

平成 27 年 5 月 8 日

金融庁総務企画局企画課調査室 御中

一般社団法人全国銀行協会

「金融分野における個人情報保護に関するガイドライン」および「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」の改正案に対する意見について

平成 27 年 4 月 6 日付で意見募集のあった標記の件に対する意見を別紙のとおり取りまとめましたので、何卒ご高配賜りますようお願い申し上げます。

以 上

「金融分野における個人情報保護に関するガイドライン」および「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」の改正案に対する意見

項番	該当箇所	意見	理由等
金融分野における個人情報保護に関するガイドライン改正案			
1	7条	登記簿謄本の情報をリスト化したものを第三者から取得する場合など、公表情報のみで構成された個人データを第三者から取得する場合において、適法に取得されたかどうかの確認方法として「公表情報(登記簿謄本等)との整合性の検証」が含まれるとの理解でよいか。	契約書等の書面の点検を行わずとも、第三者から取得した当該個人データが公表されている情報で構成されていること(整合性)を確認できれば、本条の主旨である「不適切な取得方法での情報の取得防止」は、当該個人データが公表情報であり、満たしていると考えられるため。
2	12条1項	「事業の規模」とは、委託先企業の事業規模ではなく、委託する事業自体の規模との理解でよいか。	規定の趣旨等の明確化のため。
3	12条1項	「委託する事業の規模」に関しては、一律の基準等はなく、各金融機関のリスクベース等で判断するものとの理解でよいか。例えば、「委託先に取扱いを委託する個人データの量(件数)」などを勘案して、各金融機関が判断することも妨げられないとの理解でよいか。	規定の趣旨等の明確化のため。
4	12条3項①	左記の規定における「必要に応じて」の具体的内容や、「これに代わる合理的な方法による確認」の具体的確認方法には、一律の基準等はなく、各金融機関のリスクベース等で判断するものとの理解でよいか。	規定の趣旨等の明確化のため。
5	12条3項①	例えば、委託開始前や委託中(1年毎)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の安全管理措置等についての実務指針」の各項目の実施状況を確認する書面を委託先から提出してもらう方法や、第三者による監査報告書を委託先から受け入れるといった方法は、「これに代わる合理的な方法による確認」として許容されるとの理解でよいか。	規定の趣旨等の明確化のため。

項番	該当箇所	意見	理由等
6	12条3項②	「個人データ管理責任者等」の定義は「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」に定義されているものと同義であるとの理解でよいか。また、「等」に含まれる具体的な範疇に特段の定めはなく、各金融機関が実務等を踏まえて判断するものとの理解でよいか。	規定の趣旨等の明確化のため。
7	12条3項②	「定期的に監査を行う等」には、例えば、「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」の各項目の実施状況を確認する書面を委託先から提出してもらい、個人データを取り扱う場所に赴いて、方針・規定・実施体制の整備状況や運用状況を確認すること、またはそれに代わる第三者による監査報告書を委託先から受け入れるといった方法等が含まれるとの理解でよいか。	規定の趣旨等の明確化のため。
8	12条3項②	「安全管理措置等」の「等」には、例えば、委託先が再委託を行う場合に、「委託先の事前報告または承認手続を求めること」や「直接または委託先を通じて定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと」といったことも含まれるとの理解でよいか。	規定の趣旨等の明確化のため。
9	12条3項②	委託先を通して再委託先以降の管理が確認できればよく、再委託先以降を必ず直接監督しなければならない趣旨ではないとの理解でよいか。加えて、委託先と再委託先の契約の見直しを求めるものではなく、委託先を通じて再委託先を監督し、問題があると判断した場合、「再委託先として許容しない」といった判断を、各金融機関がリスクベース等にもとづきそれぞれが判断するものとの理解でよいか。	規定の趣旨等の明確化のため。
10	12条3項②	「再委託先が法20条に基づく安全管理措置を講ずることを十分に確認すること」には、例えば、再委託開始前や再委託中(1年毎)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の安全管理措置等についての実務指針」の各項目の実施状況を確認する書面(あるいはその写)や、第三者による監査報告書を委託先から受け入れるといった方法等が含まれるとの理解でよいか。	規定の趣旨等の明確化のため。
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改正案			
11	I.(2) 2-5-2(注)	「社内の対応の確認」の頻度については、一定の基準等はなく、各金融機関のリスクベース等で判断するものとの理解でよいか。	規定の趣旨等の明確化のため。

項番	該当箇所	意見	理由等
12	I.(2) 2-5-2(注)	「情報セキュリティ対策に十分な知見を有する者」に係る経験年数等の要件に関しては、一定の基準等はなく、各金融機関が実情等を踏まえて判断し、要件を設定すべきものとの理解でよいか。	規定の趣旨等の明確化のため。
13	I.(2) 4-7	「監視システムの動作の定期的な確認」とは、監視システム等が問題なく作動していることなどを確認するといったことを意味しているとの理解でよいか。	規定の趣旨等の明確化のため。
14	III. 5-3(注)	左記で定める対応を求める趣旨は、委託先との間で管理責任を明確にし、認識を共有することにあると認識しているが、例えば、委託先において個人データを取り扱う者の氏名・役職または部署名を委託契約に盛り込むことが望ましいものの、実務的に困難な場合、個人データを取り扱う部署名と責任者(必ずしも全員の氏名を求めるものではない)を覚書・別表・別データ等で盛り込むといった対応も許容されるとの理解でよいか。 また、そうした対応を行った以後、個人データを取り扱う者の異動等があり得ることから、例えば、委託先から年1回程度、定期的に報告するような対応(定期的に報告することを契約上義務づけること等)、委託先における個人データを取り扱う者の氏名・役職または部署名等を一覧として委託先社内管理し、それを委託元が確認するといった対応、定期的に実施する委託先への安全管理措置の遵守状況の検証において、個人データを取り扱う部署を把握・点検するといった措置で対応すること等も許容されるとの理解でよいか。	規定の趣旨等の明確化のため。また、個人データを取り扱う者の氏名・役職等を逐次契約に反映させることは困難な場合があるほか、委託契約の変更契約を締結するとなった場合、既存の委託先および委託元に相応の負担を強いることにもなるため。
15	III. 5-4	「定期的に監査を行う等」には、例えば、「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」の各項目の実施状況を確認する書面を委託先から提出してもらい、個人データを取り扱う場所に赴いて、方針・規定・実施体制の整備状況や運用状況を確認すること、またはそれに代わる第三者による監査報告書を委託先から受け入れるといった方法等が含まれるとの理解でよいか。	規定の趣旨等の明確化のため。
16	III. 5-4	「安全管理措置等」の「等」には、例えば、委託先が再委託を行う場合に、「委託先の事前報告または承認手続を求めること」や「直接または委託先を通じて定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと」等といった対応が含まれるとの理解でよいか。	規定の趣旨等の明確化のため。

項番	該当箇所	意見	理由等
17	Ⅲ. 6-1(注) 6-2-1(注) 6-3-1(注)	左記に規定する全ての措置を講じることが困難な場合には、物理的安全管理措置以外の措置と組み合わせるなどして、各機金融機関のリスクベース等にもとづいて判断し対応を行うことが可能との理解でよいか。	左記の規定は例示であるほか、実務上は技術的安全管理措置との組み合わせで対応しているケースや、コストや労力の点から即座に対応することが難しい場合もあるため。

以上