削除、利用の停止、消去及び第三者への提供の停止のすべてに応じることができる権限を有する「個人データ」をいう。ただし、次に掲げる場合は除く。

- [1] その存否が明らかになることにより、公益その他の利益が害されるもの。
- [2] 6か月以内に消去する（更新することは除く。）こととなるもの。

- ◎ 「その存否が明らかになることにより、公益その他の利益が害されるもの」とは、以下の場合を指す。
- i. その個人データの存否が明らかになることで、本人又は第三者の生命、身体又は財産に危害が及ぶおそれがあるもの。
 - 事例) 家庭内暴力、児童虐待の被害者の支援団体が、加害者（配偶者又は親権者）及び被害者（配偶者又は子）を本人とする個人データを持っている場合

 - ii. その個人データの存否が明らかになることで、違法又は不当な行為を助長し又は誘発するおそれがあるもの。
 - 事例1) いわゆる総会屋等による不当要求被害を防止するため、事業者が総会屋等を本人とする個人データを持っている場合
 - 事例2) いわゆる不審者、悪質なクレーマー等からの不当要求被害を防止するため、当該行為を繰り返す者を本人とする個人データを保有している場合

 - iii. その個人データの存否が明らかになることで、国の安全が害されるおそれ、他国若しくは国際機関との信頼関係が損なわれるおそれ又は他国若しくは国際機関との交渉上不利益を被るおそれがあるもの。
 - 事例1) 製造業者、情報サービス事業者等が、防衛に関連する兵器・設備・機器・ソフトウェア等の設計、開発担当者名が記録された個人データを保有している場合
 - 事例2) 要人の訪問先やその警備会社が、当該要人を本人とする行動予定や記録等を保有している場合

 - iv. その個人データの存否が明らかになることで、犯罪の予防、鎮圧又は捜査その他の公共安全と秩序の維持に支障が及ぶおそれがあるもの。
 - 事例) 警察からの捜査関係事項照会や捜索差押令状の対象となった事業者がその対応の過程で捜査対象者又は被疑者を本人とする個人データを保有している場合

(6) 「本人」

本人とは、個人情報によって識別される特定の個人をいう。

(7) 「本人に通知」

本人に直接知らしめることをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【本人への通知に該当する事例】

- 事例1) 面談においては、口頭又はちらし等の文書を渡すこと。
- 事例2) 電話においては、口頭又は自動応答装置等で知らせること。
- 事例3) 隔地者間においては、電子メール、ファックス等により送信すること、又は文書を郵便等で送付すること。
- 事例4) 電話勧誘販売において、勧誘の電話において口頭の方法によること。
- 事例5) 電子商取引において、取引の確認を行うための自動応答の電子メールに記載して送信すること。

(8)「公表」

広く一般に自己の意思を知らせること（国民一般その他不特定多数の人々が知ることができるように発表すること）をいう。ただし、公表に当たっては、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならない。

【公表に該当する事例】

- 事例1) 自社のウェブ画面中のトップページから1回程度の操作で到達できる場所への掲載、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等
- 事例2) 店舗販売においては、店舗の見やすい場所への掲示によること。
- 事例3) 通信販売においては、通信販売用のパンフレット等への記載によること。

(9)「本人に対し、その利用目的を明示」

本人に対し、その利用目的を明確に示すことをいい、事業の性質及び個人情報の取扱状況に応じ、内容が本人に認識される合理的かつ適切な方法によらなければならない。

【利用目的の明示に該当する事例】

- 事例1) 利用目的を明記した契約書その他の書面を相手方である本人に手渡し、又は送付すること（契約約款又は利用条件等の書面（電子的方式、磁気的方式その他の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。）中に利用目的条項を記載する場合は、例えば、裏面約款に利用目的が記

載されていることを伝える、又は裏面約款等に記載されている利用目的条項を表面にも記述する等本人が実際に利用目的を目にできるよう留意する必要がある。)

事例2) ネットワーク上においては、本人がアクセスした自社のウェブ画面上、又は本人の端末装置上にその利用目的を明記すること(ネットワーク上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等にその利用目的(利用目的の内容が示された画面に1回程度の操作でページ遷移するように設定したリンクやボタンを含む。)が本人の目にとまるようその配置に留意する必要がある。)

(10) 「本人の同意」

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う(当該本人であることを確認できていることが前提。)

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らない。

【本人の同意を得ている事例】

事例1) 同意する旨を本人から口頭又は書面(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。)で確認すること。

事例2) 本人が署名又は記名押印した同意する旨の申込書等文書を受領し確認すること。

事例3) 本人からの同意する旨のメールを受信すること。

事例4) 本人による同意する旨の確認欄へのチェック

事例5) 本人による同意する旨のウェブ画面上のボタンのクリック

事例6) 本人による同意する旨の音声入力、タッチパネルへのタッチ、ボタンやスイッチ等による入力

(11) 「本人が容易に知り得る状態」

事業の性質及び個人情報の取扱い状況に応じた合理的かつ適切な方法により、本人が知ろうとすれば、時間的にも、その手段においても、簡単に知ることができる状態に置いていることをいう。

【本人が容易に知り得る状態に該当する事例】

- 事例 1) ウェブ画面中のトップページから 1 回程度の操作で到達できる場所への掲載等が継続的に行われていること。
- 事例 2) 事務所の窓口等への掲示、備付け等が継続的に行われていること。
- 事例 3) 広く頒布されている定期刊行物への定期的掲載を行っていること。
- 事例 4) 電子商取引において、商品を紹介するウェブ画面にリンク先を継続的に掲示すること。

(12) 「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」
ホームページへの掲載、カタログの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうとすれば、知ることができる状態に置くことをいい、常にその時点での正確な内容を本人の知り得る状態に置かなければならない。

【本人の知り得る状態に該当する事例】

- 事例 1) 問い合わせ窓口を設け、問い合わせがあれば、口頭又は文章で回答できるような体制を構築しておくこと。
- 事例 2) 店舗販売において、店舗にパンフレットを備え置くこと。
- 事例 3) 電子商取引において、問い合わせ先のメールアドレスを明記すること。

(13) 「提供」

個人データを利用可能な状態に置くことをいう。個人データが、物理的に提供されていない場合であっても、ネットワーク等を利用することにより、個人データを利用できる状態にあれば（利用する権限が与えられていれば）、「提供」に当たる。

(14) 「加盟会社」

当事業において、個人情報を取り扱う協議会の会員会社をいう。保有個人データの数は問わない。

(15) 個人情報保護安全管理責任者

加盟会社によって指名された者で、個人情報保護体制の運営と施策の実施を行う責任者であって、個人情報の取扱いについて決定する権限を有する者である。

第3章 個人情報の取得等

(利用目的の特定)

第4条 加盟会社は、取り扱う個人情報の利用目的をできる限り特定しなければならない。顧客開発に当って広告により見込み客の個人情報を取得する際は、利用目的をできるだけ具体的に示さなければならない。

◎利用目的の特定を行うとともに、当事業の特徴からすると、顧客と窓口担当者の信頼関係が強まると、契約で定められた会員登録内容以上の深い個人情報を知り得ることが多い。こうした場合も契約上の役務の達成に必要な範囲を超えて、個人情報を得ないこと。

【具体的に利用目的を特定している事例】

事例1) 「結婚相手紹介サービスにおけるサービス内容の案内の発送、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。」

事例2) 「会員登録のため、また、入会後の相手会員への紹介等のサービスに利用いたします。」

【具体的に利用目的を特定していない事例】

事例1) 「事業活動に用いるため」

事例2) 「提供するサービスの向上のため」

事例3) 「マーケティング活動に用いるため」

(利用目的の変更)

第5条 加盟会社は、第4条により特定された利用目的を、本人が想定することが困難でない範囲内を超えて変更してはならない。

2 加盟会社は、利用目的を変更した場合は、変更された利用目的について、本人に通知するか、又は公表しなければならない。

◎本人が想定することが困難でないと認められる範囲内の基準

利用目的で示した個人情報を取り扱う事業の範囲を超えての変更は、あらかじめ本人の同意なく行うことはできない。

利用目的において、一連の個人情報の取扱いの典型を具体性をもって示していた場合は、その典型例から推測できる範囲内で変更することができる。

【本人が想定することが困難でないと認められる範囲内に該当する事例】

事例)「当社の行う結婚情報サービスにおける新商品・サービスに関する情報を電子メールにより送信することがあります。」とした利用目的において、「郵便によりお知らせすることがある」旨追加することは、許容される。

(利用目的による制限)

第6条 加盟会社は、利用目的の達成に必要な範囲を超えて、個人情報を取り扱う場合は、あらかじめ本人の同意を得なければならない。

◎同意を得るために個人情報を利用すること（メールの送付や電話をかけること等）は、当初の利用目的として記載されていない場合でも、目的外利用には該当しない。

【同意が必要な事例】

事例) 成婚退会の届けを提出してきた会員を、結婚式場業者や旅行業者に紹介する場合。

【適用除外事例】

事例1) 法令に基づき、提出又は回答が義務付けられている場合

事例2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

事例3) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

(適正な取得)

第7条 加盟会社は、偽り等の不正の手段により個人情報を取得してはならない。

◎なお、不正の競争の目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、詐欺等により取得したり、使用・開示した者には不正競争防止法（平成5年法律第47号）第14条により刑事罰（3年以下の懲役又は300万円以下の罰金）が科され得る。

【不正の手段により個人情報を取得している事例】

事例1) 法第23条に規定する第三者提供制限違反をするよう強要して個人情報を取得した場合

事例2) 他の事業者から指示して上記事例1) の不正の手段で個人情報を取得させ、その事業者から個人情報を取得する場合

(利用目的の通知又は公表)

第8条 加盟会社は、個人情報を取得する場合は、あらかじめその利用目的を公表していることが望ましい。公表していない場合は、取得後速やかに、その利用目的を、本人に通知するか、又は公表しなければならない。

【公表に該当する事例】

事例1) 自社のウェブ画面中のトップページから1回程度の操作で到達できる場所への掲載、自社の店舗・事務所内におけるポスター等の掲示、パンフレット等の備置き・配布等

事例2) 店舗販売においては、店舗の見やすい場所への掲示によること。

事例3) 通信販売においては、通信販売用のパンフレット等への記載によること。

(書面等で本人から直接に取得する場合の措置)

第9条 加盟会社は、書面等による記載、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には、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らない。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、この限りではない。

また、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ない。

(取得時及び利用目的等の変更時の措置の適用除外)

第10条 第5条、第8条及び第9条の規定は、次に掲げる場合については適用しない。

(1) 利用目的を本人に通知し、又は公表することにより人の生命、身体、財産その他の権利利益が侵害されるおそれがある場合。

(2) 利用目的を本人に通知し、又は公表することにより企業秘密に関する事等が他社に明らかになり、当該事業者の権利又は正当な利益が侵害されるおそれがある場合。

(3) 国の機関等が法令の定める事務を実施する上で、民間企業等の協力を得る必要がある場合であって、協力する民間企業等が国の機関等から受け取った個人情報の利用目的を本人に通知し、又は公表することにより、当該事務の遂行に支障を及ぼすおそれがある場合。

(4) 個人情報が取得される状況から見て利用目的が自明であると認められる場合。

第4章 個人データの管理

(データ内容の正確性の確保)

第11条 加盟会社は、利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手續の整備、誤り等を発見した場合の訂正等の手續の整備、記録事項の更新、保存期間の設定等を行うことにより、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らない。

(安全管理措置)

第12条 加盟会社は、その取り扱う個人データの漏洩、滅失又はき損の防止その他の個人情報の安全管理のため、組織的、人的、物理的及び技術的な安全管理措置を講じなければならない。

【必要かつ適切な安全管理措置を講じているとはいえない場合】

事例1) 公開されることを前提としていない個人データが事業者のウェブ画面上で不特定多数に公開されている状態を加盟会社が放置している場合

事例2) 組織変更が行われ、個人データにアクセスする必要がなくなった従事者が個人データにアクセスできる状態を加盟会社が放置していた場合で、その従事者が個人データを漏えいした場合

事例3) 本人が継続的にサービスを受けるために登録していた個人データが、システム障害により破損したが、採取したつもりのバックアップも破損しており、個人データを復旧できずに滅失又はき損し、本人がサービスの提供を受けられなくなった場合

事例4) 個人データに対してアクセス制御が実施されておらず、アクセスを許可されていない従業者がそこから個人データを入手して漏えいした場合

事例5) 個人データをバックアップした媒体が、持ち出しを許可されていない者により持ち出し可能な状態になっており、その媒体が持ち出されてしまった場合

(1) 組織的安全管理措置

【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個人データの取扱い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

《各項目について講じることが望まれる事項》

- 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をする上で望まれる事項
 - ◎従業員の役割・責任の明確化
 - ※個人データの安全管理に関する従業員の役割・責任を職務分掌規程、職務権限規程等の内部規程、契約書、職務記述書等に具体的に定めることが望ましい。
 - ◎個人情報保護管理者（いわゆる、チーフ・プライバシー・オフィサー（CPO））の設置
 - ◎個人データの取扱い（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄等の作業）における作業責任者の設置及び作業担当者の限定
 - ◎個人データを取り扱う情報システム運用責任者の設置及び担当者（システム管理者を含む。）の限定
 - ◎個人データの取扱いにかかわるそれぞれの部署の役割と責任の明確化
 - ◎監査責任者の設置
 - ◎監査実施体制の整備
 - ◎個人データの取扱いに関する規程等に違反している事実又は兆候があることに気づいた場合の、代表者等への報告連絡体制の整備
 - ◎個人データの漏えい等の事故が発生した場合、又は発生の可能性が高いと判断した場合の、代表者等への報告連絡体制の整備
 - ※個人データの漏えい等についての情報は代表窓口、苦情処理窓口を通じ、外部からもたらされる場合もあるため、苦情の処理体制等との連携を図ることが望ましい（法第31条を参照）。
 - ◎漏えい等の事故による影響を受ける可能性のある本人への情報提供体制の整備
 - ◎漏えい等の事故発生時における主務大臣及び認定個人情報保護団体等に対する報告体制の整備
- 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をする上で望まれる事項
 - ◎個人データの取扱いに関する規程等の整備とそれらに従った運用
 - ◎個人データを取り扱う情報システムの安全管理措置に関する規程等の整備とそれらに従った運用
 - ※なお、これらについてのより詳細な記載事項については、下記の【個人データの取扱いに関する規程等に記載することが望まれる事項】を参照。
 - ◎個人データの取扱いに係る建物、部屋、保管庫等の安全管理に関する規程等の整備とそれらに従った運用
 - ◎個人データの取扱いを委託する場合における受託者の選定基準、委託契約書のひな型等の整備とそれらに従った運用
 - ◎定められた規程等に従って業務手続が適切に行われたことを示す監査証拠の保持

※保持しておくことが望ましい監査証跡としては、個人データに関する情報システム利用申請書、ある従業者に特別な権限を付与するための権限付与申請書、情報システム上の利用者とその権限の一覧表、建物等への入退館（室）記録、個人データへのアクセスの記録（例えば、だれがどのような操作を行ったかの記録）、教育受講者一覧表等が考えられる。

- ③個人データの取扱い状況を一覧できる手段の整備をする上で望まれる事項
 - ◎個人データについて、取得する項目、通知した利用目的、保管場所、保管方法、アクセス権限を有する者、利用期限、その他個人データの適正な取扱いに必要な情報を記した個人データ取扱台帳の整備
 - ◎個人データ取扱台帳の内容の定期的な確認による最新状態の維持
- ④個人データの安全管理措置の評価、見直し及び改善をする上で望まれる事項
 - ◎監査計画の立案と、計画に基づく監査（内部監査又は外部監査）の実施
 - ◎監査実施結果の取りまとめと、代表者への報告
 - ◎監査責任者から受ける監査報告、個人データに対する社会通念の変化及び情報技術の進歩に応じた定期的な安全管理措置の見直し及び改善
- ⑤事故又は違反への対処をする上で望まれる事項
 - ◎事実関係、再発防止策等の公表
 - ◎その他、以下の項目等の実施
 - ア) 事実調査、イ) 影響範囲の特定、ウ) 影響を受ける可能性のある本人及び主務大臣等への報告、エ) 原因の究明、オ) 再発防止策の検討・実施

【個人データの取扱いに関する規程等に記載することが望まれる事項】

以下、（i）取得・入力、（ii）移送・送信、（iii）利用・加工、（iv）保管・バックアップ、（v）消去・廃棄という、個人データの取扱いの流れに従い、そのそれぞれにつき規程等に記載することが望まれる事項を列記する。

（i）取得・入力

i) 作業責任者の明確化

個人データを取得する際の作業責任者の明確化

取得した個人データを情報システムに入力する際の作業責任者の明確化

（以下、併せて「取得・入力」という。）

ii) 手続の明確化と手続に従った実施

取得・入力する際の手続の明確化

定められた手続による取得・入力の実施

権限を与えられていない者が立ち入れない建物、部屋（以下「建物等」という。）

での入力作業の実施

個人データを入力できる端末の、業務上の必要性に基づく限定
個人データを入力できる端末に付与する機能の、業務上の必要性に基づく限定
(例えば、個人データを入力できる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。)

iii) 作業担当者の識別、認証、権限付与

個人データを取得・入力できる作業担当者の、業務上の必要性に基づく限定
IDとパスワードによる認証、生体認証等による作業担当者の識別
作業担当者に付与する権限の限定
個人データの取得・入力業務を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認
アクセスの記録、保管と、権限外作業の有無の確認

(ii) 移送・送信

i) 作業責任者の明確化

個人データを移送・送信する際の作業責任者の明確化

ii) 手続の明確化と手続に従った実施

個人データを移送・送信する際の手続の明確化
定められた手続による移送・送信の実施
個人データを移送・送信する場合の個人データの暗号化（例えば、公衆回線を利用して個人データを送信する場合）移送時におけるあて先確認と受領確認（例えば、配達記録郵便等の利用）
FAX等におけるあて先番号確認と受領確認
個人データを記した文書をFAX等に放置することの禁止
暗号鍵やパスワードの適切な管理

iii) 作業担当者の識別、認証、権限付与

個人データを移送・送信できる作業担当者の、業務上の必要性に基づく限定
IDとパスワードによる認証、生体認証等による作業担当者の識別
作業担当者に付与する権限の限定（例えば、個人データを、コンピュータネットワークを介して送信する場合、送信する者は個人データの内容を閲覧、変更

する権限は必要ない。)

個人データの移送・送信業務を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

アクセスの記録、保管と、権限外作業の有無の確認

(iii) 利用・加工

i) 作業責任者の明確化

個人データを利用・加工する際の作業責任者の明確化

ii) 手続の明確化と手続に従った実施

個人データを利用・加工する際の手続の明確化

定められた手続による利用・加工の実施

権限を与えられていない者が立ち入れない建物等での利用・加工の実施

個人データを利用・加工できる端末の、業務上の必要性に基づく限定

個人データを利用・加工できる端末に付与する機能の、業務上の必要性に基づく、限定（例えば、個人データを閲覧だけできる端末では、CD-R、USBメモリ等の外部記録媒体を接続できないようにする。）

iii) 作業担当者の識別、認証、権限付与

個人データを利用・加工する作業担当者の、業務上の必要性に基づく限定

IDとパスワードによる認証、生体認証等による作業担当者の識別

作業担当者に付与する権限の限定（例えば、個人データを閲覧することのみが業務上必要とされる作業担当者に対し、個人データの複写、複製を行う権限は必要ない。）

個人データを利用・加工する作業担当者に付与した権限（例えば、複写、複製、印刷、削除、変更等）の記録

iv) 作業担当者及びその権限の確認

手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

アクセスの記録、保管と権限外作業の有無の確認

(iv) 保管・バックアップ

i) 作業責任者の明確化

個人データを保管・バックアップする際の作業責任者の明確化

ii) 手続きの明確化と手続きに従った実施

個人情報データを保管・バックアップする際の手順 (※) の明確化

※情報システムで個人情報データを処理している場合は、個人データのみならず、オペレーションシステム (OS) やアプリケーションのバックアップも必要となる場合がある。

定められた手順による保管・バックアップの実施

個人データを保管・バックアップする場合の個人データの暗号化

暗号鍵やパスワードの適切な管理

個人データを記録している媒体を保管する場合の施錠管理

個人データを記録している媒体を保管する部屋、保管庫等の鍵の管理

個人データを記録している媒体の遠隔地保管

個人データのバックアップから迅速にデータが復元できることのテストの実施

個人データのバックアップに関する各種事象や障害の記録

iii) 作業担当者の識別、認証、権限付与

個人データを保管・バックアップする作業担当者の、業務上の必要性に基づく限定

IDとパスワードによる認証、生体認証等による作業担当者の識別

作業担当者に付与する権限の限定 (例えば、個人データをバックアップする場合、その作業担当者は個人データの内容を閲覧、変更する権限は必要ない。)

個人データの保管・バックアップ業務を行う作業担当者に付与した権限 (例えば、バックアップの実行、保管庫の鍵の管理等) の記録

iv) 作業担当者及びその権限の確認

手続きの明確化と手続きに従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

アクセスの記録、保管と権限外作業の有無の確認

(v) 消去・廃棄

i) 作業責任者の明確化

個人データを消去する際の作業責任者の明確化

個人データを保管している機器、記録している媒体を廃棄する際の作業責任者の明確化

ii) 手続の明確化と手続に従った実施

消去・廃棄する際の手続の明確化

定められた手続による消去・廃棄の実施

権限を与えられていない者が立ち入れない建物等での消去・廃棄作業の実施

個人データを消去できる端末の、業務上の必要性に基づく限定

個人データが記録された媒体や機器をリース会社に返却する前の、データの完全消去（例えば、意味のないデータを媒体に1回又は複数回上書きする。）

個人データが記録された媒体の物理的な破壊（例えば、シュレッダー、メディアシュレッダー等で破壊する。）

iii) 作業担当者の識別、認証、権限付与

個人データを消去・廃棄できる作業担当者の、業務上の必要性に基づく限定

IDとパスワードによる認証、生体認証等による作業担当者の識別

作業担当者に付与する権限の限定

個人データの消去・廃棄を行う作業担当者に付与した権限の記録

iv) 作業担当者及びその権限の確認

手続の明確化と手続に従った実施及び作業担当者の識別、認証、権限付与の実施状況の確認

アクセスの記録、保管、権限外作業の有無の確認

(2) 人的安全管理措置

【人的安全管理措置として講じなければならない事項】

①雇用契約時及び委託契約時における非開示契約の締結

②従業者に対する教育・訓練の実施

なお、管理者が定めた規程等を守るように監督することについては、法第21条を参照。

《各項目について講じることが望まれる事項》

①雇用契約時及び委託契約時における非開示契約の締結をする上で望まれる事項

◎従業者の採用時又は委託契約時における非開示契約の締結

※雇用契約又は委託契約等における非開示条項は、契約終了後も一定期間有効であるようにすることが望ましい。

◎非開示契約に違反した場合の措置に関する規程の整備

※個人データを取り扱う従業者ではないが、個人データを保有する建物等に立ち入る可能性がある者、個人データを取り扱う情報システムにアクセスする可能性がある者についてもアクセス可能な関係者の範囲及びアクセス条件について契約書等に明記することが望ましい。なお、個人データを取り扱う従業者以外の者には、情報システムの開発・保守関係者、清掃担当者、警備員等が含まれる。

②従業者に対する周知・教育・訓練を実施する上で望まれる事項

◎個人データ及び情報システムの安全管理に関する従業者の役割及び責任を定めた内部規程等についての周知

◎個人データ及び情報システムの安全管理に関する従業者の役割及び責任についての教育・訓練の実施

◎従業者に対する必要かつ適切な教育・訓練が実施されていることの確認

(3) 物理的安全管理措置

【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

《各項目について講じることが望まれる事項》

①入退館（室）管理を実施する上で望まれる事項

◎個人データを取り扱う業務上の、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盗難等を防止する上で望まれる事項

◎離席時の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

◎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・装置等を物理的に保護する上で望まれる事項

◎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

（４）技術的安全管理措置

【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

《各項目について講じることが望まれる事項》

①個人データへのアクセスにおける識別と認証を行う上で望まれる事項

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アクセス権限を有する従業者本人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各従業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行う上で望まれる事項

個人データへのアクセス権限を付与すべき従業者数の最小化

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。）

従業者に付与するアクセス権限の最小化

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、業務上必要となる従業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行う上で望まれる事項

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行う上で望まれる事項

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施する上

で望まれる事項

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）・送信時の対策の上で望まれる事項

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）

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、本人及び従業員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

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の上で望まれる事項

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行う上で望まれる事項

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可能性があることに留意する。

（従業員の監督）

第13条 加盟会社は、その従業員に個人データを取り扱わせるときは、安全管理措置を遵守させるよう、従業員に対し必要かつ適切な監督を行わなければならない。

なお、「従業員」とは、個人情報取扱事業者の組織内にあつ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、監査役、監事、派遣社員等も含まれる。

【従業者に対して必要かつ適切な監督を行っていない場合】

事例1) 従業者が、個人データの安全管理措置を定める規程等に従って業務を行っていることを、あらかじめ定めた間隔で定期的に確認せず、結果、個人データが漏えいした場合

事例2) 内部規程等に違反して個人データが入ったノート型パソコンを繰り返し持ち出されていたにもかかわらず、その行為を放置した結果、紛失し、個人データが漏えいした場合

(委託先の監督)

第14条 加盟会社は、個人データの取扱いの全部又は一部を外部に委託する場合、その取扱いを委託した個人データの安全管理が図られるよう、委託先に対し必要かつ適切な監督を行わなければならない。

【受託者に必要かつ適切な監督を行っていない場合】

事例1) 個人データの安全管理措置の状況を契約締結時及びそれ以後も定期的に把握せず外部の事業者へ委託した場合で、受託者が個人データを漏えいした場合

事例2) 個人データの取扱いに関して定めた安全管理措置の内容を受託者に指示せず、結果、受託者が個人データを漏えいした場合

事例3) 再委託の条件に関する指示を受託者に行わず、かつ受託者の個人データの取扱状況の確認を怠り、受託者が個人データの処理を再委託し、結果、再委託先が個人データを漏えいした場合

【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る。）

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

第5章 第三者への提供

(第三者提供の制限)

第15条 加盟会社は、次に掲げる場合を除くほか、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。

(1) 法令に基づく場合

(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

2 同意の取得に当たっては、当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範囲の内容を明確に示さなければならない。

【第三者提供とされる事例】(ただし、法第23条第4項各号の場合を除く。)

事例1) 親子兄弟会社、グループ会社の間で個人データを交換する場合

事例2) フランチャイズ組織の本部と加盟店の間で個人データを交換する場合

事例3) 同業者間で、特定の個人データを交換する場合

事例4) 外国の会社に国内に居住している個人の個人データを提供する場合

【第三者提供とされない事例】(ただし、利用目的による制限がある。)

事例1) 契約に基づくサービス提供で相手会員への個人データを提供すること。

事例2) 同一事業者内で他部門へ個人データを提供すること。

(第三者に提供できる場合)

第16条 加盟会社は、第三者に提供される個人データについて、本人の求めに応じてその提供を停止することとしている場合であって、次に掲げる事項について、あらかじめ本人に通知し、又は本人が容易に知り得る状態に置いているときは、当該個人データを第三者に提供することができる。

(1) 第三者への提供を利用目的とすること。

(2) 第三者に提供される個人データの項目

(3) 第三者への提供の手段又は方法

(4) 本人の求めに応じて第三者への提供を停止すること。

(第三者提供に該当しない場合)

第17条 次に掲げる場合においては、第三者提供に該当しないものとする。

(1) 利用目的の達成に必要な範囲内において、個人データの取り扱いに関する業務の全部又は一部を委託する場合

(2) 合併、分社化、営業譲渡等により事業が承継され個人データが移転される場合

(3) 個人データを特定の者との間で共同して利用する場合で、以下の情報をあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いている場合

[1] 個人データを特定の者と共同して利用する旨

[2] 共同して利用される個人データの項目

[3] 共同利用者の範囲

[4] 利用する者の利用目的

[5] 開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称

2 加盟会社は、前項(3)に規定する項目のうち、[4]又は[5]を変更する場合は、変更する内容について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置かなければならない。

第6章 保有個人データに関する事項の公表、保有個人データの開示・訂正・利用停止等

(保有個人データに関する事項の公表等)

第18条 加盟会社は、保有個人データについて、以下の情報を本人の知り得る状態(本人の求めに応じて遅滞なく回答する場合を含む。)に置かなければならない。

(1) 事業者の氏名又は名称

(2) すべての保有個人データの利用目的

(3) 保有個人データの利用目的の通知及び保有個人データの開示に係る手数料の額(定めた場合に限る)並びに開示等の求めの手續

(4) 保有個人データの取扱いに関する苦情及び問い合わせの申出先

(利用目的の通知)

第19条 加盟会社は、本人から自己が識別される保有個人データの利用目的の通知を求められたときは、遅滞なく、本人に通知しなければならない。なお、通知しない旨を決定したときも、遅滞なく、本人に通知しなければならない。ただし、次のいずれかに該当する場合は、この限りではない。

- (1) 前条の規定により当該本人が識別される保有個人データの利用目的が明らかな場合
- (2) 第 10 条の (1) から (3) に該当する場合

(保有個人データの開示)

第 20 条 加盟会社は、本人から、自己が識別される保有個人データの開示を求められたときは、本人に対し、書面の交付による方法等（開示の求めを行った者が同意した方法があるときはその方法）により、遅滞なく、当該保有個人データを開示（当該保有個人データが存在しないときにその旨を知らせることを含む。）しなければならない。ただし、開示することにより次のいずれかに該当する場合は、その全部又は一部を開示しないことができるが、その場合は、その旨を本人に通知しなければならない。

- (1) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
- (2) 業務の適正な実施に著しい支障を及ぼすおそれがある場合
- (3) 他の法令に違反することとなる場合

※「開示の求めを行った者が同意した方法があるときはその方法」について

開示の方法としては、求めを行った者が同意している場合には電子メール、電話等様々な方法が可能であり、書面の交付による方法は同意がなくても可能との意味である。

また、開示の求めを行った者から開示の方法について特に指定がなく、加盟会社が提示した方法に対して異議を述べなかった場合（電話での開示の求めがあり、必要な本人確認等の後、そのまま電話で問い合わせに回答する場合を含む。）は、当該方法について同意があったものとみなすことができる。開示の求めがあった者からの同意の取り方として、加盟会社が開示方法を提示して、その者が希望する複数の方法の中から当該加盟会社が選択することもできる。

ただし、開示することにより上記の (1) ～ (3) のいずれかに該当する場合は、その全部又は一部を開示しないことができるが、この場合は、その旨を本人に通知しなければならない。

(保有個人データの訂正等)

第 21 条 加盟会社は、本人から、保有個人データの内容が事実でないという理由で訂正、追加又は削除（この条において「訂正等」という。）を求められたときには、利用目的の達成に必要な範囲内において、原則として合理的な期間内にこれに応ずるものとする。

なお、他の法令の規定により特別の手続が定められている場合には、当該特別の手続が優先されることとなる。

2 訂正等を行うにあたって、調査が必要な場合は、遅滞なく調査を行い、その結果に基づ

き訂正等を行ったとき又は行わない旨の決定をしたときは、本人に対し、その旨（訂正等を行ったときはその内容を含む。）通知しなければならない。

（保有個人データの利用停止等）

第22条 加盟会社は、本人から、手続違反の理由により保有個人データの利用停止等が求められた場合には、原則として、当該措置を行わなければならない。なお、利用停止等を行った場合には、遅滞なく、その旨を本人に通知しなければならない。ただし、当該保有個人データの第三者への提供の停止に多額の費用を要する場合その他の第三者への提供を停止することが困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

※1 「手続違反」とは、同意のない目的外利用、不正な取得、又は同意のない第三者提供をいう。

※2 退会（中途解約を含む）者の個人情報については、当然にも「利用停止」となるが、単に利用を停止するだけでなく、一定期間後に個人データそのものを抹消することが加盟会社に求められる。

※3 資料請求者等の見込み顧客の個人情報についても、一旦応募したもののその後自己の個人情報について訂正、削除等の申し出があった場合は速やかに行うこと。また、入会勧誘の結果、入会に至らず、それ以降は見込み顧客でないと判断したときは2月以内に抹消すること。

（理由の説明）

第23条 加盟会社は、保有個人データの公表・開示・訂正・利用停止等において、その措置をとらない旨又はその措置と異なる措置をとる旨を本人に通知する場合は、併せて、本人に対して、その理由を説明するように努めなければならない。

（開示等の求めに応じる手続）

第24条 加盟会社は、開示等の求めにおいて、その求めを受け付ける方法として、次の各号の事項を定めることができる。また、その求めを受け付ける方法を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置いておかなければならない。

- （1）開示等の求めの受付先
- （2）開示等の求めに際して提出すべき書面の様式、その他の開示等の求めの受付方法
- （3）開示等の求めをする者が本人又はその代理人であることの確認の方法
- （4）保有個人データの利用目的の通知、又は保有個人データの開示をする際に徴収する

手数料の徴収方法

なお、開示等の求めを受け付ける方法を定めない場合には、自由な申請を認めることとなる。

2 加盟会社は、円滑に開示等の手続が行えるよう、本人に対し、自己のデータの特定に必要な事項の提示を求めることができる。なお、本人が容易に自己のデータを特定できるよう、自己の保有個人データの特定に資する情報の提供その他本人の利便性を考慮しなければならない。

(手数料)

第 25 条 加盟会社は、保有個人データの利用目的の通知、又は保有個人データの開示を求められたときは、当該措置の実施に関し、手数料の額を定め、徴収することができる。また、手数料の額を定めた場合には、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置いておかなければならない。

なお、手数料を徴収する場合は、実費を勘案して合理的であると認められる範囲内において、その手数料の額を定めなければならない。

(苦情処理)

第 26 条 加盟会社は、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らない。

2 苦情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らない。

第 7 章 内部規程・方針、管理体制等

(個人情報保護方針の公表)

第 27 条 加盟会社は、個人情報保護方針を定め、文書化することとする。

2 加盟会社は、個人情報保護方針を公表することとする。

3 加盟会社は、法の施行後の状況等諸環境の変化を踏まえて、個人情報保護方針の見直しを行うよう努めるものとする。

(内部規程の策定等)

第 28 条 加盟会社は、個人情報保護方針を基に、事業活動の範囲及び事業規模を考慮し、個人情報を保護するための内部規程を策定し、これを実行することとする。

2 加盟会社は、内部規程を従業者に周知しなければならない。

3 加盟会社は、個人情報保護の実施状況及びその他の経営環境等に照らして、適切な個人情報の保護を維持するために、定期的に内部規程を見直すものとする。

(個人情報保護安全管理責任者の指名)

第 29 条 加盟会社は、法及びその他の関係法令や本指針を理解し実践する能力のある者を加盟会社の内部から 1 名以上指名し、個人情報保護安全管理責任者としての業務を行わせるものとする。

(個人情報保護安全管理責任者の責務)

第 30 条 個人情報保護安全管理者は、本指針に定められた事項を理解し、及び遵守するとともに、従業者にこれを理解させ、及び遵守させるための内部規程の整備、安全対策の実施、従業者への教育訓練、委託先の適切な監督等を実施する責任を負うものとする。

第 8 章 その他

(報告等)

第 31 条 加盟会社は、個人情報の取扱いに関し、協議会及び経済産業省等関係機関から報告を求められた場合は直ちに報告しなければならない。

2 加盟会社は、本人の同意のない第三者へ個人情報が漏洩した事実、及び漏洩したおそれがある事実を把握した場合は、協議会及び経済産業省等関係機関に報告するものとする。

3 加盟会社は個人情報の漏洩等の事案が発生した場合は、二次被害の防止、類似事案の発生回避等の観点及び本人が被る権利利益の侵害の大きさを考慮し、可能な限り事実関係等を公表するものとする。

(指導、勧告その他の措置)

第 32 条 加盟会社の個人情報の取扱いが、本指針に違反していると認められるときは、協議会は、法第 4 3 条第 2 項の規定に基づき、当該加盟会社に対して、以下のとおり指導、勧告その他の措置をとるものとする。

(1) 指導

当該加盟会社に対して、当該違反行為の中止その他違反を是正するために必要な措置をとるよう口頭または文書により指導するものとする。

(2) 勧告

前項の規定による指導を受けた加盟会社が正当な理由なくその指導に従わなかった場合において、個人の権利利益を保護するため必要と認めるときは、当該加盟会社に対して、その指導に係る措置をとるべきことを文書により勧告するものとする。

(3) その他の措置

前項の規定による勧告を受けた加盟会社が正当な理由がなくその勧告に従わなかった場合には、別に定めるところにより、その他の措置をとる。

(指針の見直し)

第 33 条 本指針は、社会情勢の変化、国民の認識の変化、技術の進歩等、法の施行後の状況等諸環境の変化を踏まえて不断の見直しを行うよう努めるものとする。

附則

1. 本指針は、平成 18 年 2 月 23 日から施行する。

以上