

「金融分野における個人情報保護に関するガイドライン」の改正について

個人情報の保護に関する法律(平成15年法律第57号。以下「個人情報保護法」といいます。)が平成17年4月に全面施行(一部は平成15年5月から施行)されてから約5年が経とうとしておりますが、平成21年11月20日に、「金融分野における個人情報保護に関するガイドライン」(平成16年金融庁告示第67号)が改正され、施行されました(以下、改正前のガイドラインについて「改正前ガイドライン」、改正後のガイドラインについて「改正後ガイドライン」といいます。)。本ニューズレターでは、同ガイドラインの改正の経緯について説明した後、改正の内容及び今後の課題について記載致します。

1. ガイドラインの改正の経緯

(1) 金融分野における個人情報保護に関するガイドライン

個人情報保護法の一部施行に伴い、政府は、平成16年4月に「個人情報の保護に関する基本方針」において、各省庁に対し、「それぞれの事業等の分野の実情に応じたガイドライン等の策定・見直しを検討」し、特に金融・信用等の分野において、個人情報の厳格な取扱いを図るよう規定しました。

これを受けて、金融庁は、本格的に審議を開始し、金融分野の事業者における個人情報の適切な取扱いを確保するため、平成16年2月に「金融分野における個人情報保護に関するガイドライン」を策定・公表するに至りました。

(2) ガイドラインの改正

個人情報保護法の全面施行から3年を迎えることを受け、平成19年6月に、同法の施行状況のフォローアップを目的として、国民生活審議会から「個人情報保護に関する取りまとめ」(意見)が公表されました。この意見では、各省庁において策定されている個人情報保護に関する事業分野ごとのガイドラインについて、「複数のガイドラインが適用される事業者があることにも留意しつつ、政府において、ガイドラインの共通化について必要な検討を行っていくべき」と指摘されました。この指摘及び平成20年4月に一部変更された「個人情報の保護に関する基本方針」⁽¹⁾に基づき、内閣府から、個人情報保護に関するガイドラインの共通化についての考え方⁽²⁾が示され、「標準的なガイドライン」が策定されました⁽³⁾。このような中、平成20年7月に開催された個人情報保護関係省庁連絡会議において、各省庁は、それぞれ策定しているガイドラインについて共通化できる部分について、その見直しの検討を行うことについて申し合わせを行いました。ここでは、ガイドラインの共通化の目的として、事業分野ごとの事情を踏まえながらも、民間分野の個人情報保護制度を対外的に分かりやすくすることが挙げられ、事業分野の特殊性に応じて、各省庁によるガイドラインの見直しが要請されました。これを受けて、平成21年11月にガイドラインが改正及び施行されました。

本ニューズレターの執筆者



あいとう そう
齋藤 創

パートナー
弁護士



いとう まや
伊藤 真弥

アソシエイト
弁護士

本ニューズレターは法的助言を目的とするものではなく、個別の案件については当該案件の個別の状況に応じ、弁護士の助言を求めて頂く必要があります。また、本稿に記載の見解は執筆担当者の個人的見解であり、当事務所または当事務所のクライアントの見解ではありません。

西村あさひ法律事務所 広報室
(電話:03-5562-8352 E-mail:info@jurists.co.jp)

2. 改正の内容

(1) リスクに応じた安全管理措置等

改正点

いわゆる「過剰反応」の状況を改善するため、「漏えい等が発生した場合の本人の権利利益の侵害の大きさ」を考慮し、リスクに応じた適切な対応をしていくことが可能であることが明示されました。

改正前ガイドラインにおいては、個人情報取扱事業者は、個人データの安全管理のため、安全管理措置に係る規程等の整備及び実施体制の整備等を講じ、従業員に対する必要且つ適切な監督を行い、また、委託を受けた者に対する必要且つ適切な監督を行わなければならないとされておりました。これに対し、改正後ガイドラインでは、個人情報取扱事業者が個人データの漏えい等の防止のために講ずべき上記安全管理措置、従業員の監督及び委託先の監督について、「個人データが漏えい、滅失又はき損等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、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」とすべき旨規定しております(改正後ガイドライン 10 条ないし 12 条)。

同改正の理由としては、昨今の個人情報保護に関する「過剰反応」、即ち、プライバシー意識の高まりや個人情報を取り扱う上での戸惑い等の要因から、社会的な必要性があるにもかかわらず、法の定め以上に個人情報の利用を控えてしまう状況を改善するためであると考えられます。

この改正により、従来要求されていた安全管理措置、従業員の監督及び委託先の監督について、改正後は「漏えい等が発生した場合の本人の権利利益の侵害の大きさ」を考慮し、リスクに応じた適切な対応をしていくことが可能となりました。

例えば、「不特定多数者が書店で随時に購入可能な名簿で、事業者において全く加工をしていないものについては、個人の権利利益を侵害するおそれは低いと考えられることから、それを処分するために文書裁断機等による処理を行わず

に廃棄し、又は廃品回収に出したとしても、事業者の安全管理措置の義務違反にはならない」旨挙げられております(改正後ガイドライン 10 条 1 項)。また、その他の具体例としては、漏えいした個人データに対して高度の暗号化処理等が施されている場合や、即時に回収できた場合等は、本人が被る権利利益の侵害の程度がある程度低いと考えられることから、本人への通知⁽⁴⁾に関しては省略することができること等が考えられます⁽⁵⁾。

(2) 消費者保護の観点からプライバシーポリシー等に盛り込む事項

改正点

プライバシーポリシー等に関して、消費者等の権利利益保護の観点から、より詳細な記述を盛り込むことが望ましいものとされました。

改正後ガイドラインでは、個人情報取扱事業者が策定・公表しているプライバシーポリシー等に、消費者等の権利利益保護の観点から、以下①ないし④に掲げる点を考慮した記述をできるだけ盛り込むことが望ましいものとされました(改正後ガイドライン 23 条 2 項)。

① 本人からの要請による個人情報の利用停止

保有個人データについて本人から求めがあった場合には、ダイレクトメールの発送停止等、自主的に利用停止等に応じること。

② 個人情報の取扱いの委託状況の透明化の推進

委託の有無、委託する事務の内容を明らかにする等、委託処理の透明化を進めること。なお、「金融分野における個人情報保護に関するガイドライン」の改正案についてのご意見等及びご意見等に関する考え方(以下「パブリックコメント回答」といいます。)において、金融庁は、委託する事務が多数に上る場合で、その全てを列挙することが困難な場合には、委託する事務の例示であっても委託処理の透明化に資するものと回答しております。

③ 顧客の種類ごとの利用目的の限定及び本人の選択による利用目的の限定

事業者がその事業内容を勘案して顧客の種類ごとに利用目的を限定して示したり、事業者が本人の選択による利用目的の限定に自主的に取り組む等、本人にとって利用目的がより明確になるようにすること。なお、「顧客の種類ごとに利用目的を限定」とは、例えば、「複数の事業を展開している場合に、その事業毎に利用目的を定める」ことや、「個人情報の取得の場面ごとに顧客の種類を分類し(例:アンケートに協力した顧客、イベントに参加した顧客、窓口にお問い合わせをした顧客等)、それぞれに応じた利用目的を示すこと」等が想定されます⁽⁶⁾。

④ 個人情報の取得元又はその取得方法の明記

個人情報の取得元又はその取得方法(取得源の種類等)を可能な限り具体的に明記すること。なお、パブリックコメント回答において、金融庁は、個人情報の取得元や取得方法が多数に上る場合は、その例示であっても本人の権利利益の保護に資するものと回答しております。

(3) 主務大臣の権限行使の対象の明確化

改正点

いわゆる「過剰反応」の改善のため、ガイドラインの規定の予測可能性を高める改正がなされました。

改正後ガイドラインでは、義務規定と努力規定の区別を明確にし、改正後ガイドライン 24 条において「「勧告」、「命令」及び「緊急命令」についての考え方」の規定を設け、個人情報保護法に基づく金融庁長官の権限行使の手続きを規定しました。

同改正の理由としては、先に述べましたいわゆる「過剰反応」が生じていることを踏まえ、個人情報取扱事業者の予測可能性を明確にすることが考えられます。

具体的には、改正後ガイドライン中「～ならない」(「努めなければならない」を除きます。)と規定されている条項に違反した場合で、且つ、当該違反について個人の権利利益を保護する

ため必要と認められる場合には、勧告等の対象となります。他方、「こととする」、「適切である」及び「望ましい」と記載されている条項については、個人情報取扱事業者は当該条項の遵守に努めるものとされ、その違反は勧告等の対象とはならないものとされました。

なお、改正後ガイドラインにおいて、「～ならない」と改正された条項に、「委託先の監督」についての条項があります(改正後ガイドライン 12 条 3 項)。「委託先の監督」は、改正前ガイドラインにも存在しておりましたが、今般、委託先の個人データの安全管理措置が図られるよう、個人データの安全管理のための措置を委託先においても「確保しなければならない」と規定されました。これにより、委託先における安全管理措置を怠った場合には、勧告等処分の対象となり得ることが明確化されました。

(4) ガイドラインを分かりやすくするための具体例等の追加

改正点

ガイドラインを消費者等にとってより理解し易いものとするために、具体例等の追加が行われました。

例えば、個人情報取扱事業者は、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ものとされておりますが(個人情報保護法 6 条、改正後ガイドライン 5 条)、「法令に基づく場合」には、この適用がありません。かかる「法令に基づく場合」として、金融商品取引法(昭和 23 年法律第 25 号)210 条、211 条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に応じる場合や、弁護士法(昭和 24 年法律第 205 号)23 条の 2 第 2 項に基づく弁護士会の照会に応じる場合等が具体例として記載されております。

また、個人情報取扱事業者が、本人から保有個人データの開示を求められた場合には、これを開示しなくてはならないものとされておりますが(個人情報保護法 25 条、改正後ガイドライン 15 条)、これを開示しなくてよい「当該個人情報取扱事業者の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」として、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や企業秘密が明らかになるおそれがある場合が、また、「他の法令に違反することとなる場合」として、犯罪収益移転防止法(平成19年法律第22号)9条2項(顧客への届出事実の漏えい)の場合が具体例として追加されています。

さらに、個人情報取扱事業者は、個人情報を取得した場合は、原則として、速やかにその利用目的を本人に通知又は公表しなければならないとされておりますが(個人情報保護法18条2項、改正後ガイドライン8条)、その例外である「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」として、「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」が具体例として追加されております。

(5) ガイドラインの見直しについて

改正点

ガイドラインに関し、必要に応じ見直しを行う旨の規定が追加されました。

改正後ガイドラインでは、ガイドラインは、社会情勢の変化、国民意識の変化、技術動向の変化等諸環境の変化を踏まえ、必要に応じ見直しを行うものと規定されました(改正後ガイドライン25条)。

3. 今後の課題

改正後ガイドラインの改正点は、大別して、過剰反応の防止のための改正、と、更なる個人情報保護のための改正、という二つの視点があるものと考えられます。

過剰反応の防止のための改正として、「漏えい等が発生した場合の本人の権利利益の侵害の大きさを考慮し、リスクに応じた適切な対応をしていくことが可能であることが明示された」点は、金融機関にとっても一定の評価が可能な点だと思われる

ます⁽⁷⁾。

他方、改正後ガイドラインにおいてはあくまで例示としては「不特定多数者が書店で随時に購入可能な名簿で事業者において全く加工していないもの」を例示するのみであり、パブリックコメント回答でも、かかる例示以上の回答は基本的になされておらず、過剰反応の防止のために十分な効果があるのかという点については、不明確さが残ります。

ガイドラインやパブリックコメント回答は一般論でありやむを得ない点もあるものの、仮に今後も過剰反応の解消がおこななければ、改正後ガイドライン25条が述べる通り、「社会情勢の変化、国民意識の変化、技術動向の変化等諸環境の変化を踏まえ、必要に応じ見直しを行う」ことが必要となることも考えられます。金融機関においては、今後、自らの判断において過剰反応ではない適切な実務の構築を行うことが当然に必要となりますが、かかる実務構築のため、当局との間の積極的な情報交換や情報発信等が必要になるものと思われる。

以上

⁽¹⁾ <http://www.caa.go.jp/seikatsu/kojin/kihontaishohyou2008.pdf>

⁽²⁾ <http://www.caa.go.jp/seikatsu/kojin/gaidoraintentou/kyoutuuka1.pdf>

⁽³⁾ <http://www.caa.go.jp/seikatsu/kojin/gaidoraintentou/kyoutuuka2.pdf>

⁽⁴⁾ 「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」(平成17年金融庁告示第1号)Ⅱ-6-1参照

⁽⁵⁾ 森敬洋「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改正」金融法務事情1883号32頁

⁽⁶⁾ 内閣府国民生活局「「個人情報の保護に関する基本方針」の一部変更案に関する国民から寄せられた御意見について<内閣府の考え方>」9頁

⁽⁷⁾ なお、そもそも金融機関が保有する個人情報には、口座番号、暗証番号、生体認証情報、与信ブラックリスト情報等々、当該データの漏えいがあった場合の経済的損失レベル、精神的苦痛レベルが高い情報が多数含まれており(原田克樹「金融分野における個人情報ガイドラインの改正と金融機関の体制整備」ファイナンシャルコンプライアンス2009年11月号55頁)、このような情報の管理については、改正後ガイドラインにおいても、改正前ガイドライン時と変わらぬ最大限の慎重な管理が必要とされる点には留意が必要となります。