

保険代理店業務に係る個人情報取扱規程

代理店名：龍谷メルシー

第1章 総則

第1条（目的）

本規程は、当代理店における保険代理店業務に係わる個人情報の適法かつ適正な取扱いの確保に関する基本的事項を定めることにより、個人の権利・利益を保護することを目的とする。

第2条（定義）

本規程における各用語の定義は、「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。）および「個人情報の保護に関する法律についてのガイドライン」「金融分野における個人情報保護に関するガイドライン」（以下「ガイドライン」という。）によるものとする。

第3条（適用）

本規程は、当代理店の従業者（保険募集に従事するか否かを問わない。）に適用する。

第4条（個人情報の安全管理に係わる基本方針）

1. 当代理店における個人情報の適法かつ適正な取扱いを確保するため、次の事項を含む個人情報の安全管理に係わる基本方針を定める。
 - （1）当代理店の名称
 - （2）安全管理措置に関する質問及び苦情処理の窓口
 - （3）個人データの安全管理に関する宣言
 - （4）基本方針の継続的改善の宣言
 - （5）関係法令等遵守の宣言
 - （6）個人情報の利用目的
2. 個人情報の安全管理に係わる基本方針は、当代理店の従業者に周知すると共に、当代理店のホームページへの掲載、事務所への掲示等により公表する。

第2章 管理体制

第5条（情報管理総括部署）

総務部を、当代理店におけるお客さま情報の取扱いの点検・改善等の監督を行う情報管理総括部署とする。

第6条（個人データ管理責任者）

1. 当代理店は、【保険部門責任者】を個人情報の安全管理に係わる業務遂行の総責任者（個人データ管理責任者）として兼務させる。
2. 個人データ管理責任者は、次に掲げる業務を所管する。
 - （1）個人データの安全管理に関する規程及び委託先の選定基準の承認及び周知
 - （2）個人データ管理者及び「本人確認に関する情報」の管理者の任命
 - （3）個人データ管理者からの報告徴収及び助言・指導
 - （4）個人データの安全管理に関する教育・研修の企画
 - （5）個人データ取扱者の把握（「個人データ取扱者リスト」の整備）
 - （6）個人データの取扱いの点検・改善等の監督
 - （7）情報セキュリティに関する新たなリスクが顕在化した場合の対応状況の確認
 - （8）その他当代理店における個人データの安全管理に関すること

＝代理店において個人データ取扱部署が単一の場合＝

3. 前項（2）に定める個人データ管理者は、個人データ管理責任者が兼務することができる。
4. 第2項（2）に定める本人確認に関する情報の管理者は、個人データ管理者が兼務することができる。

第7条（個人データ管理者）

個人データ管理者は、次に掲げる業務を所管する。

- （1）個人データ取扱者の指定及び変更等の管理
- （2）個人データの利用申請の承認及び記録等の管理
- （3）個人データを取り扱う保管媒体の設置場所の指定及び変更等
- （4）個人データの管理区分及び権限についての設定及び変更の管理
- （5）個人データの取扱状況の把握
- （6）委託先における個人データの取扱状況等の監督
- （7）個人データの安全管理に関する教育・研修の実施
- （8）個人データ管理責任者に対する報告
- （9）その他所管部署における個人データの安全管理に関すること

第8条（点検・監査の実施）

1. 個人データ管理責任者は、別に定める個人データの取扱状況の点検及び監査に係わる規程に基づき、個人データの取扱いに関する法令及び諸規定の遵守状況に関する点検または監査の実施計画を立案し、個人データ取扱部署毎に点検または監査を定期的の実施させる。
2. 点検の実施責任者は当該取扱部署の個人データ管理者とし、点検結果を個人データ管理責任者へ報告する。
3. 監査の実施責任者は当該取扱部署以外の個人データ管理者とし、点検結果を個人データ管理責任者へ報告する。

第9条（体制の見直し）

個人データ管理責任者は、前条の点検または監査の結果を踏まえ、必要に応じて個人データの取扱いに関する組織体制の見直しを行わなければならない。

第10条（秘密の保持）

保険会社の保険業務の委託を受けて取得した個人情報または個人データについて、委託契約の継続中および委託契約終了後も、法令又は行政当局により求められる場合を除き、第三者に開示してはならない。また、法令または行政当局により個人データの開示を求められた場合には、保険会社の指示に従わなければならない。

第11条（委託契約終了時における個人情報の返却等）

1. 委託契約書第25条に基づき、委託契約が契約期間の満了、解除等で終了した場合、保険会社の保険業務の委託を受けて取得した個人情報または個人データの取扱いについて、保険会社の指示に従わなければならない。
2. 前項の義務の履行の確認を保険会社が行う場合、および、保険会社の保険業務の委託を受けて取得した個人情報は個人データを新たに指定するほかの代理店に取り扱わせるにあたり、保険会社に協力しなければならない。

第3章 運用

第12条（管理原則）

個人情報および個人データは、本規程に従い適切に管理し、その重要度に応じて取得、利用、移送、保管、廃棄する。

第13条（利用目的）

1. 当代理店は、個人情報の利用目的をできる限り特定する。
2. 個人情報は、あらかじめ本人の同意を得ずに、特定された利用目的の達成に必要な範囲を超えて取り扱ってはならない。
3. 利用目的を変更する場合には、変更前の利用目的と相当の関連性を有すると認められる範囲を超えて行ってはならず、変更された利用目的は遅滞なく本人に通知または公表を行う。

第14条（目的外利用の禁止）

保険会社が本人に対して通知、公表、明示している利用目的の範囲内で委託業務に関する個人情報または個人データを取り扱うこととし、委託業務遂行以外の目的で、個人情報または個人データを利用、加工または複製を

行うことはできない。

ただし、保険会社が通知、公表、明示している利用目的とは別に、自らが本人に対して利用目的を通知、公表、明示している範囲内で個人情報または個人データを取り扱うことができる。

第15条（適正な取得）

1. 直接・間接を問わず、偽りその他不正な手段により、個人情報を取得してはならない。
2. 直接・間接を問わず、「行政手続における特定個人を識別するための番号の利用等に関する法律」で定められる個人番号を取得してはならない。
3. 第三者からの提供により個人情報を取得する場合は、提供元の法の遵守状況を確認するとともに、個人情報を適切に管理している者を提供元として選定する。

第16条（利用目的の通知・公表・明示）

1. 当代理店は、個人情報の取得に際し、当代理店の利用目的をあらかじめ公表している場合を除きその利用目的を本人に通知する。
2. 当代理店は、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利用目的を明示する。ただし、人の生命、身体また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ない。

第17条（センシティブ情報）

1. 要配慮個人情報（人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報などをいう）ならびに労働組合への加盟、門地および本籍地、保健医療および性生活（これらのうち要配慮個人情報に該当するものを除く）に関する情報（以下、「センシティブ情報」という。）については、ガイドラインで定められる場合を除き、取得、利用または第三者提供を行わない。
2. センシティブ情報を取得、利用または第三者提供する場合は、あらかじめ本人の同意を取得する。

第18条（個人データの正確性の確保）

当代理店は、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ものとする。

第19条（個人データ管理台帳）

個人データ管理責任者は、個人データの取扱状況を確認できる手段の整備のため、以下の事項を含む台帳等を整備すると共に、適宜見直しを行うものとする。

- ① 取得項目
- ② 利用目的
- ③ 保管場所・保管方法・保管期限
- ④ 管理部署
- ⑤ アクセス制御の状況

第20条（安全管理措置）

1. 当代理店は、取り扱う個人データの漏えい、滅失または毀損（以下「漏えい等」という）の防止その他個人データの安全管理のため、組織的、人的、物理的、技術的に必要かつ適切な措置（以下「安全管理措置」という。）を講じるものとする。
2. 組織的安全管理措置として、個人データの安全管理に係わる取扱規程を整備する。取扱規程は、「取得・入力」「利用・加工」「保管・保存」「移送・送信」「消去・廃棄」「漏えい等事案への対応」の個人データの各管理段階毎に定めるものとする。

第21条（漏えい時の対応）

1. 従業者は、個人情報または個人データの漏えい等事故またはそのおそれのある事案を発見した場合は、直ちにその旨を個人データ管理者に報告し、その指示を受けなければならない。
2. 個人データ管理者は、個人情報または個人データの漏えい等事故またはそのおそれのある事案が発生した旨を直ちに個人データ管理責任者に報告しなければならない。

第22条（従業者の監督）

1. 当代理店は、個人データの安全管理が図られるよう、その従業者に対する必要かつ適切な監督を行う。
2. 当代理店は、従業者に対して個人情報の保護及び適正な取扱いに関する誓約書等の提出を求める。

第23条（従業者の教育・指導）

1. 従業者に対する個人情報の保護及び適正な取扱いに関する教育・指導方針は、個人データ管理責任者が計画、決定する。
2. 従業者は、個人データ管理責任者が指定する個人情報の適正な管理に関する研修を受講しなければならない。

第24条（委託先の監督）

1. 個人データ管理責任者は、個人データの取扱いの全部または一部を外部に委託する場合は、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、別に定める個人データの外部委託に係わる規程に基づき、委託先に対する必要かつ適切な監督を行わなければならない。
2. 個人データ管理責任者は、委託先に対し以下の各号の事項を実施しなければならない。
 - (1) 委託先の個人情報保護体制が十分であることを確認した上で委託先を選定すること
 - (2) 個人データの取扱いを外部委託するにあたっては、事前に保険会社に書面により申請し、承認を得ること
 - (3) 委託先との間で、次の事項を含む委託契約書等を締結すること
 - ① 委託者の監督・監査・報告徴収に関する権限
 - ② 委託先における個人データの漏えい、盗用、改ざん及び目的外利用の禁止
 - ③ 再委託における条件
 - ④ 漏えい等事案が発生した際の委託先の責任

第25条（第三者提供の制限）

当代理店は、法令で定められた場合を除き、あらかじめ本人の同意なく個人データの第三者への提供を行わない。

第26条（個人データの開示・訂正・利用停止）

1. 当代理店は、保険代理店業務に係わる個人データに関し、個人情報保護法に基づく開示・訂正・利用停止等の求めを受けた場合は、保険会社にその旨を連絡するものとする。
2. 保険代理店業務に係わる個人データに関し、個人情報保護法に基づかない照会等を受けた場合は、本人確認を適切に行った上で当代理店から回答を行うことができる。

第27条（苦情の処理）

1. 当代理店における個人情報の取扱いに関する苦情対応の窓口は、個人データ管理者とする。
2. 従業者が、個人情報の取扱いに関する苦情を受け付けた場合は、直ちに個人データ管理者に報告し、その指示を受けなければならない。
3. 個人データ管理者は、苦情を受け付けた旨を速やかに個人データ管理責任者に報告しなければならない。

第28条（罰則／違反時の懲戒）

当代理店は、本規程に違反した従業者に対して就業規則等に基づき懲戒処分を行う。

第29条（改廃）

本規程の改廃は、代理店主の決定または取締役会の決議により行うものとする。

<附則>

第1条 本規程は 2022年4月1日より実施する。

以上

個人データの安全管理に係る取扱規程

保険代理店業務に係わる個人情報取扱規程第20条第2項に定める個人データの安全管理に係わる取扱規程を以下

のとおり定める。

1. 取得・入力段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人情報の「取得・入力」段階の取扱いについて定めたものである。

第2条（定義）

1. 「取得」とは、本人または第三者から個人情報を物理的及び電子的手段により取得することなどをいう（当代理店内の他部門からの取得は含まない）。
2. 「入力」とは、取得した個人情報をデータベース等の情報システムに物理的及び電子的に入力することなどをいう。

第3条（取得・入力に関する取扱者の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、個人情報の取得・入力に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2. 個人データ管理者は、各部署において業務上必要な者に限り個人情報の取得・入力が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の取得・入力に関する取扱者の限定）

個人データ管理者は、要配慮個人情報（人種、信条、社会的身分、病歴、前科・前歴、犯罪被害情報などをいう）ならびに労働組合への加盟、門地および本籍地、保健医療および性生活（これらのうち要配慮個人情報に該当するものを除く）に関する情報（以下、各取扱規程において「センシティブ情報」という。）の取得・入力の取扱者を必要最小限に限定しなければならない。

第5条（取得・入力の対象となる個人データの限定）

個人データ管理者は、取得・入力する個人情報を業務上必要な範囲内のものに限定しなければならない。

第6条（取得・入力時の照合及び確認手続）

1. 個人データの取扱者は、個人情報を取得するときには、情報提供者の本人確認及び権限等の確認を行わなければならない。
2. 個人データの取扱者は、個人情報を入力するときには、入力データが正確であることを確認しなければならない。

第7条（個人データの提供、取得時の確認・記録）

個人データの取扱者は、法令で定める場合を除き、個人データを第三者に提供した場合には当該提供に関する事項（提供日、提供先名称、提供内容等）について記録し、個人データを第三者から取得する場合には当該取得に関する事項（取得日、取得先名称、取得経緯、取得内容等）について確認・記録を行わなければならない。

第8条（取得・入力の規格外作業に関する申請及び承認手続）

個人データの取扱者は、本規程に定める以外の方法で個人情報を取得・入力する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第9条（機器・記録媒体等の管理手続）

1. 個人データ管理者は、取得・入力した個人情報が保存された機器・記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じ変更しなければならない。
2. 個人データの取扱者は、前項の指定及び設定に従い、個人情報が保存された機器・記録媒体等を適切に保管しなければならない。

第10条（個人データへのアクセス制御）

個人データ管理者は、取得・入力した個人情報へのアクセスを制御するために、取得・入力した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

- ① 個人データの入力に必要なID及びパスワードの管理を徹底する。
- ② 個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

- ① 受信した郵便物やFAX等の個人情報について適切な管理を行う。

第11条（取得・入力状況の記録及び分析）

1. 個人データの取扱者は、個人情報を取得・入力する場合、情報の種類や形態等に応じて、必要に応じ、かつ適切に取得・入力状況について記録を行わなければならない。
2. 個人データ管理者は、個人情報の漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第12条（センシティブ情報の取得の制限）

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、取得してはならない。

- ① 保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を取得する場合
- ② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を取得する場合
- ③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属もしくは加盟に関する従業員等のセンシティブ情報を取得する場合
- ④ 前各号のほか、金融分野ガイドライン第5条第1項各号に掲げる場合

第13条（センシティブ情報の取得に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項）

1. 個人データの取扱者は、前条①に基づきセンシティブ情報を取得する場合には、当該センシティブ情報を保険業の適切な業務運営を確保する必要性から、本人の同意（原則として書面による。）に基づき業務遂行上必要な範囲で取得しなければならない。
2. 個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を取得してはならない。
3. 個人データの取扱者は、郵送等により取得した個人データが含まれる文書等にセンシティブ情報が含まれている場合は、原則として、本人の指定した方法により、当該情報を速やかに本人に返却もしくは廃棄する。ただし、当該文書等に記載された他の情報が業務遂行上必要な場合、個人データの取扱者は、直ちに当該センシティブ情報の記載部分を判読不能な状態にして取得するものとする。

2. 利用・加工段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人データの「利用・加工」段階の取扱いについて定めたものである。

第2条（定義）

1. 「利用」とは、個人データを利用目的の範囲内で取り扱うことなどをいう。
2. 「加工」とは、個人データの更新を行うこと、または個人データを利用し、新たなデータベースを作成することなどをいう。
3. 「管理区域」とは、営業範囲を勘案してあらかじめ指定した区域をいう。

第3条（利用・加工に関する取扱者の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、個人データの利用・加工に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2. 個人データ管理者は、各部署において、業務上必要な者に限り個人データの利用・加工が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の利用・加工に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の利用・加工の取扱者を必要最小限に限定しなければならない。

第5条（利用・加工の対象となる個人データの限定）

個人データ管理者は、利用・加工する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条（利用・加工時の照合及び確認手続）

1. 個人データの取扱者は、利用する個人データが対象データとして正しいかについて確認しなければならない。
2. 個人データの取扱者は、利用する個人データが正しく加工されたかについて元データと照合しなければならない。

第7条（利用・加工の規格外作業に関する申請及び承認手続）

個人データの取扱者は、本規程に定める以外の方法で個人データを利用・加工する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第8条（機器・記録媒体等の管理手続）

1. 個人データ管理者は、利用・加工する個人データが保存された機器・記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じ変更しなければならない。
2. 個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

第9条（個人データへのアクセス制御）

1. 個人データ管理者は、利用・加工する個人データへのアクセスを制御するために、利用・加工する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
 - ① 個人データの利用・加工に必要なID及びパスワードの管理を徹底する。
 - ② 個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。
2. 個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の利用・加工を認められた必要最小限の取扱者に限り利用・加工が行われるようID及びパスワードを付与すると共に、ID及びパスワードの管理を徹底しなければならない。

第10条（利用・加工状況の記録及び分析）

1. 個人データの取扱者は、個人データを利用・加工する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に利用・加工状況について記録を行わなければならない。
2. 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第11条（センシティブ情報の利用・加工の制限）

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、利用・加工してはならない。

- ① 保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を利用・加工する場合
- ② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を利用・加工する場合
- ③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属もしくは加盟に関する従業員等のセンシティブ情報を利用・加工する場合
- ④ 前各号のほか、金融分野ガイドライン第5条第1項各号に掲げる場合

第12条（センシティブ情報の利用に際して本人同意が必要である場合における本人同意の取得及び本人への説明事項）

1. 個人データの取扱者は、前条①に基づきセンシティブ情報を利用する場合には、当該センシティブ情報を保険業の適切な業務運営を確保する必要性から、本人の同意（原則として書面による。）に基づき業務遂行上必要な範囲で利用しなければならない。
2. 個人データの取扱者は、前項において本人の同意に基づかない場合には、当該センシティブ情報を利用してはならない。
3. 個人データの取扱者は、郵送等により取得した個人データが含まれる文書等にセンシティブ情報が含まれている場合は、原則として、本人の指定した方法により、当該情報を速やかに本人に返却もしくは廃棄する。
ただし、当該文書等に記載された他の情報が業務遂行上必要な場合、個人データの取扱者は、直ちに当該センシティブ情報の記載部分を判読不能な状態にして取得するものとする。

第13条（個人データの管理区域外への持ち出しに関する措置）

1. 個人データ管理責任者は、個人データの管理区域外への持ち出しに関する取扱者の役割・責任を定め、組織内に周知しなければならない。

2. 個人データ管理者は、個人データの管理区域外への持ち出しに関する取扱者を必要最小限に限定しなければならない。
3. 個人データ管理者は、管理区域外に持ち出すことが可能な個人データを業務上必要最小限の範囲に限定しなければならない。
4. 個人データ管理者は、個人データの管理区域外への持ち出しに際し、個人データを持ち出す者が第2項で限定された取扱者本人であることを確認しなければならない。
また、個人データ管理者は、持ち出す個人データが第3項により持ち出すことを限定した個人データの範囲内であるか確認しなければならない。
5. 個人データの取扱者は、個人データを管理区域外に持ち出す場合には、個人データ管理者に申請し、承認を得たうえで行わなければならない。
6. 個人データの取扱者は、個人データを管理区域外に持ち出す場合には、必要最小限の件数に限ると共に、個人データが保存された機器・媒体等を常時携帯するなど適切に管理しなければならない。
7. 個人データの取扱者は、個人データを管理区域外に持ち出す場合には、データの種類や形態等に応じて、必要かつ適切に持ち出した個人データの状況について報告及び記録を行わなければならない。
8. 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、報告及び記録された状況を確認する。

第14条（個人データの利用者の識別及び認証）

個人データ管理者は、個人データを利用・加工する取扱者の識別及び認証機能を設けなければならない。

第15条（個人データの管理区分の設定及びアクセス制御）

1. 個人データ管理者は、個人データの利用・加工段階における管理区分の設定及びアクセス制御機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の利用・加工の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第16条（個人データへのアクセス権限の管理）

1. 個人データ管理者は、個人データの利用・加工段階におけるアクセス権限に関する機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の利用・加工の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第17条（個人データの漏えい等防止策）

個人データ管理者は、個人データの利用・加工段階における漏えい等の防止策を講じなければならない。

第18条（個人データへのアクセス記録及び分析）

個人データ管理者は、個人データの利用・加工段階におけるアクセス記録を取得し、必要な期間保管すると共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

第19条（個人データを取り扱う情報システムの稼働状況の記録及び分析）

個人データ管理者は、個人データの利用・加工段階におけるシステムの稼働状況に関し記録を取得し、必要な期間保管すると共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

3. 保管・保存段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人データの「保管・保存」段階の取扱いについて定めたものである。

第2条（定義）

1. 「保管」とは、個人データを加工せず、オフィスフロア内に置き管理することなどをいう。
2. 「保存」とは、個人データを加工せず、オフィスフロア外（書庫等）に置き廃棄に至るまで管理すること、及びパソコンや電子媒体等に電子データを格納し消去に至るまで管理すること（個人データのバックアップを含む。）などをいう。

第3条（保管・保存に関する取扱者の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、個人データの保管・保存に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2. 個人データ管理者は、各部署において、業務上必要な者に限り個人データの保管・保存が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の保管・保存に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の保管・保存の取扱者を必要最小限に限定して定めなければならない。

第5条（保管・保存の対象となる個人データの限定）

個人データ管理者は、保管・保存する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条（保管・保存の規格外作業に関する申請及び承認手続き）

個人データの取扱者は、本規程に定める以外の方法で個人データを保管・保存する場合は、個人データ管理者に申請し、承認を得た上で行わなければならない。

第7条（機器・記録媒体等の管理手続）

1. 個人データ管理者は、「個人データ管理台帳」を踏まえ、個人データが保存された機器・記録媒体等の保管場所等の指定ならびに管理区分及び権限の設定をし、必要に応じ変更しなければならない。
2. 個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

第8条（個人データへのアクセス制御）

1. 個人データ管理責任者は、保管・保存する個人データへのアクセスを制御するために、保管・保存した個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
 - ① 個人データの保管・保存に必要なID及びパスワードの管理を徹底する。
 - ② 個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。
2. 個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の保管・保存を認められた必要最小限の取扱者に限り保管・保存が行われるようID及びパスワードを付与すると共に、ID及びパスワードの管理を徹底しなければならない。

第9条（保管・保存状況の記録及び分析）

1. 個人データの取扱者は、個人データを保管・保存する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に保管・保存状況について記録を行わなければならない。
2. 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第10条（個人データに関する障害発生時の対応・復旧手続き）

1. 個人データ管理者は、保管・保存した個人データについて、取扱者に対し定期的にバックアップ等を行うよう徹底すると共に、保管・保存した個人データに障害が発生した際にはバックアップデータ等により復旧させなければならない。
2. 個人データの取扱者は、作成したバックアップデータ等を適切に管理しなければならない。

第11条（個人データの利用者の識別及び認証）

個人データ管理者は、個人データを保管・保存する取扱者の識別及び認証機能を設けなければならない。

第12条（個人データの管理区分の設定及びアクセス制御）

1. 個人データ管理者は、個人データの保管・保存段階における管理区分の設定及びアクセス制御機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の保管・保存の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第13条（個人データへのアクセス権限の管理）

1. 個人データ管理者は、個人データの保管・保存段階におけるアクセス権限に関する機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の保管・保存の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第14条（個人データの漏えい等防止策）

個人データ管理者は、個人データの保管・保存段階における漏えい等の防止策を講じなければならない。

第15条（個人データへのアクセス記録及び分析）

個人データ管理者は、個人データの保管・保存段階におけるアクセス記録を取得し、必要な期間保管すると共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

第16条（個人データを取り扱う情報システムの稼働状況の記録及び分析）

個人データ管理者は、個人データの保管・保存段階におけるシステムの稼働状況に関し記録を取得し、必要な期間保管すると共に、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

4. 移送・送信段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人データの「移送・送信」段階の取扱いについて定めたものである。

第2条（定義）

1. 「移送」とは、物理的な手段により個人データを異なる場所や人に移すことなどをいう。
2. 「送信」とは、電子的な手段により個人データを異なる場所や人に移すことなどをいう。

第3条（移送・送信に関する取扱者の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、個人データの移送・送信に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2. 個人データ管理者は、各部署において業務上必要な者に限り個人データの移送・送信が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の移送・送信に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の移送・送信の取扱者を必要最小限に限定して定めなければならない。

第5条（移送・送信の対象となる個人データの限定）

個人データ管理者は、移送・送信する個人データを業務上必要な範囲内のものに限定しなければならない。

第6条（移送・送信時の照合及び確認手続）

個人データの取扱者は、個人データを移送・送信するときには、移送・送信先に相違がないか照合及び確認を行わなければならない。

第7条（移送・送信の規格外作業に関する申請及び承認手続）

個人データの取扱者は、本規程に定める以外の方法で個人データを移送・送信する場合は、個人データ管理者に申請し、承認を得た上で行わなければならない。

第8条（個人データへのアクセス制御）

1. 個人データ管理者は、移送・送信する個人データへのアクセスを制御するために、移送・送信する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。
 - ① 個人データの移送・送信に必要なIDおよびパスワードの管理を徹底する。
 - ② 個人データが保存された機器・記録媒体等を保管するスペースへの部外者の立ち入りを制限する。

2. 個人データ管理者は、センシティブ情報へのアクセス制御について、当該情報の移送・送信を認められた必要最小限の取扱者に限り移送・送信が行われるようID及びパスワードを付与すると共に、ID及びパスワードの管理を徹底しなければならない。

第9条（移送・送信状況の記録及び分析）

1. 個人データの取扱者は、個人データを移送・送信する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に移送・送信状況について記録を行わなければならない。
2. 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

第10条（センシティブ情報の移送・送信の制限）

個人データの取扱者は、センシティブ情報については、次に掲げる場合を除くほか、移送・送信してはならない。

- ① 保険業の適切な業務運営を確保する必要性から、本人の同意に基づき業務遂行上必要な範囲でセンシティブ情報を移送・送信する場合
- ② 相続手続を伴う保険金支払事務等の遂行に必要な限りにおいて、センシティブ情報を移送・送信する場合
- ③ 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体もしくは労働組合への所属もしくは加盟に関する従業員等のセンシティブ情報を移送・送信する場合
- ④ 前各号のほか、金融分野ガイドライン第5条第1項各号に掲げる場合

第11条（個人データに関する障害発生時の対応・復旧手続）

1. 個人データ管理者は、移送・送信する個人データについて、取扱者に対し定期的にバックアップ等を行うよう徹底すると共に、移送・送信した個人データに障害が発生した際にはバックアップデータ等により復旧させなければならない。
2. 個人データの取扱者は、作成したバックアップデータ等を適切に管理しなければならない。

第12条（個人データの利用者の識別及び認証）

個人データ管理者は、個人データを移送・送信する取扱者の識別及び認証機能を設けなければならない。

第13条（個人データの管理区分の設定及びアクセス制御）

1. 個人データ管理者は、個人データの移送・送信段階における管理区分の設定及びアクセス制御機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス制御機能の設定にあたっては、センシティブ情報の移送・送信の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第14条（個人データへのアクセス権限の管理）

1. 個人データ管理者は、個人データの移送・送信段階におけるアクセス権限に関する機能を設けなければならない。
2. 個人データ管理者は、前項のアクセス権限に関する機能の設定にあたっては、センシティブ情報の移送・送信の取扱者が必要最小限の者に限定されるよう設定しなければならない。

第15条（個人データの漏えい等防止策）

個人データ管理者は、個人データの移送・送信段階における漏えい等の防止策を講じなければならない。

第16条（個人データへのアクセス記録及び分析）

個人データ管理者は、個人データの移送・送信段階におけるアクセス記録を取得し、必要な期間保管するとともに、個人データの漏えい等の防止のため、必要に応じてこれを分析しなければならない。

5. 消去・廃棄段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人データの「消去・廃棄」段階の取扱いについて定めたものである。

第2条（定義）

1. 「消去」とは、個人データが保存されている媒体の個人データを電子的な方法その他の方法により削除することなどをいう。
2. 「廃棄」とは、個人データが保存されている媒体を物理的に廃棄することなどをいう。

第3条（消去・廃棄に関する取扱者の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、個人データの消去・廃棄に関する取扱者の役割・責任を定め、組織内に周知しなければならない。
2. 個人データ管理者は、業務上必要な者に限り個人データの消去・廃棄が行われるよう取扱者を限定しなければならない。

第4条（センシティブ情報の消去・廃棄に関する取扱者の限定）

個人データ管理者は、個人データのうち、センシティブ情報の消去・廃棄の取扱者を必要最小限に限定して定めなければならない。

第5条（消去・廃棄時の照会及び確認手続）

1. 個人データの取扱者は、個人データの消去・廃棄に際し、消去・廃棄する個人データについて、「個人データ管理台帳」等により保管期間を照会または消去・廃棄理由を確認のうえ、消去・廃棄しなければならない。
2. 個人データの取扱者は、個人データを消去・廃棄する際には、当該データが保存されている機器・記録媒体等の性質に応じ適正な方法で消去・廃棄しなければならない。

第6条（消去・廃棄の規格外作業に関する申請及び承認手続）

個人データの取扱者は、本規程に定める以外の方法で個人データを消去・廃棄する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第7条（機器・記録媒体等の管理手続）

1. 個人データ管理者は、消去・廃棄する個人データが保存された機器・記録媒体等の設置場所の指定ならびに管理区分及び権限の設定をし、必要に応じ変更しなければならない。
2. 個人データの取扱者は、前項の指定及び設定に従い、個人データが保存された機器・記録媒体等を適切に保管しなければならない。

第8条（個人データへのアクセス制御）

個人データ管理者は、消去・廃棄する個人データへのアクセスを制御するために、消去・廃棄する個人データが保存された機器・記録媒体等に関して以下の措置を講じなければならない。

- ① 個人データの入力に必要なIDおよびパスワードの管理を徹底する。
- ② 個人データが保存された機器・記録媒体等を保管するスペースへの部外者の対置入りを制限する。

第9条（消去・廃棄状況の記録及び分析）

1. 個人データの取扱者は、個人データを消去・廃棄する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に消去・廃棄状況について記録を行わなければならない。
2. 個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認する。

6. 漏えい等事案への対応の段階における取扱規程

第1条（目的）

本規程は、当代理店における個人データの安全管理措置のうち、個人データの漏えい等事案への対応の段階における取扱いについて定めたものである。

第2条（定義）

「漏えい等事案」とは、個人情報に記載・収録された帳票や電子記録媒体（USBメモリー・CD・DVD等）の盗難または紛失、郵便物の誤送付、電子メールやファックスの誤送信、システムの設定ミス等によるインターネット上で個人情報の第三者による閲覧、不正アクセス等での個人情報の窃取等の事故により、個人情報の漏えい、滅失またはき損が生じ、または生じるおそれがある場合をいう。

第3条（漏えい等事案への対応に関する対応部署の役割・責任及び取扱者の限定）

1. 個人データ管理責任者は、漏えい等事案への対応に関する部署（以下、「対応部署」という。）の役割・責任を定め、組織内に周知しなければならない。
2. 対応部署の個人データ管理者は、各部署において、業務上必要な者に限り漏えい等事案への対応が行われるよう取扱者を限定しなければならない。

第4条（漏えい等事案への対応の規格外作業に関する申請及び承認手続き）

個人データの取扱者は、本規程に定める以外の方法で漏えい等事案に対応する場合は、個人データ管理者に申請し、承認を得たうえで行わなければならない。

第5条（発見者の報告・被害拡大の防止）

漏えい等事案が発生した場合、発見者は、個人情報の回収を行うなど漏えい範囲の拡大防止等必要な措置をとると共に、直ちに対応部署に報告しなければならない。

第6条（漏えい等事案の影響等に関する調査手続）

漏えい等事案が発生した部署の個人データ管理者は、個人データ管理責任者及び対応部署と連携のうえ、漏えいした個人データの取扱状況の記録内容（システムのログ等を含む、以下同じ）の分析を行い、漏えいした個人データの量、質、事故の原因、態様、被害の程度等漏えい等事案の内容及び影響の調査を行うとともに、漏えい等事案による被害が発覚時よりも拡大しないよう必要な措置を講ずることとする。

第7条（再発防止策・事後対策の検討に関する手続）

漏えい等事案が発生した部署の個人データ管理者は、対応部署と協議のうえ、漏えいした個人データの取扱状況の記録内容の調査を踏まえた真因の分析、再発防止策・事後対策の策定を実施し、個人データ管理責任者へ報告することとする。

第8条（保険会社への報告・本人への通知に関する手続）

1. 対応部署は、報告を受けた漏えい等事案について、保険会社の定める手続きに従い直ちに保険会社に報告しなければならない。
2. 対応部署の個人データ管理者は保険会社の指示に従い、社外への報告等（警察への届出、二次被害の防止・類似事案の発生回避の観点からの漏えい等事案の事実関係及び再発防止策の公表等）の要否及びその方法について決定しなければならない。
3. 対応部署の個人データ管理者は保険会社の指示に従い、原則漏えい等事案の発生について本人に通知しなければならない。

第9条（漏えい等事案への対応記録及び分析）

1. 対応部署の個人データの取扱者は、漏えい等事案へ対応する場合、データの種類や形態等に応じて、必要に応じ、かつ適切に漏えい事案への対応状況について記録を行わなければならない。
2. 対応部署の個人データ管理者は、個人データの漏えい等の防止のため、必要に応じ、記録された状況を確認することとする。

以上

個人データの取扱状況の点検及び監査に係る規程

保険代理店業務に係わる個人情報取扱規程第8条第1項に定める個人データの取扱状況の点検及び監査に係わる規程を以下のとおり定める。

第1条（目的）

本規程は、当代理店における個人データの取扱状況に関する点検及び監査について定めたものである。

第2条（実施部署）

1. 個人データ管理責任者は、個人データを取り扱う部署において個人データの点検に関する点検責任者および点検担当者を選任し、当該部署が自ら点検を実施するよう指示しなければならない。

2. 点検責任者と点検担当者は兼務することができる。
3. 個人データ管理責任者は、監査を実施する部署を指定し、その部署から個人データの監査に関する監査責任者及び監査担当者を選任し、監査を実施するよう指示しなければならない。
ただし、監査を実施する部署が個人データを取り扱うときには、個人データ管理責任者は、当該部署以外の部署から当該部署を監査する監査責任者及び監査担当者を選任しなければならない。

第3条（点検）

1. 個人データ管理責任者は、個人データの取扱状況の点検に関する計画を立案し、点検責任者に対し、定期的及び臨時の点検を実施するよう指示しなければならない。
2. 点検担当者は、点検責任者の指示に基づいて確実に点検を実施しなければならない。
3. 点検担当者は、点検により個人データの取扱いに関する規程に違反する事項などを発見した場合には、点検責任者に報告しなければならない。
4. 点検責任者は、規程に違反する事項について、個人データ管理責任者に報告すると共に個人データ管理責任者の指示を踏まえ、改善のための措置を講じなければならない。

第4条（監査）

1. 個人データ管理責任者は、個人データの取扱状況の監査に関する計画を立案し、監査責任者に対し、定期的及び臨時の監査を実施するよう指示しなければならない。
2. 監査担当者は、監査責任者の指示に基づいて確実に監査を実施しなければならない。
3. 監査担当者は、監査により個人データの取扱いに関する規程に違反する事項などを発見した場合には、監査責任者に報告しなければならない。
4. 監査責任者は、規程に違反する事項について、個人データ管理責任者に報告すると共に個人データ管理責任者の指示に従い、改善のための措置を講じなければならない。

以 上

個人データの外部委託に係る規程

保険代理店業務に係わる個人情報取扱規程第24条第1項に定める個人データの外部委託に係る規程を以下のとおり定める。

第1条（目的）

本規程は、当代理店による個人データの取扱いの委託について、個人データを適正に取扱っていると認められる者を選定すること、及び委託先における個人データに対する安全管理措置が図られることを確保するため定めたものである。

第2条（定義）

1. 「委託」とは、契約の形態や種類を問わず、当代理店が他の者に個人データの取扱いの全部または一部を行わせることを内容とする契約の一切を含む。
2. 「委託先」とは、当代理店が、個人データの取扱いの全部または一部を第三者に委託する場合の当該第三者のことをいう。

第3条（外部委託にあたっての所属保険会社への申請及び承認）

個人データ管理責任者は、個人データの外部委託にあたって、所属保険会社に書面により申請し、承認を得なければならない。ただし、所属保険会社が別に定める場合はこの限りではない。

第4条（委託先選定の基準）

1. 個人データ管理者は、委託先を選定するにあたって、「委託先選定チェックリスト」を別に定め、これに基づき委託先を選定するとともに、「委託先選定チェックリスト」を定期的に見直さなければならない。
2. 個人データ管理者は、「委託先選定チェックリスト」の策定及び見直しにあたっては個人データ管理責任者の承認を得なければならない。
3. 個人データ管理責任者は、承認した「委託先選定チェックリスト」を組織内に周知しなければならない。

第5条（委託先における選定基準の遵守状況の確認）

個人データ管理者は、委託契約後に「委託先選定チェックリスト」に定められた事項の委託先における遵守状況を定期的または随時に確認すると共に、委託先が当該基準を満たしていない場合には、委託先に対して改善を求めなければならない。

第6条（委託契約）

1. 個人データ管理責任者は、選定した委託先との間で、以下の安全管理に関する事項を盛り込んだ委託契約の締結等を行しなければならない。
 - ① 当社の委託先に対する監督及び監査報告徴収に関する権限
 - ② 委託先における個人データの漏えい、盗用、改竄及び目的外利用の禁止
 - ③ 再委託における条件
 - ④ 漏えい等が発生した際の委託先の責任
2. 個人データ管理責任者は、定期的に委託契約等に盛り込む安全管理に関する事項を見直さなければならない。

第7条（委託先における委託契約上の安全管理措置の遵守状況の確認）

個人データ管理者は、定期的または随時に委託先における委託契約上の安全管理の遵守状況を確認するとともに、委託先が遵守していない場合には、委託先に対して改善を求めなければならない。

第8条（海外にある委託先に個人データの取扱いを委託する場合の追加措置）

個人データ管理者は、個人データの取扱いを海外にある外部に委託するにあたって、以下の安全管理措置を講じるとともに、個人情報保護法で求められる、委託先における個人データの安全管理措置に相当する措置（以下、「相当措置」という）を義務付けた委託契約を委託先との間で締結しなければならない。

（1）次の項目について年に1回、定期的に書面等により確認を行う。

①移転先の第三者による相当措置の実施状況

②移転先の第三者の所在する外国における相当措置の実施に影響を及ぼすおそれのある制度の有無

（2）相当措置の実施に支障が生じた際には、是正を求め、当該相当措置の継続的な実施の確保が困難となったときは、当該個人データの提供を停止する。

（3）委託契約では、委託契約の範囲内で個人データを取り扱う旨、必要かつ適切な安全管理措置を講じる旨、従業員に対する必要かつ適切な監督を行う旨、再委託が必要な場合の事前承諾、個人データの第三者提供の禁止等を定める。

以 上