

金融機関等における個人データ保護のための取扱指針

第1章 総則

第1条 目的

第2条 定義

第3条 顧客への周知

第4条 取扱指針の拡張

第2章 収集、利用及び提供

第5条 個人データの収集

第6条 個人データの利用及び提供

第3章 適正管理

第7条 個人データの適正管理

第8条 個人データの安全保護措置

第9条 外部委託

第4章 開示請求等への対応

第10条 開示請求等への対応

第5章 管理体制の整備

第11条 管理体制の整備

< 説明の補足 >

第1章 総則

(目的)

第1条 この取扱指針は、金融機関等が個人データを取り扱う際の基本的事項を定めることを目的とする。

[説明]

この取扱指針は、個人データの保護の観点から、各金融機関等が個人データを取り扱う際の方向性を示したものである。

(定義)

第2条 この取扱指針において、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。

- 一 金融機関等 金融機関(銀行、長期信用銀行、全国信用金庫連合会、信用金庫、商工組合中央金庫、全国信用協同組合連合会、信用組合、労働金庫連合会、労働金庫、農林中央金庫、信用農業協同組合連合会)、保険会社、証券会社及び日本クレジットカード協会加盟クレジットカード会社をいう。

二 顧客 金融機関等の商品及びサービスに関する契約を締結し、又は締結することを申し込む個人をいう。

三 個人データ 顧客に関するデータ(事業を営む顧客の当該事業に関するデータを除く。)であって、特定の顧客を識別できるデータ(他のデータと照合することにより、特定の顧客を識別できることとなるものを含む。)のうち、容易に検索できるように記録され、又は記録されることが予定されているものをいう。

(説明)

この条は、この取扱指針において、必要な用語の定義を行ったものである。

第1号

「金融機関等」の範囲については、次の根拠法令による。

(1) 銀行、長期信用銀行

銀行法(昭和56年法律第59号)第2条第1項に規定する銀行または長期信用銀行法(昭和29年法律第187号)第2条に規定する長期信用銀行

(2) 全国信用金庫連合会、信用金庫

信用金庫法(昭和26年法律第238号)

(3) 商工組合中央金庫

商工組合中央金庫法(昭和11年法律第14号)

(4) 全国信用協同組合連合会、信用組合

中小企業等協同組合法(昭和24年法律第181号)

(5) 労働金庫連合会、労働金庫

労働金庫法(昭和28年法律第227号)

(6) 農林中央金庫

農林中央金庫法(大正12年法律第42号)

(7) 信用農業協同組合連合会

農業協同組合法(昭和22年法律第185号)

(8) 保険会社

保険業法(平成7年法律第105号)

(9) 証券会社

証券取引法(昭和23年法律第25号)第2条第9項に規定する証券会社

第2号

この取扱指針は、金融機関等が個人データを取り扱う際の基本的事項を定めたものであり、顧客以外の個人、例えば、金融機関等の従業員に関する情報を直接の対象とはしていない。

第3号

この号は、OECDガイドライン第1(b)並びにEU指令第2条(a)、(b)、(c)及び第3条1に対応するものである。

- (1) 「顧客に関するデータ」には、法人に関して記録された情報に含まれる当該法人の役員に関する情報、及び事業目的であることが明らかな取引に関する情報は含まれない。
- (2) 「特定の顧客を識別できるデータ」には、例えば、次のような情報が含まれる。
- 氏名が含まれる情報
氏名は含まれていないものの当該情報に含まれる個人別に付された番号、記号、画像、音声その他の情報により当該顧客を識別できる情報
当該情報のみでは識別できないが、当該情報に含まれる番号、記号その他の情報と金融機関等が保有する他の情報又は公開された情報をコンピュータ等による処理で組み合わせることによって当該顧客を識別できる情報
- (3) 「容易に検索できるように記録され、又は記録されることが予定されているもの」には、例えば、次のような情報が含まれる。
- 手書きの申込書や入力原票等の書類に記載されている情報のうち、容易に検索できるようにするためにコンピュータ等による処理が行われ、又は行われることが予定されている情報
顧客別又は取引別に作成された手書き文書によって構成されたファイルで、かつ、五十音順や特定の番号順等の基準で整理され容易に検索できるファイル(印鑑簿等)に記録され、又は記録されることが予定されている情報
- (4) 次の情報は、この取扱指針の「個人データ」には含まれない。
- 営業日誌若しくはスケジュール表等単に期日順に作成された手書き文書、又は一時的に記録した電子情報のうち、容易に検索できるように記録されることが予定されていない情報
 - 評価等に関する情報

(顧客への周知)

第3条 金融機関等は、個人データの取扱いについて顧客へ周知するものとする。

(説明)

この条は、OECDガイドライン第12「公開の原則」に対応するものである。

金融機関等は、個人データの保護についての考え方、利用及び提供の状況、並びに開示請求及び訂正請求の方法について、顧客に知るための機会を与えるものとする。(後掲<説明の補足>1.参照)

(取扱指針の拡張)

第4条 金融機関等は、個人データの保護に関するルールの策定その他有効な措置をとるに当たっては、業務の実態に応じて取扱指針の項目を追加し、又は修正することができる。

(説明)

この条は、OECDガイドライン第6に対応するものである。

各金融機関等においてこの取扱指針にもとづきルールの設定その他有効な措置をとる場合には、業務の実態に応じた項目を追加し、修正することができる。この場合、この指針が定める水準を低下させないように留意しつつ、関係者にわかりやすい記述とすることが望ましい。

第2章 収集、利用及び提供

(個人データの収集)

第5条 金融機関等は、業務上必要な範囲内で個人データを収集するものとする。

- 2 金融機関等は、個人データの収集に際して、個人データの利用又は提供の目的を明確にし、顧客の同意を得るものとする。
- 3 金融機関等は、政治的見解、信教(宗教、思想及び信条をいう。)、労働組合への加盟、人種及び民族、門地及び本籍地、保健医療及び性生活、並びに犯罪歴に関する個人データについては、収集し、利用し又は提供してはならない。ただし、顧客の同意を得た場合、及び法令の規定による場合はこの限りでない。
- 4 金融機関等は、適法かつ公正な手段によって個人データを収集するものとする。
- 5 金融機関等は、個人データを第三者から収集するに当たっては、顧客の利益を不当に侵害しないようにするものとする。

(説明)

この条は、OECDガイドライン第7「収集制限の原則」及び第9「目的明確化の原則」並びにEU指令第6条1(a)、(b)、(c)、第7条、第8条、第10条及び第11条に対応するものである。

第1項

金融機関等の場合には、銀行法、証券取引法、保険業法等それぞれの業務を規制する法令等で、業務の内容が明確化され、その範囲が厳しく制限されている。したがって、金融機関等としては、「業務上」とすることで収集する個人データは限定されると考えられる。

「業務上必要な範囲内」とは、例えば、次のような場合をいう。

- (1) 顧客の申込み又は契約締結に当たり、商品又はサービスが個々の顧客に適合しているかを判定する場合
- (2) 既に締結している契約を適切かつ安全に履行する場合
- (3) 顧客のニーズを把握し、それに適合した商品及びサービスを開発し、又は提案する場合
- (4) 法令の定める義務を履行する場合(「所得税法第10条」に基づく少額貯蓄非課税制度の適格性審査又は「外国為替及び外国貿易法第18条」に基づくマネーロンダリング防止等)

第2項

(1) 金融機関等は、例えば、次のような場合においては、明示的な方法により顧客の同意を得るものとする。

■ 個人信用情報機関等の情報を与信判断等に利用する場合及び個人信用情報を個人信用情報機関等へ提供する場合

■ 第三者(グループ会社を除く。)に提供する場合

(2) 上記(1)の「明示的な方法」とは、例えば、次のような方法をいう。

■ 申込書又は契約書等により個人データを収集する場合に、書面により同意を得る方法

- ・ 顧客自らが申込書等に同意する旨を記載する方法
- ・ 顧客が同意する旨の条項を記載した契約書、申込書又は所定の書面等に署名若しくは記名捺印する方法
- ・ 書面に設けられた同意する旨を記載した欄にチェックする方法

■ 電話又は面談により個人データを収集する場合に、口頭により同意を得る方法

■ コンピュータ等により個人データを収集する場合に、本人確認を行ったうえで電子的手段により同意を得る方法

(3) 次の場合には、顧客が個人データの利用又は提供の目的について同意しているものとみることができる。

■ 利用又は提供の目的が一般的に明らかである場合で、顧客がその情報収集に応じるとき。

「一般的に明らかである場合」とは、例えば、次のような場合をいう。

- ・ 契約書の表題等で、顧客が目的を理解していると判断される場合
- ・ 市場調査又は統計処理等に利用する場合

■ 法令又は顧客によって公開された書類等(各種登記簿又は著作物の著者に関する情報)から個人データを収集する場合

■ 口座情報又は取引履歴等、契約締結に伴い収集した、又は契約履行の結果生じた個人データを業務上必要な範囲内で利用する場合

例えば、次のような場合をいう。

- ・ 顧客に適合した商品及びサービスを開発し、又は提案する場合
- ・ 普通預金残高等既に収集済みの情報を与信判断の参考とする場合

■ 収集した個人データを金融機関等が、ダイレクトマーケティングの目的で利用する場合

- ・ 「ダイレクトマーケティング」とは、金融機関等又はそのグループ会社が、個人データを利用して特定の商品又はサービスに適合する顧客を限定して行う、ダイレクトメールの送付やテレマーケティングその他のセールス活動(店舗等で直接面談して行うセールス活動を除く。)をいう。

■ グループ会社間で個人データを提供する場合

- ・ 「グループ会社」とは、連結財務諸表の対象となる親会社、子会社及び関連会社をいう。

顧客との契約を履行するために必要な範囲で個人データを提供する場合
例えば、次のような場合をいう。

- ・ 為替取引において被仕向銀行に個人データを提供する場合
- 保険契約等において契約内容に関する個人データを代理店に提供する
場合

- (4) 上記(3) 及び の場合には、その内容について、パンフレット、ダイレクトメール等へ掲載しなければならない。(後掲<説明の補足>2.参照)
- (5) 金融機関等は、申込書又は契約書の契約手続きの際に、契約締結又は契約履行に必ずしも必要とはいえない個人データを収集する場合には、その収集が任意であることを顧客が理解できるように努めるものとする。
- (6) 金融機関等は、個人データの収集に際して、顧客が同意の拒絶又は反対の意思を表明した場合には、それに対する金融機関等の対応について説明を行うものとする。

第3項

「顧客の同意を得た場合」とは、例えば、次のような場合をいう。

- (1) 勤務先情報及び振込依頼書の受取人情報として、政治又は宗教等に関する団体名を収集する場合
- (2) 健康又は生命に関する保険契約を締結する際に、保健医療に関する個人データを収集する場合
- (3) 特定の団体に所属することを条件とした提携ローンで、その団体への所属を確認するため、政治又は宗教に関する団体の情報を収集する場合

第4項

金融機関等は、例えば、次のような方法による収集をしてはならない。

- (1) 収集する目的を偽っての収集
- (2) 第三者から個人データを収集するに際して、その第三者が漏洩等の不当な行為をしていることを知った上での収集

第5項

金融機関等は、個人データを第三者から収集するに当たっては、顧客がその事実を知らないことがあり得るため、当該顧客の利益(生命、健康又は財産等の重大な利益をいう。)を不当に侵害することがないように十分留意するものとする。

(個人データの利用及び提供)

第6条 金融機関等は、前条第2項に定める範囲において、個人データを利用し又は提供するものとする。

- 2 前項の規定にかかわらず、金融機関等は、次の各号のいずれかに該当するときは、個人データを利用し又は提供することができる。
 - 一 顧客の同意をあらためて得た場合

- 二 法令の規定による場合
- 三 顧客の利益のために必要である場合
- 四 公共の利益のために必要である場合

〔説明〕

この条は、OECDガイドライン第10「利用制限の原則」並びにEU指令第6条1(a)、(b)、(c)及び第7条に対応するものである。

第1項

- (1) 「提供」とは、金融機関等がその管理する個人データを顧客及び外部委託先以外の者に利用可能なものにするをいう。
- (2) 金融機関等は、個人データの収集に際して、顧客の同意を得た利用又は提供の目的の範囲において、個人データを利用し又は提供するものとする。

第2項

金融機関等は、利用又は提供の目的の範囲外であっても、例えば、次のような場合には、個人データを利用又は提供することができる。

- (1) 契約手続きの際に収集した個人データを、第三者(グループ会社を除く。)に提供するため、あらためて同意を得た場合
- (2) 裁判官の発付する令状により強制処分として搜索若しくは押収がなされる場合、又は法律上の照会権限を有する者からの照会(「刑事訴訟法第197条第2項」等)がなされた場合
- (3) 顧客が疾病又は傷害により意思表示不能になった際に、預金口座等の情報を当該顧客の利益のために法定代理人に提供する場合
- (4) 犯罪の防止等、公共の利益のために必要である場合

第3章 適正管理

(個人データの適正管理)

第7条 金融機関等は、個人データを業務上必要な範囲内で正確かつ最新の状態に管理するものとする。

2 金融機関等は、業務上必要な期間を経過した後は、個人データの廃棄その他の処理を行うものとする。

〔説明〕

この条は、OECDガイドライン第8「データの正確性の原則」及びEU指令第6条1(d)、(e)に対応するものである。

第1項

不正確な個人データが利用されると、顧客について誤った認識がもたれ、当該顧

客にとって不利益な結果を生ずるおそれがあるため、金融機関等は個人データを正確な状態に管理する必要がある。

また、収集した時点で正確であった個人データでも、後に利用される時点では事実と合わなくなっていることも考えられるため、最新性の確保も必要である。

しかしながら、取引密度や利用目的等によっては必ずしも個人データの更新を必要としない場合もあるため、金融機関等は業務上必要な範囲内で正確性及び最新性を確保するものとする。

第2項

「廃棄その他の処理」とは、金融機関等が、個人データを廃棄すること、削除すること、又は識別できない状態にすることをいう。

(個人データの安全保護措置)

第8条 金融機関等は、個人データへの不当なアクセス又は個人データの紛失、破壊、改ざん、漏洩その他の危険に対して、必要な安全保護措置を講じるものとする。

(説明)

この条は、OECDガイドライン第11「安全保護の原則」及びEU指令第17条1に対応するものである。

(1) 金融機関等は、安全保護措置を講じる際に、個人データの機密性、量、分類、形式及び記憶装置等を考慮するものとする。

(2) 金融機関等は、例えば、次のような手法を用いて個人データを安全に保護するものとする。

■ 個人データを保護している格納箱の施錠、又は設置している建物への入室の制限等の物理的措置

■ 個人データを閲覧し又は利用することができる者を制限する内部規定を作成する等の組織的措置

■ パスワード、ID番号、暗号等を使用した電子的措置

(3) 安全保護措置については、(財)金融情報システムセンター『金融機関等コンピュータシステムの安全対策基準』及び『金融機関等における個人データの厳正管理のための留意点』を参照するものとする。

(外部委託)

第9条 金融機関等は、個人データの取扱いを委託する場合には、外部委託先との委託契約を締結するに当たって、金融機関等と同等の個人データの保護に関する事項について定めるものとする。

(説明)

この条は、EU指令第17条4に対応するものである。

- (1) 「外部委託先」とは、コンピュータ処理会社又はメール発送業者等、金融機関等から個人データの収集、利用若しくは提供又は個人データを必要とする業務を受託している者をいう。
- (2) 金融機関等は、外部委託先との委託契約において、外部委託先がその従業員も含め、受託により知り得た個人データを金融機関等の指示又は法令の規定に基づいてのみ利用し、かつ、当該個人データを当該受託業務以外の業務のために利用しないことを定めるものとする。
- (3) 外部委託先との委託契約における保護措置については、(財)金融情報システムセンター『金融機関等における個人データの厳正管理のための留意点』の外部委託に関する規定を参照するものとする。

第4章 開示請求等への対応

(開示請求等への対応)

第10条 金融機関等は、顧客から自己の個人データについて開示の請求があった場合、訂正の請求があった場合、及び利用又は提供の中止の請求があった場合には、これに応じるものとする。

[説明]

この条は、OECDガイドライン第13「個人参加の原則」並びにEU指令第12条及び第14条(b)に対応するものである。

- (1) 「開示」とは、金融機関等が、顧客に対して、当該顧客に関する個人データの保有の有無及び内容を伝達すること、又は閲覧に供することをいい、「中止」とは、金融機関等が、個人データのダイレクトマーケティングの目的での利用、又はグループ会社への提供を行わないことをいう。
- (2) 金融機関等は、顧客から合理的な間隔をあけて、収集した個人データ及び契約の履行の結果生じた個人データについて開示するように請求があった場合には、請求者が当該顧客であることを確認の上、当該個人データの保有の有無及びその内容を、合理的な期間内に、当該顧客が容易に理解できるように、合理的な方法で、開示するものとする。なお、必要な場合には相応の手数料を徴求することができる。
- (3) 金融機関等は、顧客の開示請求に応じることができない場合には、その理由を説明するものとする。

「顧客の開示請求に応じることができない場合」とは、例えば、次のような場合をいう。

■ 終了した取引に関する個人データ等、顧客の現に得ている利益と関連性に乏しい、又は顧客へもたらされる利益が極めて小さいと考えられる開示請求を受けた場合

- データが保有期限経過後又はコンピュータにより処理される以前のため検索不能である場合
 - 他の顧客の個人データが含まれている場合
 - 金融機関等の企業秘密等を侵害するおそれがある場合
- (4) 金融機関等は、顧客から合理的な間隔をあけて、金融機関等が開示した個人データの訂正又は変更を行うように請求があった場合には、公的資料等で客観的に確認でき、かつ、金融機関等が当該個人データの利用の目的に照らして必要と判断したときは、合理的な期間内に、個人データの訂正又は変更を行うものとする。なお、必要な場合には相応の手数料を徴求することができる。
- (5) 金融機関等は、顧客から中止するように請求があった場合には、既に当該顧客の同意を得ている場合を含め、合理的な期間内に、中止するものとする。

第5章 管理体制の整備

(管理体制の整備)

第11条 金融機関等は、個人データを保護するために、管理体制の整備に努めるものとする。

(説明)

この条は、OECDガイドライン第14「責任の原則」及びEU指令第6条2に対応するものである。

- (1) 金融機関等は、収集した個人データ(外部委託先及びグループ会社が管理している個人データを含む。)の取扱いについて責任を負うものとする。
- (2) 金融機関等は、個人データを保護するために、個人データの保護に関するルールを作成や、これに沿う形での事務の取扱い等に関するルールを作成に努めるものとする。
- (3) 金融機関等は、個人データの保護全般の取りまとめを担当する部署を定め、担当者(氏名又は役職名)を指名すること等により管理体制を整備し、内部監査、従業員への教育、顧客の相談及び苦情への適切な対応に努めるものとする。
- (4) 金融機関等は、顧客から個人データの保護の考え方又は当該顧客に関するデータの取扱状況等について質問を受けたときは、その内容について調査し、合理的な期間内に、かつ合理的な方法で回答するものとする。
- (5) 金融機関等は、顧客からの苦情が正当なものと認められる場合、この苦情の解決に努めるものとする。

<説明の補足>

1. 顧客への周知について(第3条の説明)

- (1) 顧客への周知の方法としては、店頭取引、電話による取引及び電子的手段による取引等、取引の種類に応じて、例えば、次のような方法を選択するものと

する。

■ 店頭への冊子(パンフレットを含む。)の備付け

■ ポスターの掲示

■ インターネットホームページへの掲載

■ ディスクロージャー誌等への掲載

(2) 顧客への周知の内容については、顧客が理解しやすく、かつ、読みやすいものとし、例えば、次のようなものを含むものとする。

■ 個人データが主としてどのような目的のために収集若しくは利用されるか、又はどのような業務を行っている者に提供されるかについての説明

・ 金融機関等は、適切な契約を締結し、及び契約を安全かつ確実に履行するために、個人データを収集し、又は利用すること。

・ 金融機関等は、法令の規定により提供が求められる場合等を除き、顧客の同意を得ないで個人データを提供しないこと。

・ 金融機関等が個人データを提供するグループ会社の名称及び業務内容

■ 顧客が開示請求又は訂正請求を行う方法

・ 開示請求及び訂正請求はどの部署に対して(支店又は営業所の場合を含む。)、どのような方法(文書又は口頭等)で行うか。

・ 請求が有料の場合はその旨

■ 個人データに関する質問又は苦情を受け付ける部署名及び連絡先

2. ダイレクトマーケティングの目的で個人データを利用する場合及びグループ会社間で個人データを提供する場合について(第5条第2項(4)の説明)

金融機関等が、収集した個人データをダイレクトマーケティングの目的で利用する場合及びグループ会社間で個人データを提供する場合には、次の内容について、パンフレット、ダイレクトメール等へ掲載しなければならない。

(1) ダイレクトマーケティングの目的での利用及びそれに対する中止請求

■ ダイレクトマーケティングの目的で個人データを利用することについて、顧客が中止を請求できること。

■ 中止を請求する場合の方法及び連絡先

(2) グループ会社への提供及びそれに対する中止請求

■ グループ会社へ個人データを提供することについて、顧客が中止を請求できること。

■ 個人データを提供するグループ会社の名称及びその業務内容

■ 中止を請求する場合の方法及び連絡先

<参考>パンフレット例

～お客様に関する情報の取扱いについて～

弊社では、お客様からの信頼を第一と考え、以下の考え方に沿って、お預かりしたお客様に関する情報をお客様のご希望に沿って取り扱うとともに、正確性・機密性の保持に努めています。

1 情報を収集する目的

お客様とのお取引を安全確実に進め、より良い商品・サービスを提供させて頂くため、お客様に関する必要最小限の情報を収集させて頂いております。これらの情報は、ご本人かどうかの確認、融資のご利用に際しての判断、新しい商品・サービスのご紹介などの目的のために利用されます。

2 収集する情報の種類

最も一般的なものは、お客様の住所、氏名です。その他では、ローンなどの信用供与の際に、資産、ご年収、ご勤務先、信用履歴などが必要となる場合があります。

3 情報の収集方法

十分な安全保護措置を講じた上で、主に申込書・契約書や取引書類に記載・入力された情報を収集しています。このほか、ローンなどを申し込まれたお客様につきましては、個人信用情報機関等に信用情報を照会する場合があります。

4 情報の利用・提供

弊社および弊社グループ会社(グループ会社一覧は別添リスト<略>を参照してください。)では、次の場合を除いて、お客様の情報を利用したり外部に提供することはありません。

- ・お客様が同意されている場合
- ・法令により必要と判断される場合
- ・お客様または公共の利益のために必要であると考えられる場合

5 情報の管理方法

お客様の情報を正確、最新なものにするよう常に適切な措置を講じています。また、お客様の情報への不当なアクセスなどが行われることを防止するため、万全を尽くしています。

6 お客様からの開示、訂正、中止のご請求

(開示、訂正)

お客様からご自身に関する情報の開示のご依頼があった場合は、請求者がご本人であることを確認させて頂いたうえで、特別な理由のない限りお答えしています。また、お預かりした情報が不正確である場合には、正確なものに変更させて頂きません。下記のお問い合わせ窓口までお申し出下さい。

(中止)

ダイレクトメールと電話によるご案内、および弊社グループ会社間でのお客様の情報の共有について、お客様がご希望されない場合は下記のお問い合わせ窓口までお申し出下さい。取扱いを中止させていただきます。

[お問い合わせ窓口]

開示・訂正・中止のご請求、その他の不明点についてのご照会は、下記までご連絡頂きますよう、お願いします。

株式会社

部

所在地

電話 XXXX-XXXX-XXXX