

損害保険会社に係る個人情報保護指針

(改定版)

2019年7月10日

一般社団法人 外国損害保険協会

目次

	頁
損害保険会社に係る個人情報保護指針	
第1条(目的等)	3
第2条(個人情報保護宣言の策定・公表)	4
第3条(個人情報の利用目的)	5
第4条(個人番号及び特定個人情報の利用)	7
第5条(個人情報の取得等)	7
第6条(個人番号の提供の求めの制限)	7
第7条(個人データの第三者提供)	8
第8条(外国にある第三者への個人データの提供)	9
第9条(第三者提供時の確認・記録義務)	10
第10条(匿名加工情報の取扱い)	12
第11条(特定個人情報の提供制限)	12
第12条(特定個人情報の収集・保管制限)	12
第13条(センシティブ情報の特例)	13
第14条(個人データの安全管理措置)	15
第15条(特定個人情報に関する安全管理措置)	17
第16条(損害保険代理店に対する指導・監督)	17
第17条(本人からの請求等に応じる手続)	18
第18条(苦情処理)	19
第19条(本協会の役割)	19

損害保険会社に係る個人情報保護指針

（目的等）

- 第1条 この指針は、「個人情報の保護に関する法律」（以下「保護法」という。）及び「行政手続における特定の個人を識別するための番号の利用等に関する法律」（以下、「番号法」という。）の規定の趣旨に沿って、損害保険会社はその事業の遂行に際して個人情報を取り扱う際に開示すべき利用目的、講ずべき安全管理のための措置その他の事項につき、具体的な基準を定めることにより、損害保険会社の個人情報、個人番号及び特定個人情報の適正な取扱いを確保することを目的とする。
- 2 この指針は、一般社団法人外国損害保険協会（以下「本協会」という。）に加盟する損害保険会社及び保護法第51条第1項の同意を行う損害保険会社（以下「損害保険会社」という。）がその事業の遂行に際して個人情報、個人番号及び特定個人情報を取り扱う場合（雇用管理などの内部事務に伴い個人情報を取り扱う場合を除く。）につき適用する。
- 3 この指針において使用する用語は、別に定義する場合を除き、保護法において使用する用語の例による。なお、この指針における「個人情報」及び「個人データ」とは、個人番号及び特定個人情報を除くものをいう。

＜参考事項＞

1. 指針の策定

この指針は、本協会が、保護法第47条第1項に規定する「認定個人情報保護団体」であることを踏まえ、保護法第53条第1項に規定する「個人情報保護指針」として策定するものである。

2. 指針が適用される対象事業者（損害保険会社等）

この指針が適用される対象事業者は、本協会加盟の損害保険会社とする。なお、非加盟の損害保険会社等は、本協会が認定個人情報保護団体として行う業務の対象となることに同意するときは、対象事業者となることができる（保護法第51条第1項）。

3. 指針が適用される事業の範囲（その事業の遂行に際して）

損害保険会社は、損害保険業のほかに付随業務（保険業法第98条）や法定他業（同法第99条）を営んでいる。この指針は、特に定めがない限り、損害保険会社が営む全ての業務（雇用管理などの内部事務を除く。）に適用される。なお、雇用管理などの内部事務については、各社が「個人情報の保護に関する法律についてのガイドライン（通則編）」（以下、「通則ガイドライン」という。）等を踏まえて個別に対応するものとする。

＜参考条文＞

保護法第47条（認定）、第51条（対象事業者）、第53条（個人情報保護指針）

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、「金融分野ガイドライン」という。）第1条（目的等）

通則ガイドライン2（定義）

番号法第2条（定義）

（個人情報保護宣言の策定・公表）

- 第2条 損害保険会社等は、保護法その他の関連法令等及びこの指針を踏まえ、自社の個人情報（個人番号及び特定個人情報を含む。）の保護に関する考え方や方針に関する宣言（個人情報保護宣言）を策定し、公表するものとする。
- 2 損害保険会社等は、その公表する個人情報保護宣言を実効性あるものとするべく、社内体制の整備等に努めるものとする。

＜参考事項＞

1. 個人情報保護宣言

政府の「個人情報の保護に関する基本方針」（2004年4月2日閣議決定。2008年4月25日一部変更。2009年9月1日一部変更。2016年2月19日一部変更。2016年10月28日一部変更。以下「政府方針」という。）が「個人情報取扱事業者は、（中略）例えば、消費者の権利利益を一層保護する観点から、個人情報保護を推進する上での考え方や方針（いわゆる、プライバシーポリシー、プライバシーステートメント等）を対外的に明確化するなど、個人情報の保護及び適正かつ効果的な活用について主体的に取り組むことが期待されているところであり、体制の整備等に積極的に取り組んでいくことが求められている」としていることを踏まえ、この指針が適用されるすべての損害保険会社等が個人情報保護宣言を策定するとともに、ホームページへの掲載などの適切な方法により公表することとする。

2. 個人情報保護宣言の記載事項

損害保険会社等が策定すべき個人情報保護宣言には、次のような項目を規定するものとする。

(1) 自社の個人情報保護に関する考え方

例：個人情報保護の重要性に鑑み、損害保険業に対する社会の信頼をより向上させるため、個人情報の保護に関する法律その他の関連法令等を遵守し、個人情報の適正な取扱いを確保する。

(2) 自社の個人情報保護に関する取組方針

- ① 利用目的、同意を得て行う第三者提供及び共同利用の概要
- ② 個人データに係る安全管理措置の概要
- ③ 保有個人データに関する事項
- ④ 開示等の求めに応じる手続
- ⑤ 問い合わせ及び苦情の受付窓口
- ⑥ 取組方針及び取組内容の継続的改善の宣言
- ⑦ 特定個人情報の取扱いに関する事項

3. 社内体制の整備等

金融分野ガイドラインおよび金融庁監督指針等における社内体制等にかかる規定を考慮し、すべての損害保険会社等は、社内体制の整備等に努めることとする。

損害保険会社等が個人情報保護の確保・推進のために講ずべき措置として、例えば次のようなものがある。

(1) 社内責任体制の整備

例：全社的な取組方針・推進体制を企画・立案・実施・検証する部署又は組織の設置

例：個人情報保護管理者の設置

(2) 社内規程等の整備

例：個人情報の取扱要領等を定める社内規程・マニュアル類の整備

(3) 安全管理措置の整備（この指針第14条参照）

＜参考条文＞

金融分野ガイドライン第18条（個人情報保護宣言の策定）

(個人情報の利用目的)

- 第3条 損害保険会社等は、利用目的を定めるときは、自らが個人情報を利用する範囲を本人が合理的に予想できる程度に特定するものとする。
- 2 損害保険会社等は、利用目的を公表するとともに、損害保険業の遂行に際して取得する個人情報の利用目的を明示するときは、保険契約申込書その他の書面に記載するものとする。
- 3 損害保険会社等は、個人情報の利用目的を変更するときは、保護法 第15条第2項に掲げる要件を満たすとともに、変更後の利用目的を公表するものとする。
- 4 損害保険会社等は、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わないものとする。やむを得ずかかる取扱いを行うときは、保護法 第16条第3項各号に掲げる場合を除き、あらかじめ本人の同意（原則として書面による。）を得るものとする。

<参考事項>

本条は個人番号及び特定個人情報を除く個人情報の取扱いを定める規定である。個人番号及び特定個人情報の利用については次条に定める。

1. 利用目的の特定

損害保険業の遂行に際して取得する個人情報の利用目的は、各社が次のような要素を勘案して特定するものとする。

(1) 保険契約申込時に取得する個人情報の利用目的

- ① 申込に係る保険契約の引受の審査
- ② 保険契約の履行及び付帯サービスの提供
- ③ 自社が取り扱う当該契約以外の商品・サービス等の案内・提供（グループ会社・提携会社等が提供するものを含む）（注）
例：当社が取り扱う損害保険、生命保険、投資信託、確定拠出年金
例：グループ（提携）会社である〇〇会社が取り扱う△△商品（サービス）

(2) 保険金請求時に取得する個人情報の利用目的

- ① 請求に係る保険事故の調査（関係先への照会等を含む）
- ② 請求に係る保険金の支払

（注）提供する商品・サービスは、提供される商品・サービスを本人が合理的に予想できるよう特定するものとし、説明書面では概要とし、詳細はホームページに掲載することも認められる。

2. 利用目的の公表・書面記載

損害保険会社等は、その事業の遂行に係る全ての利用目的をホームページへの掲載等の適切な継続性のある方法により公表する。利用目的を変更する場合における変更後の利用目的についても同様とする。また、そのうち損害保険業の遂行に際して取得する個人情報の利用目的を明示する場合は、更に保険契約申込書その他の書面に記載する（インターネットによる申込等の場合は、ウェブ上での利用目的の掲載を含む）。

保険募集に際して、事前にアンケート等により見込客情報を取得する場合がある。この場合も、保険募集の一環として行われる限り、例えば「アンケートにより取得した個人情報を利用して保険商品を案内する」といった利用目的をアンケートに記載するものとする。

なお、新規業務の開始、既存業務の見直し等に伴い、新たな利用目的が加わり、又は、従来の利用目的を変更する必要があることがあるので、利用目的のフォローを行う社内責任体制を整備する必要がある。

ただし、上記利用目的の公表および書面記載に関しては、次に該当する場合は除くものとする。

- ① 利用目的を本人に通知し、又は公表することにより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
（例）
 - ・ 暴力団等の反社会的勢力情報、疑わしい取引の届出の対象情報、振り込み詐欺に利用された口座に関する情報、業務妨害行為を行う悪質者情報の提供者が逆恨みを買うおそれがある場合
- ② 利用目的を本人に通知し、又は公表することにより損害保険会社等の権利又は正当な利益を害するおそれがある場合
（例）
 - ・ 開発中の新サービス、営業ノウハウが明らかになることにより、企業の健全な競争を害する場合
 - ・ 振り込み詐欺に利用された口座に関する情報を取得したことが明らかになることにより、情報提供を受けた企業に害が及ぶ場合
- ③ 国の機関又は地方公共団体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、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とき。
（例）
 - ・ 犯罪捜査への協力のため、被疑者等に関する情報を取得した場合
- ④ 取得の状況からみて利用目的が明らかであると認められる場合
（例）
 - ・ 電話等での資料請求に対して、請求者が提供した住所及び氏名に関する情報を請求された資料の送付のみに利用する場合
 - ・ 今後連絡を取り合うために名刺交換をした場合

- ・着信において相手方の電話番号が非通知でない場合で、同じ用件で当方から相手方に電話を掛け直す場合

3. 目的外利用の禁止

損害保険会社等は、目的外利用を行わないものとする（保護法 第16条第1項）。この適用除外となる同条第3項に掲げる場合（本人の事前同意なく利用目的の達成に必要な範囲を超えて取り扱う場合）とは、例えば次のような場合である。

(1) 法令に基づく場合（保護法第16条第3項第1号）

例：所得税法第225条第1項等の規定に基づく税務署長への支払調書等提出

例：国税通則法第74条の2等に基づいて税務当局が行う質問検査及び国税犯則取締法第1条等に基づいて収税官吏、徴税吏員の行う犯則事件の任意調査

例：犯罪による収益の移転防止に関する法律第8条第1項に基づく疑わしい取引の届出

例：弁護士法第23条の2に基づく弁護士による報告請求

例：刑事訴訟法第197条第2項に基づく警察からの捜査関係事項照会

例：刑事訴訟法第218条に基づく令状による差押え・搜索・検証

例：地方税法第72条の63に基づく事業税に係る質問検査

例：会社法第381条第3項による親会社の監査役の子会社に対する調査への対応

例：会社法第396条及び金融商品取引法第193条の2の規定に基づく財務諸表監査への対応

例：金融商品取引法第210条、第211条等に基づく証券取引等監視委員会の職員による犯則事件の調査

なお、法令に、第三者が個人情報の提供を求めることができる旨の規定はあるが、正当な事由に基づきそれに応じないことができる場合には、損害保険会社等は、当該法令の趣旨に照らして目的外利用の必要性と合理性が認められる範囲内で対応するよう留意する。

(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。（保護法第16条第3項第2号）

例：暴力団等の反社会的勢力情報、業務妨害行為を行う悪質者情報等を企業間で共有する場合

(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。（保護法第16条第3項第3号）

例：病気の予防、治療に関する研究等を目的とする情報交換を行う場合

(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。（保護法第16条第3項第4号）

例：税務当局の任意調査に応じる場合

例：警察の任意調査に応じる場合

例：一般統計調査に回答する場合

なお、損害保険会社等は、任意の求めの趣旨に照らして目的外利用の必要性と合理性が認められる範囲内で対応するよう留意する。

※EU域内から十分に認定に基づき提供を受けた個人データの利用の範囲については、本指針第9条の参考事項5を参照。

4. 本人同意の取得

本人同意の取得は、原則として「書面」によるが、「書面」には電磁的記録を含むという趣旨（以下同様）である。

5. 事業承継時の取扱い

損害保険会社等が合併その他の事由により他の損害保険会社等から事業を承継し、それに伴い個人情報を取得した場合、承継会社は、被承継会社が設定した利用目的の達成に必要な範囲内で当該個人情報を取り扱う必要がある（保護法第16条第2項）。

<参考条文>

保護法第15条（利用目的の特定）、第16条（利用目的による制限）、第18条（取得に際しての利用目的の通知等）

金融分野ガイドライン第2条（利用目的の特定）、第3条（同意の形式）、第4条（利用目的による制限）、第6条（取得に際しての利用目的の通知等）

通則ガイドライン2-12（「本人の同意」）、3-1（個人情報の利用目的）、3-2-3（利用目的の通知又は公表）、3-2-4（直接書面等による取得）、3-2-5（利用目的の通知等をしなくてもよい場合）

(個人番号及び特定個人情報の利用)

第4条 損害保険会社等は、個人番号及び特定個人情報の利用目的を公表するとともに、個人番号関係事務の実施に際して取得する個人番号及び特定個人情報の利用目的を明示するときは、個人番号及び特定個人情報を入手する際などの書面に記載するものとする。

2 損害保険会社等は、番号法第9条に定める目的を超えて個人番号及び特定個人情報を利用してはならない。

<参考条文>

保護法第18条(取得に際しての利用目的の通知等)

番号法第9条(利用範囲)、第29条(特定個人情報ファイルの作成の制限)

(個人情報の取得等)

第5条 損害保険会社等は、業務上必要な範囲内で、かつ、適法で公正な手段により個人情報を取得するものとする。

2 損害保険会社等は、個人情報を本人以外の者から取得するときは、本人の利益を不当に侵害しないようにするものとする。

3 損害保険会社等は、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とともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めるものとする。

<参考事項>

1. 個人情報取得の原則

損害保険会社等は、個人情報を取得するときは、①取得する個人情報を「業務上必要な範囲内」に留めるとともに、②取得手段を適法かつ公正なものとする必要がある。保護法は、取得手段につき「不正なもの」を排除する(保護法第17条)だけだが、この指針では保護法制定以前からの取扱いを踏襲し、2つの要件を課すこととする。

なお、例えば、本人確認のために運転免許証や住民票の提出を受けた場合、本人特定事項(氏名・住所・生年月日)以外の情報まで取得することになるが、本人が任意で提出する限り、かかる取得まで禁止する趣旨ではない(但し、個人番号を除く。また、センシティブ情報の取得、利用又は第三者提供については第13条を、安全管理措置については金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針(以下、「金融分野実務指針」という。)を参照)。

2. 第三者からの取得

個人情報取扱事業者(転得者)が第三者(原取得者)から個人情報を取得する場合、転得者が原取得者による不正取得に加担してはならず、また、不正取得された個人情報であることを認識した上で当該情報を取得してはならない。

損害保険会社等は、上記のほか、更に「本人の利益を不当に侵害しない」ものとする。具体的には、本人の利益を侵害する可能性のある個人情報を取得するときは、取得情報を業務上必要な範囲に留めることにおいて、他の情報以上に慎重な取扱いを行う必要がある。「本人の利益を不当に侵害しない」場合として、例えば、満期返戻金を支払うために居所不明の契約者の住民票を第三者から取り付ける場合が該当する。

第三者から個人データを取得する際の確認・記録義務については、この指針第9条参照。

3. 取得情報の保守

損害保険会社等は、可能な限り、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない(保護法第19条)。

<参考条文>

保護法第17条(適正な取得)、第19条(データ内容の正確性の確保等)

金融分野ガイドライン第7条(データ内容の正確性の確保等)

通則ガイドライン3-2-1(適正取得)、3-3-1(データ内容の正確性の確保等)

(個人番号の提供の求めの制限)

第6条 損害保険会社等は、番号法第19条各号のいずれかに該当して特定個人情報の提供を受けることができる場合を除き、個人番号の提供を求めてはならない。

<参考条文>

番号法第14条(提供の要求)、第15条(提供の求めの制限)、第19条(特定個人情報の提供の制限)

(個人データの第三者提供)

第7条 損害保険会社等は、個人データを第三者に提供するときは、保護法第23条第1項各号及び第2項に掲げる場合を除き、次に掲げる事項を示した上で、本人の同意（原則として書面による。）を得るものとする。

- (1) 個人データを提供する第三者
 - (2) 提供を受けた第三者における利用目的
 - (3) 第三者に提供される情報の内容
- 2 損害保険会社等は、個人データ（この指針第12条に定めるセンシティブ情報を除く。以下この項において同じ。）の第三者提供にあたって、保護法第23条第2項各号に掲げる事項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くとともに、個人情報保護委員会に届け出たときは、本人の同意を得ることなく、当該個人データを第三者に提供することができる。
- 3 損害保険会社等は、前項に基づき、必要な事項を個人情報保護委員会に届け出たときは、その内容を自らもインターネットの利用その他の適切な方法により公表するものとする。
- 4 損害保険会社等は、保険契約の締結又は保険金の請求に際して行われる不正行為の排除等の目的のために損害保険会社等の間において契約等情報の登録又は交換を行うときは、保護法第23条第5項第3号に規定する事項を公表するものとし、かつ、本人の同意（原則として書面による。）を得よう努めるものとする。
- 5 損害保険会社等は、グループ会社又は特定の会社との間で個人データを共同して利用するときは、保護法第23条第5項第3号に規定する事項を公表するものとする。

<参考事項>

本条は個人番号及び特定個人情報を除く個人データの第三者提供にかかる規定である。個人番号及び特定個人情報の提供制限にかかる規定は第11条に定める。

1. 第三者提供の原則

保護法は、個人情報取扱事業者が個人データを第三者に提供するときは、本人の事前同意を取り付ける（保護法第23条第1項本文）ことを義務づけているが、この指針では、金融分野ガイドライン第11条第1項を踏まえ、①個人データを提供する第三者、②提供を受けた第三者における利用目的、③第三者に提供される情報の内容、を示した上で同意を取り付けることとしている。

損害保険業における第三者提供としては、次のような事例が考えられ、いずれも本人の同意を得るものとする。

- (1) 医療機関等の関係先に業務上必要な照会を行う際に、当該関係先に対して本人特定に必要な個人データ（例：氏名）を提供する場合
- (2) 再保険契約の締結や再保険金の受領等のために、出再先等に必要個人データを提供する場合
「再保険」に関しては、再保険会社は本人から直接同意を取得できない立場にあるため、元受保険会社が再保険に関して、情報がどのように利用されるか本人が理解できるように記載を行い、包括的な同意を得るものとする。
なお、同意取付義務が免除される保護法第23条第1項各号に掲げる場合とは、この指針第3条に係る参考事項に記載するものと同じである。

2. オプトアウト

保護法第23条第2項から第4項までは、いわゆるオプトアウトにより個人データの第三者提供を行う場合について規定している。保護法第23条第2項各号に掲げる事項とは、次のとおり。

- (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) 第三者への提供の方法
- (4) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
- (5) 本人の求めを受け付ける方法

損害保険会社等は、上記(2)、(3)又は(5)の事項を変更する場合は、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くとともに、個人情報保護委員会に届け出なければならない（保護法第23条第3項）。

個人情報保護委員会は、保護法第23条第2項及び第3項に基づく届出があったときは、当該届出に係る事項を公表することとされている（保護法第23条第4項）。

なお、保護法第23条第2項は、要配慮個人情報についてオプトアウトによる第三者提供を禁じているが、損害保険会社等は、要配慮個人情報に該当しないセンシティブ情報についてもオプトアウトによる第三者提供を行わないものとする。

3. 情報交換制度

損害保険業界では、保険契約の締結又は保険金の請求に際して行われる不正行為の排除等の目的のために、引き受けた保険契約に関する情報や受け付けた保険事故に関する情報等を登録し、又は交換する制度を運営している。登録制度は、所定の保険契約に関する事項を日本損害保険協会に登録し、参加会社・団体の照会を受けて日本損害保険協会が重複契約等の有無及び内容を回答するものである。交換制度は、保険契約者の申告内容の正否を確認すること等を目的として、損害保険会社等間で保険契約又は保険事故に関する情報を交換するものである。これら制度については、保護法第23条第5項第3号に規定する事項を公表する（必須）とともに、原則として、あらかじめ登録又は交換の目的を示した上で、本人の同意（原則として書面による）を得ることとする。

情報交換制度について、保護法第23条第5項第3号による特定共同利用要件によれば本人の同意取得は不要であるが、損害保険業界としては同意を得よう努める（努力義務）こととする。

4. グループ内共同利用

保護法上、共同利用を行う場合の要件として、あらかじめ「本人に通知」するか「本人が容易に知り得る状態に置く」ことが挙げられている（保護法第 23 条第 5 項第 3 号）。グループ内共同利用を「本人が容易に知り得る状態に置く」ためには、ホームページへの掲載等、継続性のある方法により公表することとする。

<参考条文>

保護法第 23 条（第三者提供の制限）

金融分野ガイドライン第 11 条（第三者提供の制限）

通則ガイドライン 3-4（個人データの第三者への提供）

（外国にある第三者への個人データの提供）

第 8 条 損害保険会社等は、個人データを外国にある第三者に提供するにあたっては、保護法第 24 条に従い、次の各号のいずれかに該当する場合を除き、あらかじめ、外国にある第三者への個人データの提供を認める旨の本人の同意を得なければならない。

- (1) 当該第三者が、我が国と同等の水準にあると認められる個人情報保護制度を有している国として保護法施行規則で定める国にある場合
- (2) 当該第三者が、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制として保護法施行規則で定める基準に適合する体制を整備している場合
- (3) 保護法第 23 条第 1 項各号に該当する場合

<参考事項>

本条は、外国にある第三者への個人データの提供にかかる規定である。

1. 保護法第 24 条が適用されない場合

第 8 条第 1 項各号に該当する場合、保護法第 24 条は適用されないため、「外国にある第三者への個人データの提供を認める旨の本人の同意」を得る必要はない（ただし、第 1 号および第 2 号に該当する場合は、日本国内の第三者に個人データを提供する場合と同様、保護法第 23 条が適用されることに留意）。

例えば、海外の遠隔地で海外旅行保険の契約者に保険事故が発生し緊急の対応を要する際に、損害保険会社が委託をしている現地のクレームエージェントに情報提供を行う場合等は、保護法第 23 条第 1 項第 2 号（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。）に該当するため、保護法第 24 条は適用されないと考えられる。

2. 我が国と同等の水準にあると認められる個人情報保護制度を有している外国

保護法施行規則第 11 条の指定基準に基づき、個人情報保護委員会告示において「我が国と同等の水準にあると認められる個人情報保護制度を有している外国」を指定している。

3. 個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制の基準

保護法施行規則第 11 条の 2 は、個人情報取扱事業者が講ずべき措置に相当する措置を継続的に講ずるために必要な体制の基準として、次のいずれかに該当することを規定している。

- (1) 個人情報取扱事業者と個人データの提供を受ける者との間で、当該提供を受ける者における当該個人データの取扱いについて、適切かつ合理的な方法により、保護法第 4 章第 1 節の規定の趣旨に沿った措置の実施が確保されていること。
- (2) 個人データの提供を受ける者が、個人情報の取扱いに係る国際的な枠組みに基づく認定を受けていること。

(1) の「適切かつ合理的な方法」および「保護法第 4 章第 1 節の規定の趣旨に沿った措置」の具体的な内容については、個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）を参照。(2) の「個人情報の取扱いに係る国際的な枠組みに基づく認定」については、APEC の CBPR システムの認証が該当する。

<参考条文>

保護法第 24 条（外国にある第三者への提供の制限）

保護法施行規則第 11 条（個人の権利利益を保護する上で我が国と同等の水準にあると認められる個人情報の保護に関する制度を有する外国）

保護法施行規則第 11 条の 2（個人情報取扱事業者が講ずべきこととされている措置に相当する措置を継続的に講ずるために必要な体制の基準）

個人情報の保護に関する法律についてのガイドライン（外国にある第三者への提供編）

個人情報の保護に関する法律に係る EU 域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(4)

(第三者提供時の確認・記録義務)

- 第9条 損害保険会社等は、個人データを第三者(保護法第2条第5項各号に掲げる者を除く。以下この条において同じ。)に提供したときは、保護法施行規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名又は名称その他の保護法施行規則で定める事項に関する記録を作成しなければならない。ただし、当該個人データの提供が保護法第23条第1項各号又は第5項各号のいずれか(外国にある第三者への個人データの提供にあっては、第23条第1項各号のいずれか)に該当する場合は、この限りでない。
- 2 損害保険会社等は、第三者から個人データの提供を受けるに際しては、保護法施行規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が保護法第23条第1項各号又は第5項各号のいずれかに該当する場合は、この限りでない。
- (1) 当該第三者の氏名または名称および住所ならびに法人にあっては、その代表者(法人でない団体が代表者または管理人の定めのあるもの)にあっては、その代表者または管理人)の氏名
- (2) 当該第三者による当該個人データの取得の経緯
- 3 損害保険会社等は、前項の規定による確認を行ったときは、保護法施行規則で定めるところにより、当該個人データの提供を受けた年月日、当該確認に係る事項その他の保護法施行規則で定める事項に関する記録を作成しなければならない。
- 4 損害保険会社等は、第1項および前項に基づき作成した記録について、保護法施行規則で定める期間保存しなければならない。

<参考事項>

本条は、第三者に個人データを提供する場合および第三者から個人データの提供を受ける場合の確認・記録義務について規定している。

1. 確認・記録義務の適用対象

個人情報の保護に関する法律についてのガイドライン(第三者提供時の確認・記録義務編)では、明文により確認・記録義務が適用されない第三者提供と、解釈により確認・記録義務が適用されない第三者提供について、それぞれ示されている。

明文により確認・記録義務が適用されない第三者提供は、保護法第23条第1項各号に該当する場合(詳細はこの指針第3条に係る参考事項参照)と保護法第23条第5項各号に該当する場合(委託、事業承継又は共同利用に伴って提供する方法)である。

解釈により確認・記録義務が適用されない第三者提供は、次のとおり整理されている。

(1) 提供者および受領者に確認・記録義務が適用されない場合

- ・「本人による提供」または「本人に代わって提供」に該当する場合

例) 損害保険会社が事故車の修理手配をする際に、本人が選択した提携修理工場に当該本人に係る情報を提供する場合

例) 取引先・保険契約者から、専門業者・弁護士等の紹介を求められ、専門業者・弁護士等のリストから紹介を行う場合

- ・「本人と一体と評価できる関係にある者に提供」または「提供者が、最終的に本人に提供することを意図した上で、受領者を介在して提供(本人がそれを明確に認識できる必要あり)」

例) 損害保険会社代理店の募集人が、家族と共に来店した顧客に対して、加入している自動車保険の補償内容等を説明する場合

- ・「ホームページ等で公表されている情報や報道機関により報道されている情報を提供」に該当する場合

(2) 受領者に確認・記録義務が適用されない場合

- ・提供者にとっては「個人データ」に該当するが、受領者にとっては「個人データ」に該当しない場合

例) 個人情報取扱事業者の営業担当者が、取引先を紹介する目的で、データベースとして管理しているファイルから名刺1枚を取り出してそのコピーを他の個人情報取扱事業者の営業担当者に渡す場合

- ・受領者にとって「個人情報」に該当しない場合

例) 提供者が氏名を削除するなどして個人を特定できないようにしたデータの提供を受けた場合

- ・「提供を受ける」行為があるとはいえない場合

例) 単に閲覧する行為、口頭、FAX、メール、電話等で、受領者の意思とは関係なく、一方的に個人データを提供された場合

2. 確認義務

損害保険会社等は、第三者から個人データの提供を受ける際は、「第三者の氏名および住所並びに法人にあっては、その代表者の氏名」および「第三者による個人データの取得の経緯」を確認しなければならない。前者については、第三者から口頭等により申告を受ける方法その他の適切な方法、後者については、個人データの取得先や取得行為の態様等を示す契約書その他の書面の提示を受ける方法その他の適切な方法によるものとする。

3. 記録義務

損害保険会社等は、第三者に個人データを提供する場合および第三者から個人データの提供を受ける際は、下表に掲げる事項の記録を、文書、電磁的記録またはマイクロフィルムを用いて作成しなければならない。

<個人データの提供者の記録事項>

	提供年月日	第三者の氏名等	本人の氏名等	個人データの項目	本人の同意
オプトアウトによる第三者提供	○	○	○	○	
本人の同意による第三者提供		○	○	○	○

<個人データの受領者の記録事項>

	提供を受けた年月日	第三者の氏名等	取得の経緯	本人の氏名等	個人データの項目	個人情報保護委員会による公表	本人の同意
オプトアウトによる第三者提供	○	○	○	○	○	○	
本人の同意による第三者提供		○	○	○	○		○
個人情報取扱事業者 に該当しない者からの 第三者提供		○	○	○	○		

記録は、原則として、個人データの授受の都度、速やかに作成しなければならない。ただし、個人データの授受の態様に応じて、一括して記録を作成する方法、契約書等の代替手段による方法を用いることもできる（オプトアウトによる第三者提供の場合は不可）。また、提供者（または受領者）は受領者（または提供者）の記録義務の全部または一部を代替して行うことができる。

4. 保存期間

損害保険会社等は、作成した記録を下表の期間保存しなければならない（保存期間は、記録の作成方法によって異なる。）。

<記録の保存期間>

記録の作成方法の別	保存期間
「契約書等の代替手段による方法」により記録を作成した場合	最後に当該記録に係る個人データの提供を行った日から起算して1年を経過する日までの間
「一括して記録を作成する方法」により記録を作成した場合	最後に当該記録に係る個人データの提供を行った日から起算して3年を経過する日までの間
上述以外の場合	3年

5. EU域内から十分性認定に基づき個人データの提供を受ける場合

保護法第26条第1項及び第3項の規定に基づき、EU域内から当該個人データの提供を受ける際に特定された利用目的を含め、その取得の経緯を確認し、記録することとする。

同様に、損害保険会社等が、EU域内から十分性認定に基づき個人データの提供を受けた他の個人情報取扱事業者から、当該個人データの提供を受ける場合、保護法第26条第1項及び第3項の規定に基づき、当該個人データの提供を受ける際に特定された利用目的を含め、その取得の経緯を確認し、記録することとする。

上記のいずれの場合においても、損害保険会社等は、保護法第26条第1項及び第3項の規定に基づき確認し、記録した当該個人データを当初又はその後提供を受ける際に特定された利用目的の範囲内で利用目的を特定し、その範囲内で当該個人データを利用することとする（保護法第15条第1項、法第16条第1項）。

<参考条文>

保護法第25条（第三者提供に係る記録の作成等）、第26条（第三者提供を受ける際の確認等）

保護法施行規則第12条（第三者提供に係る記録の作成）、第13条（第三者提供に係る記録事項）、第15条（第三者提供を受ける際の確認）、第17条（第三者提供を受ける際の記録事項）

個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）

個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(3)

(匿名加工情報の取扱い)

- 第10条 損害保険会社等は、匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、特定の個人を識別できないように、かつ、その作成に用いる個人情報を復元できないようにするために、保護法施行規則第19条各号で定める基準に従い、当該個人情報を加工しなければならない。
- 2 損害保険会社等は、匿名加工情報を作成したときは、その作成に用いた個人情報から削除した記述等及び個人識別符号並びに加工の方法に関する情報（以下「加工方法等情報」という。）の漏えいを防止するために、保護法施行規則第20条で定める基準に従い、必要な措置を講じなければならない。
- 3 損害保険会社等は、匿名加工情報の安全管理措置、苦情処理等の匿名加工情報の適正な取扱いを確保するために必要な措置を自ら講じ、かつ、当該措置の内容を公表するよう努めなければならない。
- 4 損害保険会社等は、匿名加工情報を作成したときは、当該匿名加工情報の作成後遅滞なく、インターネット等を利用し、当該匿名加工情報に含まれる個人に関する情報の項目を公表しなければならない。
- 5 損害保険会社等は、匿名加工情報を第三者に提供するときは、提供に当たりあらかじめ、インターネット等を利用し、第三者に提供される匿名加工情報に含まれる個人に関する情報の項目及びその提供方法について公表するとともに、当該第三者に対して、当該提供に係る情報が匿名加工情報である旨を電子メール又は書面等により明示しなければならない。
- 6 損害保険会社等は、匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成の元となった個人情報の本人を識別する目的で、当該匿名加工情報の加工方法等情報を取得し、又は当該匿名加工情報を他の情報と照合してはならない。

<参考事項>

1. 損害保険会社等が匿名加工情報を取り扱う際に従うべき事項

本条は、匿名加工情報取扱事業者等の義務に関する規定である。

損害保険会社等は、匿名加工情報を取り扱うときは、保護法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（匿名加工情報編）に従い、適切な安全管理措置等を講じなければならない。

2. EU域内から十分性認定に基づき提供を受けた個人情報について匿名加工情報を作成する場合

EU域内から十分性認定に基づき提供を受けた個人情報については、損害保険会社等が、加工方法等情報を削除することにより、匿名化された個人を再識別することを何人にとっても不可能とした場合に限り、匿名加工情報とみなすこととされている。

<参考条文>

保護法第36条（匿名加工情報の作成等）、第37条（匿名加工情報の提供）、第38条（識別行為の禁止）、第39条（安全管理措置等）
保護法施行規則第19条（匿名加工情報の作成の方法に関する基準）、第20条（加工方法等情報に係る安全管理措置の基準）
個人情報の保護に関する法律についてのガイドライン（匿名加工情報編）
個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール(5)

(特定個人情報の提供制限)

第11条 損害保険会社等は、番号法第19条各号のいずれかに該当する場合を除き、特定個人情報の提供をしてはならない。

<参考条文>

番号法第19条（特定個人情報の提供の制限）

(特定個人情報の収集・保管制限)

第12条 損害保険会社等は、番号法第19条各号のいずれかに該当する場合を除き、特定個人情報を収集又は保管してはならない。

<参考条文>

番号法第20条（収集等の制限）

(センシティブ情報の特例)

第 13 条 損害保険会社等は、要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これらのうち要配慮個人情報に該当するものを除く。）に関する個人情報（本人、国の機関、地方公共団体、保護法第 76 条第 1 項各号若しくは施行規則第 6 条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。以下「センシティブ情報」という。）を、次に掲げる場合を除くほか、取得、利用又は第三者提供をしないこととする。

- (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し、利用し、又は第三者提供する場合
- (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し、利用し、又は第三者提供する場合
- (3) 保険料収納事務等の遂行上必要な範囲において、政治・宗教等の団体若しくは労働組合への所属若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し、利用し、又は第三者提供する場合
- (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

2 損害保険会社等は、前項第 1 号に該当する場合において、本人以外の者からセンシティブ情報を取得するにあたっては、当該本人以外の者が保護法第 23 条に定める要件を満たしていることを確認するか、本人から同意を得るものとする。

<参考事項>

1. センシティブ情報の範囲

本人の権利利益を保護すべき度合いの高いセンシティブ情報の範囲は、金融分野ガイドラインと同様、「要配慮個人情報並びに労働組合への加盟、門地、本籍地、保健医療及び性生活（これらのうち要配慮個人情報に該当するものを除く。）に関する個人情報（本人、国の機関、地方公共団体、保護法第 76 条第 1 項各号若しくは施行規則第 6 条各号に掲げる者により公開されているもの、又は、本人を目視し、若しくは撮影することにより取得するその外形上明らかなものを除く。）」とする。

センシティブ情報は、他の情報以上に慎重な取扱いが要請される一方で、損害保険実務においては、勤務先情報や所属団体情報として労働組合・政治団体・宗教団体等の名称を、保険引受の可否を判断するために保健医療情報を、それぞれ保険契約申込書等に記入していただくなど、業務利用の必要性がある。

2. センシティブ情報の取得

損害保険会社等は、金融分野ガイドライン第 5 条第 1 項各号に掲げる場合を除き、センシティブ情報の取得、利用又は第三者提供を行わないものとする。例えば、本人確認のために運転免許証や住民票の提出を受けた場合、本人特定事項以外にセンシティブ情報（例えば本籍地）があるときは、当該情報を塗りつぶして保管する等、取得に際して適切な対応を行うものとする。保険業の適切な業務運営を確保する必要があるときには、本人の同意があることを前提に、かつ、業務上必要な範囲でセンシティブ情報を取得、利用、又は第三者提供することが金融分野ガイドラインで認められている。

損害保険会社等は、この指針第 13 条第 1 項第 1 号に該当する場合において、センシティブ情報を第三者から取得するときは、①原取得者が本人から第三者提供について同意を得ていることを確認するか、②（原取得者とは別に）本人の同意を得る、のいずれかを行うこととする。なお、原取得者が金融分野における個人情報取扱事業者である場合には、要配慮個人情報に該当しないセンシティブ情報であっても、オプトアウトによる第三者提供が認められないことに留意する必要がある。

この指針第 13 条第 1 項第 2 号には、例えば次のような場合がある。

例：死亡保険金受取人の確認のため、戸籍謄本に記載の本籍地情報を取得、利用又は第三者提供する場合

この指針第 13 条第 1 項第 3 号には、例えば次のような場合がある。

例：契約者情報や勤務先情報として、政治・宗教等の団体名を取得、利用又は第三者提供する場合

この指針第 13 条第 1 項第 4 号には、例えば次のような場合がある。

例：いわゆる総会屋および暴力団の違法行為に関する情報の収集および交換を行う場合

3. 金融分野ガイドライン上のセンシティブ情報と保護法上の要配慮個人情報との関係

センシティブ情報に要配慮個人情報が含まれていることにより、同じセンシティブ情報であっても、それが要配慮個人情報以外であるか、それとも要配慮個人情報であるかによって取り扱いが異なる場合等がある。

具体的には、この指針第 13 条第 1 項第 2 号および第 3 号の場合、対象となる情報が要配慮個人情報以外であれば取得に際して本人同意が不要なところ、要配慮個人情報であれば取得に際して原則同意が必要となる。

また、この指針第 13 条第 1 項第 1 号および金融分野ガイドライン第 5 条第 1 項第 8 号（センシティブ情報に該当する生体認証情報を本人の同意に基づき、本人確認に用いる場合）の場合、保護法上は利用に際して本人同意を要しない要配慮個人情報を取り扱う場合も、その他のセンシティブ情報と同様に同意が必要となる。

4. EU域内から十分に認定に基づき提供を受けた個人データ

EU域内から十分に認定に基づき提供を受けた個人データに、GDPR において特別な種類の個人データと定義されている性生活、性的指向又は労働組合に関する情報が含まれる場合には、損害保険会社等は、当該情報についても要配慮個人情報・センシティブ情報と同様に取り扱うこととする。

<参考条文>

金融分野ガイドライン第5条（機微（センシティブ）情報）

個人情報保護に関する法律に係るEU域内から充分性認定により移転を受けた個人データの取扱いに関する補完的ルール（1）

(個人データの安全管理措置)

第 14 条 損害保険会社等は、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、個人データの取得・利用・保管等の各段階に応じた「組織的安全管理措置」、「人的安全管理措置」及び「技術的安全管理措置」を含む、必要かつ適切な措置を講じなければならない。

当該措置は、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、個人データの取扱状況及び個人データを記録した媒体の性質等に起因するリスクに応じたものとする。

- 2 本条における「組織的安全管理措置」とは、個人データの安全管理措置について従業者の責任と権限を明確に定め、安全管理に係る基本方針・取扱規程等を整備・運用し、その実施状況の点検・監査を行うこと等の、個人情報取扱事業者の実施体制整備及び実施措置をいう。
- 3 本条における「人的安全管理措置」とは、従業者との個人データの非開示契約等の締結及び従業者に対する教育・訓練等を実施し、個人データの安全管理が図られるよう従業者を監督することをいう。
- 4 本条における「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、情報システムの監視等、個人データの安全管理に関する技術的な措置をいう。
- 5 損害保険会社等は、個人データの安全管理に係る基本方針・取扱規程等の整備として、以下の「組織的安全管理措置」を講じなければならない。

(組織的安全管理措置)

(1) 規程等の整備

- ①個人データの安全管理に係る基本方針の整備
- ②個人データの安全管理に係る取扱規程の整備
- ③個人データの取扱状況の点検・監査に係る規程の整備
- ④外部委託に係る規程の整備

(2) 各管理段階における安全管理に係る取扱規程

- ①取得・入力段階における取扱規程
- ②利用・加工段階における取扱規程
- ③保管・保存段階における取扱規程
- ④移送・通信段階における取扱規程
- ⑤消去・廃棄段階における取扱規程
- ⑥漏えい事案等への対応の段階における取扱規程

- 6 損害保険会社等は、個人データの安全管理に係る実施体制の整備として、以下の「組織的安全管理措置」、「人的安全管理措置」、及び「技術的安全管理措置」を講じなければならない。

(組織的安全管理措置)

- ①個人データの管理責任者等の設置
- ②就業規則等における安全管理措置の整備
- ③個人データの安全管理に係る取扱規程に従った運用
- ④個人データの取扱状況を確認できる手段の整備
- ⑤個人データの取扱状況の点検・監査体制の整備と実施
- ⑥漏えい事案等に対応する体制の整備

(人的安全管理措置)

- ①従業者との個人データの非開示契約等の締結
- ②従業者の役割・責任の明確化
- ③従業者への安全管理措置の周知徹底、教育及び訓練
- ④従業者による個人データの管理手続きの遵守状況の確認

(技術的安全管理措置)

- ①個人データの利用者の識別及び認証
- ②個人データの管理区分の設定及びアクセス制御
- ③個人データへのアクセス権限の管理
- ④個人データの漏えい・き損等防止策
- ⑤個人データへのアクセスの記録及び分析
- ⑥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
- ⑦個人データを取り扱う情報システムの監視及び監査

- 7 損害保険会社等は、個人データの取扱いの全部又は一部を委託するときは、委託先の選定の基準を定め、あらかじめ委託先の情報管理体制を確認し、委託後の業務遂行状況を監視し、事故発生時の責任関係を明確にするなど、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。当該監督は、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、委託する事業の規模及び性質並びに個人データの取扱状況等に起因するリスクに応じたものとする。なお、二段階以上の委託が行われた場合には、委託先の事業者が再委託先等の事業者に対して十分な監督を行っているかについても監督を行わなければならない。

- 8 損害保険会社等は、その事業の遂行に際して取り扱う個人情報の漏えい事案等または匿名加工情報の作成に用いた個人情報から削除した記述等および個人識別符号ならびに保護法第 36 条第 1 項の規程により行った加工の方法に関する情報の漏えい事案の事故が生じたときは、本人への通知及び当局への報告を行うとともに、二次被害の防止、類似事案の発生回避等の必要性がある場合には、事実関係等を公表しなければならない。

＜参考事項＞

本条は個人番号及び特定個人情報を除く個人データの安全管理措置にかかる規定である。個人番号及び特定個人情報の安全管理措置にかかる規定は次条に定める。

1. 損害保険会社等が講ずべき安全管理措置

損害保険会社等が、その取り扱う個人データに係る安全管理措置として講ずべき具体的内容については、金融分野実務指針を踏まえ、別途定める損保安全管理実務指針によるものとする。

2. 委託先（損保代理店以外）の監督

金融分野ガイドライン、金融分野実務指針および金融庁監督指針等を踏まえ、すべての損害保険会社等は、委託先等における顧客等に関する情報管理について適切な取扱いを確保するものとする。

(1) 委託先の選定の基準

保険会社の経営の合理性の観点からみて十分なレベルのサービスの提供を行い得るか、契約に沿ったサービス提供や損害等負担が確保できる財務・経営内容か、保険会社のレピュテーション等の観点から問題ないか等の観点から、委託先の選定を行っているか。

(2) 委託先の情報管理体制の確認

委託先における目的外使用の禁止も含めて顧客情報管理が整備されており、委託先に守秘義務が課されているか。

(3) 委託業務の遂行状況の監視

契約内容は、委託業務の内容等に応じ、例えば、保険会社が委託業務及びそれに関する委託先の経営状況に関して委託先より受ける報告の内容について明確に示されるなど十分な内容となっているか。

委託業務に関する責任者の設置、モニタリング、検証態勢（委託契約において保険会社が委託先に対して事務処理の適切性に係る検証を行うことができる旨の規定を盛り込む等の対応を含む）等の社内管理態勢が整備されているか。

保険会社において、委託業務についても監査の対象となっているか。

(4) 事故発生時の責任体制の明確化

契約内容は、委託業務の内容等に応じ、例えば、委託契約に沿ってサービスが提供されない場合における委託先の責務及び委託に関連して発生するおそれのある損害の負担の関係（必要に応じて担保提供等の損害負担の履行確保等の対応を含む）について明確に示されるなど十分な内容となっているか。

委託業務の履行状況等に関し委託先から保険会社への定期的レポートに加え、必要に応じ適切な情報が迅速に得られる態勢となっているか。

3. 漏えい事案等の事故への対応

損害保険会社等は、個人情報の漏えい事案等または匿名加工情報の作成に用いた個人情報から削除した記述等および個人識別符号ならびに保護法第36条第1項の規程により行った加工の方法に関する情報の漏えい事案の事故が発生した場合に備えて、この指針第14条第1項に掲げる社内責任体制を整備するほか、実際に事故が生じたときは、本人への連絡及び関係当局への報告を行うとともに、二次被害の防止、類似事案の発生回避等の観点から、事実関係等を公表するものとする。ただし、公表することにより模倣行為を誘発したり、プライバシーを侵害する等の懸念があり、公表が適当でないと判断される場合は、この限りではない。

＜参考条文＞

保護法第20条（安全管理措置）、第21条（従業者の監督）、第22条（委託先の監督）

金融分野ガイドライン第7条（データ内容の正確性の確保等）、第8条（安全管理措置）、第9条（従業者の監督）、

第10条（委託先の監督）、第17条（個人情報等の漏えい事案等への対応）

通則ガイドライン3-3-1（データ内容の正確性の確保等）

金融分野実務指針2-6-1

(特定個人情報に関する安全管理措置)

- 第 15 条 損害保険会社等は、個人番号及び特定個人情報の漏えい、滅失又はき損の防止等、個人番号及び特定個人情報の管理のために、必要かつ適切な安全管理措置を講じなければならない。
- 2 従業者に個人番号及び特定個人情報を取り扱わせるに当たっては、個人番号及び特定個人情報の安全管理措置が適切に講じられるよう、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らない。
 - 3 損害保険会社等は、金融分野ガイドライン及び金融分野実務指針のほか、番号法第 12 条及び特定個人情報の適正な取扱いに関するガイドライン（事業者編）に定める特定個人情報に関する安全管理措置（事業者編）に基づき、必要かつ適切な安全管理措置を講じなければならない。
 - 4 損害保険会社等は、個人番号関係事務の全部または一部を委託するときは、番号法に基づき損害保険会社等自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。二段階以降の委託を行う場合の再委託先等に対する点検においても番号法第 10 条を踏まえた監督を行うものとする。

<参考条文>

番号法第 10 条（再委託）、第 11 条（委託先の監督）、第 12 条（個人番号利用事務実施者等の責務）

保護法第 20 条（安全管理措置）、第 21 条（従業者の監督）

特定個人情報の適正な取扱いに関するガイドライン（事業者編）第 4-2-（2） 安全管理措置 ※

※ 安全管理措置の具体的な内容については、「（別添）特定個人情報に関する安全管理措置（事業者編）」を参照のこと。

(損害保険代理店に対する指導・監督)

- 第 16 条 損害保険会社は、その損害保険業に係る個人情報を損害保険代理店が取得し、又は利用する際にこの指針に準じた取扱いがなされるよう、当該代理店に対して安全管理の確保を含む必要かつ適切な監督を行うものとする。
- 2 損害保険会社は、損害保険代理店が個人情報の利用目的を通知、公表又は明示するときは、損害保険会社の利用目的との誤認が生じないように、当該代理店に対して必要かつ適切な監督を行わなければならない。

<参考事項>

1. 損保代理店の取得・利用・安全管理措置

損害保険契約に係る個人情報の取得（保険契約の締結等）又は利用（所属保険会社が取り扱う当該契約以外の商品及びサービスの案内及び提供等）は、殆どの場合、損保代理店を介して行われるため、損保代理店の管理下にある個人情報に係る安全管理措置を含め、この指針第 3 条、第 5 条及び第 14 条の規定は、損保代理店が損害保険契約に係る個人情報を取り扱う場合について準用される必要がある。なお、この指針第 3 条、第 5 条及び第 14 条を満たしたうえで、それを超える安全管理措置については、当該代理店の営業規模やシステム化の状況、取り扱う個人情報の量等を勘案して、損害保険会社が講ずべきものと異なる部分が生じ得る。

2. 損保代理店の利用目的

複数の損害保険会社に所属する乗合代理店は、1 の損害保険会社が引き受けた損害保険契約に係る個人情報を、他の損害保険会社を取り扱う損害保険契約等をお勧めするために利用することがあり、また、損害保険代理業以外の業務を営む兼業代理店は、損害保険契約に係る個人情報を、その営む他の業務に係る商品及びサービスをお勧めするために利用することがある。乗合代理店又は兼業代理店は、個人情報取扱事業者に該当する場合であって、上述のような利用実態があるときは、自らの利用目的を通知し、公表し、又は明示する必要がある。この場合においては、損害保険会社は、損害保険会社の利用目的と損保代理店の利用目的との間で誤認が生じないように、必要かつ適切な監督を行う必要がある。

<参考条文>

金融分野ガイドライン第 1 条（目的等）

(本人からの請求等に応じる手続)

第 17 条 損害保険会社等は、保護法第 27 条第 1 項各号に掲げる事項を公表するものとする。

2 損害保険会社等は、保険契約者等から自らの保険契約の内容又は保険事故の処理状況等に係る照会を受けたときは、保護法第 28 条第 2 項に定める手続によることを要しない。ただし、当該保険契約者等が同条第 1 項の規定によることを明示するときは、この限りでない。

3 損害保険会社等は、本人から保護法第 27 条第 2 項、第 28 条第 1 項、第 29 条第 1 項又は第 30 条第 1 項若しくは第 3 項の規定による請求等を受けたときは、各条項に定める適用除外要件に該当する場合を除き、各条項に沿った適切な対応を行うものとする。

4 損害保険会社等は、保護法第 31 条の通知をするときは、本人に対して、判断の根拠及び根拠となる事実を示すなど、その理由の説明を付すものとする。

<参考事項>

1. 保有個人データに関する事項の公表

保護法は、個人情報取扱事業者が保有個人データに関する事項を「本人の知り得る状態に置く」ことを義務づけている（保護法第 27 条第 1 項）。損害保険会社等は、当該事項の周知方法として、ホームページでの掲載など適切な継続性のある方法による公表とする。

保護法第 2 条第 7 項に基づく施行令第 4 条各号に掲げる場合及び施行令第 5 条に定める期間以内に消去することとなるもの（「保有個人データ」に該当しない場合）とは、例えば次のような場合である。

①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

例：癌などの罹患の事実など、本人に重大な精神的苦痛を与え、心身状況に悪影響を与える恐れがあるもの

②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

③国の安全が害されるおそれがあるもの

④犯罪の予防、鎮圧又は捜査等に支障がおよぶおそれがあるもの

例：警察からの照会記録

例：犯罪収益移転防止法第 8 条第 3 項（顧客等への届出事実の漏えい）に該当する場合

⑤6か月以内に消去することとなるもの

※E.U域内から十分に認定に基づき提供を受けた個人データについては、消去することとしている期間にかかわらず、保有個人データとして取り扱う。

2. 契約内容・事故処理状況に係る照会の特例

保険契約者等の関係者から契約内容や事故処理状況の照会を受けたときは、保護法上の開示請求手続とは別に、従来どおり対応することとする。ただし、当該関係者から保護法上の開示請求手続による旨の意思表示があったときは、その意思に沿った対応を行う。

3. 保護法上の開示等請求

保護法上の開示等請求を受けたときは、法定要件に沿った適切な対応を行う。

本人から求められた措置の全部若しくは一部をとらない旨を通知する場合又は本人から求められた措置と異なる措置をとる場合は、本人に対し、判断の根拠及び根拠となる事実を示すなど、その理由の説明を付して通知する。

4. 開示等拒否理由

保護法第 28 条第 2 項各号に掲げる場合（保有個人データの全部又は一部を開示しないことができる場合）とは、例えば次のような場合である。

(1) 本人の権利利益を侵害するおそれがある場合（第 1 号）

例：病名等を開示することにより本人の心身状況を悪化させるおそれがある場合

例：契約者等との守秘義務違反とされる場合（守秘義務違反とされるかは個別当事者毎にみる）

(2) 個人情報取扱事業者の業務に支障を及ぼすおそれがある場合（第 2 号）

例：保険引受判断に係る情報を開示することにより保険引受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

例：データの検索に著しく困難を要する場合

例：成約見込など、顧客に関する営業上の評価情報であって、本人に開示した場合、顧客との信頼関係に著しい支障を及ぼすおそれがある場合

例：債務者区分等、債務者に対する評価情報であって、本人に開示した場合、債務者との信頼関係に著しい支障を及ぼすおそれがある場合

例：与信審査内容等の個人情報取扱事業者が付加した情報の開示請求を受けた場合

例：保有個人データを開示することにより評価・試験等の適正な実施が妨げられる場合

例：企業秘密が明らかになるおそれがある場合

なお、開示すべき保有個人データの量が多いことのみでは該当しない。

5. 開示等請求手続

損害保険会社等各社が、保護法の規定に沿って、その実情に応じた開示等請求手続（手数料を含む）を設定する。

<参考条文>

保護法第2条（定義）、第27条（保有個人データに関する事項の公表等）、第28条（開示）、第29条（訂正等）、第30条（利用停止等）、第31条（理由の説明）、第32条（開示等の請求等に応じる手続）、第33条（手数料）

施行令第4条（保有個人データから除外されるもの）、第5条（保有個人データから除外されるものの消去までの期間）、第8条（保有個人データの適正な取扱いの確保に関し必要な事項）、第9条（個人情報取扱事業者が保有個人データを開示する方法）

金融分野ガイドライン第12条（保有個人データに関する事項の公表等）、第13条（開示）、第14条（理由の説明）、第15条（開示等の請求等に応じる手続）

個人情報の保護に関する法律に係るEU域内から十分性認定により移転を受けた個人データの取扱いに関する補完的ルール（2）

通則ガイドライン3-5-1（保有個人データに関する事項の公表等）、3-5-2（保有個人データの開示）、3-5-3（保有個人データの訂正等）、3-5-4（保有個人データの利用停止等）、3-5-6（開示等の請求等に応じる手続）

（苦情処理）

第18条 損害保険会社等は、個人情報、個人番号及び特定個人情報の取扱いに関する苦情を適切かつ迅速に処理するものとする。

2 損害保険会社等は、前項の目的を達成するため、前条第1項の規定により苦情の申出先を公表するほか、苦情処理手順を策定するなど必要な社内体制を整備するものとする。

<参考事項>

苦情処理

損害保険会社等は、保護法第35条に定める努力義務ではなく、この指針に基づく義務として苦情処理の適切かつ迅速な遂行を行うものとする。

<参考条文>

保護法第35条（個人情報取扱事業者による苦情の処理）

金融分野ガイドライン第16条（個人情報取扱事業者による苦情の処理）

通則ガイドライン3-6（個人情報の取扱いに関する苦情処理）

（本協会の役割）

第19条 本協会は、保護法第47条第1項の認定を受けて、同項各号の業務を行うものとする。

2 本協会は、損害保険会社等がこの指針を遵守していないと認めるときは、当該損害保険会社等に対して必要な指導、勧告その他の措置を行わなければならない。

3 本協会は、社会情勢や国民意識の変化、損害保険業を巡る環境の変化等に応じて、この指針を見直すものとする。

<参考事項>

1. 本協会の役割

本協会は、認定個人情報保護団体として、苦情処理、情報提供その他の法定業務を行う。

2. 本協会の権限

本協会は、この指針の遵守を確保するため、損害保険会社等がこの指針を遵守していないと認めるときは、必要な指導又は勧告を行わなければならない。

3. 指針の見直し

本協会は、個人情報保護に係る社会環境の変化に応じ、また、損害保険会社等における漏えい事案等の事故につき情報収集、原因分析等を行い、必要に応じて指針を見直すこととする。

<参考条文>

保護法第47条（認定）、第51条（対象事業者）、第52条（苦情の処理）、第53条（個人情報保護指針）、第54条（目的外利用の禁止）

以上