

「金融分野における個人情報保護に関するガイドライン」及び「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」の一部改正（案）に対する意見募集手続の結果について

「御意見に対する考え方」においては、以下の略称を用いています。

正式名称	略称
金融分野における個人情報保護に関するガイドライン	金融分野ガイドライン
金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針	実務指針
金融機関における個人情報保護に関するQ & A	金融分野Q & A
個人情報の保護に関する法律	個人情報保護法
個人情報の保護に関する法律施行規則	個人情報保護法施行規則
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）	通則ガイドライン
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）	外国第三者提供ガイドライン

以下の欄は、12月22日より開始した意見募集の際にお寄せいただいた御意見について記載しております。

No	該当条項	御意見	御意見に対する考え方
1	全体	今回のパブリックコメントの結果の公表時又は公表後すみやかに、「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）」と「金融分野における個人情報保護に関するガイドライン」の二段表」についても、改訂版を公表いただきますようお願いいたします。	本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。

No	該当条項	御意見	御意見に対する考え方
2	全体	<p>「金融分野における個人情報保護に関するガイドライン」及び「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」はそれぞれ横書きなのですから、新旧対照表も横書きの表で記載してください。</p> <p>通常金融庁所管の監督指針等横書きのもののパブリックコメントでは(直近の例でいえば、令和3年12月24日付「金融商品取引業等に関する内閣府令及び金融サービス仲介業者等に関する内閣府令の一部を改正する内閣府令(案)」等の公表について)別紙3から別紙6までが挙げられます。)、改正前が左に、改正後が右に設けられており、通常とは異なる書式であるため、大変読み難いです。何か特別な理由があつて縦書きの表を使用しているのでしょうか。理由についてご教示ください。</p>	<p>金融分野ガイドライン及び実務指針は、御意見にある監督指針等と異なり、告示として定められたものであり、現行の告示を基礎としてその一部を改正する必要があるためです。</p>
3	全体	<p>インターネット上の意見募集フォームを利用する場合について、「※文字化け等を防ぐため、半角カナ、丸数字、特殊文字は使用しないでください。」と注意書きがあります。パブリックコメントに付された「金融分野における個人情報保護に関するガイドライン」及び「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」は、丸数字やハイフンを使用して条文番号が振られており、意見を述べるにあたり、条文を特定するのに条文番号である丸数字等が使えないこと自体がそもそもおかしいと思います。また、ガイドラインの新旧対照表のファイルからそのまま</p>	<p>e-Gov上の御意見の投稿に際し、半角カナ、丸数字、特殊文字を使用できない点に係る御意見については、今後の参考といたします。</p> <p>なお、今般の改正は、現行の告示を基礎としてその一部を改正するものであり、それ以外の部分も含めて丸数字等を使用しないようにすることは困難です。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>コピーアンドペーストして、意見提出ができないことは、インターネット上からの意見募集を妨げる大きな要素となります。少なくとも、どのように表記をすれば良いか代替手段を例示すべきです。</p> <p>また、インターネット上の意見募集フォーム自体の改修を早急に行い、丸数字等の入力をできるようにするか、金融庁所管の監督指針ガイドライン等の条文番号について当該丸数字等を使用しないようにしてください。</p>	
4	全体	業法に与らない所謂フィンテック事業者等にも同等の義務を課すことでイコールフィッティングを図るものと思料します。	金融分野ガイドライン及び実務指針は、金融庁が所管する分野における個人情報、仮名加工情報、匿名加工情報又は個人関連情報を取り扱う個人情報取扱事業者等が適用の対象となります。
5	金融分野ガイドライン 第1条	引続き、金融機関自身の雇用管理情報、株主情報については、本ガイドラインの対象外であって、その取扱いは「個人情報の保護に関する法律についてのガイドライン（通則編）」等の共通ガイドラインにもとづき行うという理解でよいか。	御理解のとおりです。
6	金融分野ガイドライン 第3条	法（令和4年4月1日施行にかかるもの）31条1項では、個人関連情報取扱事業者は、提供先である第三者が個人関連情報を個人データとして取得することが想定されるときは、当該第三者において個人関連情報取扱事業者から個人関連情報の提供を受けて個人データとして取得する旨の本人の同意が得られていることを確認する義務があるとされている。	<p>提供元の個人関連情報取扱事業者は、提供先の第三者が個人関連情報を個人データとして取得することが想定される場合には、通則ガイドライン3-7-3に従って、本人の同意が得られていること等を確認する必要があります。</p> <p>なお、提供元の個人関連情報取扱事業者は、提供先の金融分野における個人情報取扱事業者による同意取得を代行する場合は、通則ガイドライン3-7-2、金融</p>

No	該当条項	御意見	御意見に対する考え方
		<p>この点、当該第三者が金融分野の事業者である場合、本改正案3条や14条に従い本人から同意を取得することが求められることになると考えられるが、提供元である個人関連情報取扱事業者における確認事項や確認方法は、通則ガイドラインで規定される内容、方法と同じという理解でよいか確認したい。</p>	<p>分野ガイドライン第3条及び第14条第1項に従って、本人の同意を取得する必要があります。</p>
7	金融分野ガイドライン第5条	<p>今回の改正対象ではないが、個人情報保護法が規定する「要配慮個人情報」に、当「ガイドライン」第5条で上乘せされている項目（下記）が見受けられる。「要配慮個人情報」と平仄を併せるべく、削除して頂きたい。</p> <p>労働組合への加盟 門地 本籍地 性生活</p> <p>その他（例えば、医師等の診断等によらず、自己判断により市販薬を服用しているといったケース）（出典 現行「金融分野における個人情報保護に関するQ&amp;A」8頁）</p>	<p>本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>
8	金融分野ガイドライン第8条	<p>物理的安全管理措置が従前「金融分野における個人情報保護に関するガイドライン」には記載されていなかったところ、今回の改正で記載されるようになった。そこで、その理由及び改正前後での「物理的安全管理措置」の差異について伺いたい。以下に記載のとおり理解でよいか。</p>	<p>御理解のとおりです。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>＜当方の理解＞</p> <p>今回意見募集を行っている「金融分野における個人情報保護に関するガイドライン」の改正前から、個人情報の保護に関する法律第20条（安全管理措置）及び個人情報保護委員会の通則編ガイドラインに基づき「物理的安全管理措置」を「金融分野における個人情報保護に関するガイドライン」の適用対象である事業者も講じることが求められていた。しかし、その旨は、「金融分野における個人情報保護に関するガイドライン」には記載がなかった。</p> <p>この度の改正では、「物理的安全管理措置」を「金融分野における個人情報保護に関するガイドライン」の適用対象である事業者も講じることが求められることを明記することにした。このように明記することが目的であるため、「金融分野における個人情報保護に関するガイドライン」の適用対象である事業者に求められる「物理的安全管理措置」の内容及び措置の水準は、「金融分野における個人情報保護に関するガイドライン」の改正前後で変化はない。</p>	
9	金融分野ガイドライン 第8条	安全管理措置において、「物理的安全管理措置」が追記された背景について、これまで「物理的安全管理措置」が記載されていなかった理由とあわせて教えていただきたい。	金融分野ガイドラインは、従前、「組織的安全管理措置」、「技術的安全管理措置」の観点で整理してきたところ、今般、通則ガイドラインと合わせ、「物理的安全管理措置」に係る規定を設けることとしました。
10	金融分野ガイドライン	“当該外国の個人情報の保護に関する制度等を把握する”とは具体的にどのようなことをどこまでを認識して	個人情報取扱事業者は、外国において個人データを扱う場合には、当該外国における個人情報の保護

No	該当条項	御意見	御意見に対する考え方
	<p>第8条 実務指針 6-1-2</p>	<p>いれば把握していると言えるのか？ 個人データの安全管理のために必要かつ適切な措置を講じることが当該外国の法律上問題ないことを確認できればよいか。</p> <p>また、実務指針において委託先選定の基準として“外的環境の把握”も含まれるが、委託先が個人情報の保護に関する制度等を把握しているかどうかについて具体的にどのように判断をすればよいか。例えば、研修等が行われていれば、把握していると判断してよいのか。</p> <p>(理由)</p> <p>諸外国の個人情報の法律に精通することは困難と考える。“制度等を把握している”とは、どこまで認識していることが把握していると言えるのか基準が曖昧なため。</p>	<p>に関する制度のみならず、当該外国における本人の権利利益に重大な影響を及ぼす可能性のある制度（個人情報の域内保存義務に係る制度や事業者に対し政府の情報収集活動への協力義務を課す制度等）等を確認した上で、それらに起因するリスクに応じて、必要かつ適切な安全管理措置を講ずる必要があります。</p> <p>また、金融分野における個人情報取扱事業者は、委託先選定の基準において、委託先が金融分野ガイドライン第8条第6項に従って外的環境の把握を行っていることを定める必要がありますが、委託先が当該選定の基準に合致しているか否かは、委託先に委託先における確認内容等を報告させること等により、判断することになると考えられます。</p>
11	<p>金融分野ガイドライン 第8条(2)</p>	<p>物理的安全管理措置に関しては、従来、「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）においては規定がなく、個人情報保護委員会が定める「個人情報保護法ガイドライン（通則編）」（以下、通則ガイドライン）が適用されていたが、今回の金融分野実務指針一部改正案において規定が新設されたため新設規定（案）が適用されることになる。</p> <p>物理的安全管理措置に関して、通則ガイドラインには「中小規模事業者における手法の例示」がなされているが、新設規定（案）では中小規模事業者に対する規定が</p>	<p>金融分野ガイドラインは、従前、「組織的安全管理措置」、「技術的安全管理措置」の観点で整理してきたところ、今般、通則ガイドラインと合わせ、「物理的安全管理措置」に係る規定を設けることとしました。</p> <p>「個人データの取扱区域等の管理」とは、個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域及びその他の個人データを取り扱う事務を実施する区域についてそれぞれ適切な管理を行わなければならないものであり、「個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等」には、通則ガイドラインの</p>

No	該当条項	御意見	御意見に対する考え方
		<p>なされていない。例えば、4-1では、「個人データの取扱区域等の管理」として講じなければならない措置として「個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等」が新設された。従来、通則ガイドラインでは「中小規模事業者における手法の例示」により「個人データを取り扱うことのできる従業者及び本人以外が容易に個人データを閲覧等できないような措置を講ずる」ことも許容されていたが、新設規定（案）では許容されないようにも読める。</p> <p>金融分野における個人情報取扱事業者といっても業容には差があり、役職員が数人の事業者では、例えば、「個人データ等を取り扱う重要な情報システムの管理区域への入退室管理」は極めて困難である。「個人データ等を取り扱う重要な情報システムの管理区域への入退室管理等」の「等」は、通則ガイドラインの「中小規模事業者における手法の例示」によることも許容されるという趣旨であることを確認したい。</p>	<p>「中小規模事業者における手法の例示」に挙げるものを含む上記を達することができる方法を含みます。</p>
12	金融分野ガイドライン 第8条第1項、 第8項	<p>生命保険会社では、従来、安全管理措置を、1. 組織的安全管理措置、2. 人的安全管理措置、3. 技術的安全管理措置の3つに分けて、必要な安全管理措置を講じております。</p> <p>今回の改正で、「物理的安全管理措置」という用語が、金融分野ガイドライン上、新設されておりますが、従来から生命保険会社は、個人情報保護法および同法ガイドライン（通則編）に基づき、「物理的安全管理措</p>	<p>金融分野ガイドラインは、従前、「組織的安全管理措置」、「技術的安全管理措置」の観点で整理してきたところ、今般、通則ガイドラインと合わせ、「物理的安全管理措置」に係る規定を設けることとしました。</p> <p>現在、「物理的安全管理措置」に相当する措置を既に定めているのであれば、本改正に合わせ、社内規程等において「物理的安全管理措置」に係る項目を新たに立てる必要はありません。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>置」に相当する安全管理措置を講じており、今後も法令に則り「物理的安全管理措置」に相当する安全管理措置を講じてまいります。</p> <p>上記の前提の下、生命保険会社の個人情報保護宣言や社内規程等において「物理的安全管理措置」という用語を用いることは必須ではなく、実態として物理的安全管理措置に相当する措置を含め、必要な安全管理措置を講じていれば足りるという理解でよろしいでしょうか。</p>	
13	金融分野ガイドライン 第8条第4項	<p>物理的安全管理措置について、「個人データの取扱区域等の管理」とはどの程度の範囲までか。例えば取扱区域として当行店舗内とするのか。リモートワーク等、店舗外にあるパソコンから個人データにアクセスする場合についてどのような対応が求められるか。</p>	<p>個人データの取扱区域の範囲に関しては、各個人情報取扱事業者の個人データの取扱状況や事業の規模等に応じて適切な範囲を設定いただくものと考えます。</p> <p>リモートワーク等の場合も含め、金融分野ガイドライン及び実務指針における安全管理措置に係る規定の趣旨を踏まえ、適切に御対応いただく必要があります。</p>
14	金融分野ガイドライン 第8条第4項、 第6項	<p>個人情報保護法第32条1項4号、および政令第10条1項では、「保有個人データの安全管理のために講じた措置（本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置くこと」が求められています。</p> <p>金融分野におけるガイドラインの第8条が該当しますが、「物理的安全管理措置」と「外的環境の把握」について、どのような方法で知り得る状態に置いたとみなされるのか、すなわちプライバシー・ステートメント等においてどの程度の粒度をもって記載すべきなのか、具体的</p>	<p>「保有個人データの安全管理のために講じた措置」については、本人の適切な理解と関与を可能としつつ、個人情報取扱事業者の適正な取扱いを促す観点から、「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」に置くことが求められるものです。</p> <p>「本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）」に置くとは、ホームページへの掲載、パンフレットの配布、本人の求めに応じて遅滞なく回答を行うこと等、本人が知ろうとすれば、</p>



No	該当条項	御意見	御意見に対する考え方
		<p>に示されたい。また、同様に、問い合わせ窓口を設けた上で、本人の求めがあった場合には、「物理的安全管理措置」と「外的環境の把握」についてどの程度の粒度をもって示すべきなのか、回答例などを示されたい。</p>	<p>知ることができる状態に置くことをいい、常にその時点での正確な内容を本人の知り得る状態に置かなければなりません。例えば、問合せ窓口を設け、問合せがあれば、口頭又は文書で回答できるよう体制を構築しておく場合がこれに当たります。</p> <p>「物理的安全管理措置」について、本人の知り得る状態に置く内容の事例としては、以下が考えられます。</p> <ul style="list-style-type: none"> <li>・ 個人データを取り扱う区域において、従業員の入室管理及び持ち込む機器等の制限を行うとともに、権限を有しない者による個人データの閲覧を防止する措置を実施</li> <li>・ 個人データを取り扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するための措置を講じるとともに、事業所内の移動を含め、当該機器、電子媒体等を持ち運ぶ場合、容易に個人データが判明しないよう措置を実施</li> </ul> <p>また、「外的環境の把握」について、個人情報取扱事業者が外国の個人情報の保護に関する制度等を把握した上で講じた安全管理措置の内容を本人の知り得る状態に置く必要があります。外国（本邦の域外にある国又は地域）の名称については、必ずしも正式名称を求めるものではありませんが、本人が合理的に認識できると考えられる形で情報提供を行う必要があります。また、本人の適切な理解と関与を促す観点から、</p>

No	該当条項	御意見	御意見に対する考え方
			<p>保有個人データを取り扱っている外国の制度についても、本人の知り得る状態に置くといった対応が望ましいものと考えます。外国の個人情報の保護に関する制度について、個人情報保護委員会において、個人情報取扱事業者の参考となる一定の情報を取りまとめて公表しておりますので、本人の知り得る状態に置くことが望ましい外国の制度の粒度に関し御参照ください。</p> <p>上記の他、保有個人データの安全管理のために講じた措置として本人の知り得る状態に置くべき内容の粒度については、通則ガイドライン3-8-1(1)【安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】及び【中小規模事業者(※10)における安全管理のために講じた措置として本人の知り得る状態に置く内容の事例】を御参照ください。</p>
15	金融分野ガイドライン 第8条第6項	金融分野において想定される、「外国において個人データを取り扱う場合」および「必要かつ適切な措置」の具体例を示していただきたい。	<p>例えば、以下に掲げるような場合は、「外国において個人データを取り扱う場合」に該当します。</p> <ul style="list-style-type: none"> <li>・個人情報取扱事業者が、外国にある支店・営業所に個人データを取り扱わせる場合</li> <li>・個人情報取扱事業者が、外国にある第三者に個人データの取扱いを委託する場合</li> </ul> <p>また、安全管理措置は、事業の規模及び性質、保有個人データの取扱状況等に起因するリスクに応じて、必要かつ適切な内容としなければならない。その内容は個人情報取扱事業者によって異なりますので、一律にはお答えしかねます。</p>

No	該当条項	御意見	御意見に対する考え方
16	金融分野ガイドライン 第8条第6項	例えば海外支店や出張所において、国内にある者を本人とする個人情報の漏えい等事案が発生した場合は、日本の当局に漏えい等の報告をすることが求められるか。	<p>外国にある個人情報取扱事業者等が、日本の居住者等国内にある者に対する物品又は役務の提供に関連して、国内にある者を本人とする個人情報等を、外国において取り扱う場合には、個人情報保護法が適用されます（個人情報保護法第166条）。</p> <p>このため、外国にある個人情報取扱事業者等は、個人情報保護法第26条第1項に従って、個人情報保護法施行規則第7条各号に該当する漏えい等事案が発生した場合は、個人情報保護委員会又は監督当局に報告をする必要があります。また、個人である顧客等に関する個人データの漏えい等事案が発生した場合は、各業法に基づき、監督当局に報告をする必要があります。</p>
17	金融分野ガイドライン 第8条第7項	「漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）」とありますが、「漏えい等のおそれのある事案」を加えた立法事実、制度趣旨及び想定される具体例について、ご教示ください。	<p>改正前の金融分野ガイドライン第8条第5項の規定する「漏えい事案等」とは、「漏えい等のおそれがある事案」を含むものであるところ、今回の改正では、これを分かりやすく示す観点から、通則ガイドラインにおいて「漏えい等又はそのおそれのある事案」を「漏えい等事案」と定義していることと合わせ、「漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）」と表現を修正しております。改正前後で実質的な変更はありません。</p> <p>個人情報取扱事業者は、漏えい等の「おそれ」を把握した場合には、早急に事態を把握して、必要な措置を講じる必要があると考えられます。これを踏まえ、</p>

No	該当条項	御意見	御意見に対する考え方
			<p>金融分野ガイドライン第8条第7項では、「漏えい等事案（漏えい等又はそのおそれのある事案をいう。）」を把握した場合に講ずべき対応等を定めた取扱規程を定めることを求めています。</p> <p>漏えい等の「おそれ」は、その時点で判明している事実関係からして、（漏えい等が発生した確証まではないものの、）漏えい等が発生したことが疑われる場合に認められます。例えば、個人データを格納しているサーバにおいて、外部からの不正アクセスによりデータが窃取された痕跡が認められた場合には、個人データの「漏えい」の「おそれ」が認められます。</p>
18	金融分野ガイドライン 第10条第3項①	<p>「個人データを取り扱う場所に赴く方法」に「（テレビ会議システム（映像と音声の送受信により相手の状態を相互に認識できる方法をいう。））を利用する方法を含む。以下同じ。）」を追記いただいておりますが、テレビ会議システム以外にも例えばWEB会議システム（ZoomやTeams等）についても「映像と音声の送受信により相手の状態を相互に認識できる方法」であれば該当すると認識しておりますが、その理解でよろしいでしょうか。</p> <p>上記の認識に相違ない場合、例えば、「（テレビ会議システム等（映像と音声の送受信により相手の状態を相互に認識できる方法をいう。））を利用する方法を含む。以下同じ。）」と「等」をつけていただくなど、解釈の明確化を図っていただけませんか。</p>	<p>「映像と音声の送受信により相手の状態を相互に認識できる方法」には、Web会議システムも含まれるという点は、御理解のとおりです。明確化のため、「テレビ会議システム等」に修正いたします。</p> <p>また、確認方法については、個別の事案ごとの判断となりますが、委託先から、委託先における安全管理に係る基本方針・取扱規定等を記載した書面の提出を受け、当該書面を確認することも「これに代わる合理的な方法」として認められるものと考えられます。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>また、「これに代わる合理的な方法による確認」とありますが、例えば、書面による確認を行なった上で、後日当該書面を参照できるよう保存するというような方法も許されるという理解でよろしいでしょうか。</p>	
19	金融分野ガイドライン 第10条第3項②	<p>同ガイドライン改正前は、「委託先に事前報告又は承認手続を求める、直接又は委託先を通じて定期的に監査を実施する等により、」と規定されていたところ、今回の改正で「かつ」という表現に改められた。</p> <p>この点について以下に記した、当方の理解で合っているか。</p> <p>&lt;当方の理解&gt;</p> <p>同ガイドライン改正前は、事業者は（１）「委託先に事前報告又は承認手続を求めること」と（２）「直接又は委託先を通じて定期的に監査を実施すること」のいずれも行うことは同ガイドライン上求められていなかった。しかし、今回の改正によって、（１）「委託先に事前報告又は承認手続を求めること」と「直接又は委託先を通じて定期的に監査を実施すること」のいずれも事業者は行うことが求められるようになった。</p>	<p>改正前の金融分野ガイドライン第10条第3項②は、「委託先に事前報告又は承認手続を求め」ること、並びに、「直接又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」及び「再委託先が個人情報保護法第23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」ことを要求していたところ、今回の改正では、これを分かりやすく示す観点から、表現を修正しております。改正前後で実質的な変更はありません。</p>
20	金融分野ガイドライン 第10条第3項②	<p>「漏えい等事案が発生した場合の委託先の責任」とありますが、漏えい等のおそれのある場合において、委託先にどのような責任を負わせるのが具体的に妥当であると考えていますでしょうか。</p> <p>また、委託先に漏えい等のおそれのある事案が発生し</p>	<p>前段について、例えば、委託契約において、委託先の講ずべき安全管理措置の内容を定め、これを遵守しなかった場合の委託先の損害賠償責任の規定を設けること等が考えられます。</p> <p>後段について、例えば、委託契約において、委託先</p>

No	該当条項	御意見	御意見に対する考え方
		<p>た際に、委託元である金融機関がそれを把握するためには、委託先から適切に報告をさせるための方策を別途考える必要があると思います。この具体的な方策について、貴庁として何か具体案がありますでしょうか。また、委託先に漏えい等のおそれのある事案が発生した際に、適切に報告がなされることを始めから期待せず、形式的に安全管理措置について契約に謳っていただければ良いものとお考えでしょうか。</p> <p>貴庁の見解をご教示ください。</p>	<p>は個人データの漏えい等事案が発生した場合には当該事案が生じた旨を速やかに委託元に通知する義務を負うといった規定を設けること等が考えられます。</p>
21	金融分野ガイドライン 第11条	<p>「個人データ」の漏えい等が発生した場合、従来は現行第17条および「金融機関における個人情報保護に関するQ&amp;A」（以下「Q&amp;A」という）問4-6により全件が義務的報告とされていたが、本改正以降は、金融機関についても、「個人データ」の漏えい等のうち一部の重大事案（個人情報保護法施行規則第7条列記事案）のみが義務的報告となると理解している。</p> <p>そのうえで、今後想定される「Q&amp;A」の改正に関連し、次の事項について確認させていただきたい。</p> <p>(1) 上記義務的報告となる事案以外の個人データの漏えい等事案は、引き続き義務的報告とされるのか、努力義務とされるのか、または報告対象外とされるのか。</p> <p>(2) 個人データに該当しない個人情報（および加工方法等情報）の漏えい等事案の当局報告については、</p>	<p>金融分野における個人情報取扱事業者は、個人情報保護法施行規則第7条各号に該当する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、個人情報保護法第26条第1項に基づき、（個人情報保護委員会から報告受理権限の委任を受けた）監督当局に報告をする義務を負います。また、個人である顧客等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、各業法に基づき、監督当局に報告をする義務を負います（金融分野ガイドライン第11条第1項）。</p> <p>加えて、金融分野における個人情報取扱事業者は、個人情報等の漏えい等が発生し、又は発生したおそれがある事態を知ったときは、監督当局に報告をする努力義務を負います（金融分野ガイドライン第11条第2項）。</p> <p>本意見募集は、金融分野ガイドライン及び実務指針</p>

No	該当条項	御意見	御意見に対する考え方
		<p>引き続き努力義務とされるのか、または報告対象外とされるのか。</p> <p>(3) 本改正を踏まえた「Q&amp;A」(漏えい等報告様式含む)の改正はいつ頃を予定しているか。また、パブリックコメントに付す予定はあるか。</p>	<p>の一部改正(案)の内容に関するものであるため、(3)に係る御意見は、本意見募集の対象外と考えます。</p>
22	金融分野ガイドライン 第11条	<p>個人データ等の漏えい等の報告について、報告の対象が「施行規則第7条各号関係に限る」とされた。</p> <p>現在は、「金融機関における個人情報保護に関するQ&amp;A」において、軽微なものについては四半期に一度まとめて報告できるとの考えが示されて、別紙様式として、その報告書の様式例が示されているが、ガイドライン改正後、この報告の方法は維持されるのか。</p> <p>(理由)</p> <p>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により、報告対象が限定されたことにより、従来の軽微報告が維持されるのかを確認したい。</p>	<p>個人情報保護法第26条第1項に基づく漏えい等報告(金融分野ガイドライン第11条第1項前段)については、通則ガイドライン3-5-3に従って行う必要があります。報告対象事態を知った後「速やかに」報告を行う必要があります。四半期に一回程度にまとめて報告を行うということは許容されません。</p> <p>各業法に基づく漏えい等報告(金融分野ガイドライン第11条第1項後段)及び金融分野ガイドラインに基づく漏えい等報告(金融分野ガイドライン第11条第2項。努力義務。)については、従前のおり、軽微な漏えい等事案については四半期に一回程度にまとめて御報告いただいで差し支えありません。</p>
23	金融分野ガイドライン 第11条	<p>「個人データ等の漏えい等の報告等」とあるが、現行の「ガイドライン」第17条では、個人情報保護法が規定する「個人データ」の漏えいに加えて、「個人情報」の漏えい報告まで求めている(同「Q&amp;A」の問4の6でも同旨)が、次項以下に述べる理由により、過重と思われるため、個人情報(個人データを構成しない個人情報)を含めず「個人データの漏えい等の報告等」として頂きたい。</p>	<p>個人情報等の漏えい等事案については、一般に、金融機関の取り扱う顧客情報は経済的価値が高く、漏えい等による不正利得のおそれ大きいことも踏まえ、漏えい等事案が発生した場合に金融機関が監督当局に漏えい等事案を漏れなく報告し、監督当局においてそれらを分析し原因への対処を行うことで、重大な漏えい等事案を未然に防ぐという観点で、努力義務として、監督当局への報告を求めることとします(金融分</p>

No	該当条項	御意見	御意見に対する考え方
		<p>個人情報保護法や、他の主要先進国の金融規制当局が求めている漏えい報告に比べて、金融分野における個人情報保護に関するガイドライン、同「Q&amp;A」が求める漏えい報告の対象範囲が広過ぎるため、過重な負担が生じている。今回の第11条では、「金融分野における個人情報取扱事業者は、施行規則第7条各号に定める事態を知ったときは、(中略)報告しなければならない。」と記載しているのであるから、報告義務が発生するのは、規則7条において規定されている「個人の権利利益を害するおそれ大きいもの」として定める4項目に限定して頂きたい。</p> <p>「Q&amp;A」は、今回のパブリックコメントに付されていないが、現行のQ&amp;Aの問4の5の4において、「個人データの漏えいとは個人データが外部に流出すること」と定義されている。上記の4項目に止まることなく漏えい報告の対象が広範に規定されているため、他の主要先進国における漏えい報告の範囲に比べて、日本の対象範囲が広過ぎる結果となっている。</p> <p>例えば、オーストラリアの金融監督当局 APRA の漏えい報告ルール CPS234 の section 35 においては、金融機関に課される報告義務は、ア material なインパクトを持つ漏えい、及び イ 海外の当局に報告した漏えい、と規定されている。</p> <p>このため、日本に拠点を持つオーストラリアの金融機関は、金融庁に報告した漏えい事案についても、全て</p>	<p>野ガイドライン第11条第2項。努力義務。)</p>



No	該当条項	御意見	御意見に対する考え方
		APRA に報告を行っているが、アに比較してイの事案が軽微なものが多いことが際立ってしまっている。	
24	金融分野ガイドライン 第 11 条	<p>「Q&amp;A」は、今回のパブリックコメントに付されていないが、Q&amp;A の問 4 の 5 の 4 に以下の記載がある。</p> <p>「個人データ」の「漏えい」とは「個人データが外部に流出すること」であり、たとえ流出した媒体において暗号化処理がされていたとしても、「個人データ」の「漏えい」に当たります。また、暗号化処理ではなく、パスワードが設定されている場合も同様です。なお、暗号化処理やパスワード設定がされていることは、「漏えい」後に公表や本人への通知等を行うべきか否かを判断する際の判断要素の一つになると考えられます。</p> <p>他方、平成 29 年の個人情報保護委員会告示第 1 号「個人データの漏えい等の事案が発生した場合等の対応について」では、以下のとおり規定されている。</p> <p>「実質的に個人データ又は加工方法等情報が外部に漏えいしていないと判断される場合には、例えば、次のような場合が該当する。</p> <p>漏えい等事案に係る個人データ又は加工方法等情報について高度な暗号化等の秘匿化がされている場合、</p> <p>漏えい等事案に係る個人データ又は加工方法等情報を第三者に閲覧されないうちに全てを回収した場合」</p>	本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。

No	該当条項	御意見	御意見に対する考え方
		<p>金融分野における「Q&amp;A」における漏えいの解釈の方が広い結果、社外流出した個人データを第三者に閲覧されないうちに全て回収した場合や、パスワードでプロテクトされた携帯電話スマートフォン等を紛失したがパスワードでプロテクトされていた又は遠隔操作で直ちにデータを消去した場合なども漏えい報告が求められることとなっている。</p> <p>保護委員会告示と同一の解釈を採用規定して頂きたい。</p>	
25	金融分野ガイドライン 第11条	<p>パブコメに付されていない「Q&amp;A」では、以下のよう に記載されている。</p> <p>「FAXの誤送信、郵便物等の誤送付及びメール誤送信などについては、個人情報取扱事業者が個別の事案ごとに、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性などを検討し直ちに報告を行う必要性が低いと判断したものであれば、業務上の手続きの簡素化を図る観点から、四半期に一回程度にまとめて報告しても差し支えありません」</p> <p>他方、「個人データの漏えい等の事案が発生した場合等の対応について」（平成29年個人情報保護委員会告示第1号）では、「FAX若しくはメールの誤送信、又は荷物の誤配等のうち軽微なもの」という軽微基準が示されており、これらは報告を要しないとされている。</p>	<p>本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>

No	該当条項	御意見	御意見に対する考え方
		委員会告示で採用されている軽微基準を「Q&A」でも採用して頂きたい。	
26	金融分野ガイドライン 第11条	漏えい等が発生した場合の個人情報保護委員会（実際には事業所管大臣）宛の「速報」「確報」の提出方法は、従来から運用している監督官庁宛の報告方法（Eメールでの押印無しファイル送付）でよいか。	令和4年4月1日以降、監督当局への漏えい等報告については、金融庁のホームページの電子申請・届出システムを利用して行ってください。なお、新システムの利用に必要なGビズIDの取得等への対応のため、従前経過措置として認められていた電子メールによる受付は令和4年3月31日をもって終了いたします。
27	金融分野ガイドライン 第11条	郵便局や宅配業者の誤配達による漏えい等が発生した場合には、「規則第7条」で定める「個人の権利利益を害するおそれが大きいもの」であっても、個人情報保護委員会（実際には事業所管大臣）宛の報告は不要にしていただけでないか。	<p>一般に、個人情報取扱事業者が配送事業者を利用して個人データを含むものを送る場合において、当該配送事業者の誤配達により、個人情報保護法施行規則第7条各号に定める個人データの漏えいが発生した場合には、当該個人情報取扱事業者の取り扱う個人データの漏えいが発生したものとして、当該個人情報取扱事業者が報告義務を負うこととなります。当該配送事業者の誤配達により漏えいが発生した場合であっても、報告義務を免れることにはなりません。</p> <p>なお、上記場合において、当該配送事業者は、通常、配送を依頼された中身の詳細については関知しないことから、当該配送事業者との間で特に中身の個人データの取扱いについて合意があった場合等を除き、当該個人データに関しては取扱いの委託をしているものではないものと解されます。このため、当該配送事業者の誤配達により報告対象となる個人データの漏えいが発生したときには、当該配送事業者ではなく、当</p>

No	該当条項	御意見	御意見に対する考え方
			<p>該配送事業者を利用した当該個人情報取扱事業者が報告義務を負うこととなります。</p>
28	<p>金融分野ガイドライン 第11条第1項</p>	<p>「施行規則第7条各号関係に限る」とし、「通則ガイドライン3-5-3に従って、個人情報保護委員会に報告しなければならない」とありますが個人情報保護委員会からの権限委任に基づき、対象となる個人データ性質にかかわらず、個人データの漏えい等の事案が発生した場合、個人情報保護委員会ではなく、監督当局に報告することになる、ということでしょうか。なお、従前の「金融機関における個人情報保護に関する」Q&amp;Aの問（参考）においては、金融機関自身の雇用管理情報、株主情報の漏えい事案等への対応については、金融ガイドラインの対象外として個人情報保護委員会への報告となっており、第11条第1項の対象となる情報についての整理を明らかにしていただきたい。</p> <p>法律施行規則第7条関係に該当しない漏えい事案についての報告についても、監督当局への報告が必要となる事案について具体的にお示しください。個人顧客に関する「個人データ」の漏えい等の事案で軽微なものは四半期報告で監督当局に報告すればよろしいでしょうか。</p>	<p>金融分野における個人情報取扱事業者は、個人情報保護法第26条第1項に基づき、同法施行規則第7条各号に該当する個人データの漏えい等事案について報告をする場合、（個人情報保護委員会より報告受理権限の委任を受けた）監督当局へ御報告いただくこととなります。詳細は、金融分野Q&amp;Aでお示しすることとします。</p> <p>また、金融分野における個人情報取扱事業者は、個人である顧客等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、各業法に基づき、監督当局に報告をする義務を負います（金融分野ガイドライン第11条第1項後段）。具体的には、例えば、個人である顧客の口座番号や預金残高の漏えい等事案が対象となります。</p> <p>なお、各業法に基づく漏えい等報告（金融分野ガイドライン第11条第1項後段）及び金融分野ガイドラインに基づく漏えい等報告（金融分野ガイドライン第11条第2項。努力義務。）について、例えば、FAXの誤送信、郵便物等の誤送付及び電子メール誤送信などについては、個別の事案ごとに、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性などを検討し直ちに報告を行う必要性が低いと判断したものであれば、業務上の手続の簡素化を</p>

No	該当条項	御意見	御意見に対する考え方
			<p>図る観点から、四半期に一回程度にまとめて報告いただいても差し支えありません。</p>
29	<p>金融分野ガイドライン 第11条第1項</p>	<p>「個人データ」の「漏えい、滅失、毀損」とは、どのようなものをさしますか。会社支給の携帯電話、ノートパソコン、PDA等は、会社管理のアプリケーションがインストールされ、2重認証により利用可能となります。ハード自体に個人データは掲載されず、会社のシステムにリモートでアクセスするようになっており、第三者がアクセスすることが困難な設定となっています。更に、デバイス紛失後は直ちにリモートですべての会社のシステムに係わるアプリケーションを完全削除することができます。このようなケースにおいて、デバイスの紛失は個人顧客の個人データ漏えいに当たりますか。</p>	<p>「漏えい、滅失、毀損」の定義については、通則ガイドライン3-5-1を御参照ください。</p> <p>個別の事案ごとの判断となりますが、ノートパソコン等の端末を社外で紛失した場合、たとえ当該端末に「個人データ」が記録されていなかったとしても、当該端末から個人データを格納しているサーバにアクセス可能な場合には、当該端末を紛失した時点で、個人データの「漏えい」が発生した「おそれ」が認められると考えられます。これは、当該端末にパスワード等を設定している場合も同様です。</p> <p>ただし、当該端末の紛失後に一定の措置を講じて、当該端末から個人データを閲覧することを不可能な状態にした場合において、閲覧不可能な状態とするまでの間に第三者が閲覧していないことがアクセスログ等から確認された場合には、「漏えい」に該当しないこととなります。</p>
30	<p>金融分野ガイドライン 第11条第1項</p>	<p>金融庁個人情報保護ガイドライン第11条第1項の「施行規則第7条各号に定める事態を知ったとき」には、同施行規則第7条第1号の「要配慮個人情報を含むデータの漏えい等が発生し、(中略)又はそのおそれがある事態」が含まれるが、同ガイドライン第5条に定める「機微(センシティブ)情報」は、個人情報保護法第2条第3項に定める要配慮個人情報の他、労働組合への</p>	<p>要配慮個人情報に該当しない機微(センシティブ)情報の漏えい等事案は、個人情報保護法施行規則第7条第1号には該当しません。ただし、同施行規則第7条第2号～第4号に該当する場合には、個人情報保護法第26条第1項に基づき、(個人情報保護委員会より報告受理権限の委任を受けた)監督当局に報告をする義務を負います(金融分野ガイドライン第11条第1</p>

No	該当条項	御意見	御意見に対する考え方
		<p>加盟、門地、本籍地、保健医療及び性生活に関する情報を含むと規定されているところ、これら、要配慮個人情報以外の機微（センシティブ）情報に含まれる情報について漏えい等又はそのおそれがある事態を知ったときは、個人情報保護委員会への報告は不要と読める。</p> <p>この場合、個人情報保護委員会への報告は不要でよい。また、個人情報保護委員会への報告は不要であるとした場合は、金融庁への報告も不要と考えてよい。</p>	<p>項前段)。</p> <p>また、要配慮個人情報や機微（センシティブ）情報を含むか否かにかかわらず、個人である顧客等に関する個人データの漏えい等事案が生じた場合には、各業法に基づき、監督当局に報告をする義務を負います（金融分野ガイドライン第11条第1項後段）。</p>
31	金融分野ガイドライン第11条第1項、第2項	<p>個人データ等の漏えい等の報告等について、改定前第17条では、「個人情報等の漏えい事案等・・・の事故が発生した場合には、監督当局等に直ちに報告することとする。」「個人情報等の漏えい事案等の事故が発生した場合には、当該事案等の対象となった本人に速やかに当該事案等の事実関係等の通知等を行うこととする。」とあったが、改定後の第11条では「施行規則第7条各号に定める事態を知ったときは・・・に報告しなければならない。」「施行規則第7条各号に定める事態を知ったときは・・・本人への通知等を行わなければならない。」とあることから、改定後は「個人情報等の漏えい事案等・・・の事故が発生した場合」から「施行規則第7条各号に定める事態を知ったとき」に限定されたという理解でよい。</p>	<p>改正前の金融分野ガイドライン第17条と改正後の金融分野ガイドライン第11条で、実質的な変更はありません。金融分野における個人情報取扱事業者は、一定の個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、漏えい等報告の義務を負い（金融分野ガイドライン第11条第1項）、また、個人情報等の漏えい等が発生し、又は発生したおそれがある事態を知ったときは、漏えい等報告の努力義務を負います（金融分野ガイドライン第11条第2項）。</p>
32	金融分野ガイドライン第11条第3項	<p>ガイドライン第11条第3項にある「漏えい等事案の内容等に応じて、・・・当該事案等の事実関係及び再発防止策等について、速やかに公表することとする。」という点について、「速やかに」とは、3～5日以内を</p>	<p>「速やかに公表する」について、具体的に公表を行う時点は、個別の事案において、二次被害の防止や類似事案の発生回避等の観点から、その時点で把握している事案の内容、公表を行うことで本人の権利利益が保護</p>

No	該当条項	御意見	御意見に対する考え方
		指すのでしょうか。 (具体的な期限となる日数の目安があるか。) もし、日数の目安がある場合には、いつの時点から起算するものかを示していただきたい。	される蓋然性、公表を行うことで生じる弊害等を勘案して判断する必要があります。
33	金融分野ガイドライン 第11条第3項	前段の「漏えい等事案が発覚した場合は、当該事態の内容等に応じて、次に掲げる事項について必要な措置を講じなければならない」とありますが、「漏えい等のおそれのある事案」が発覚した場合において、①事業所内部における報告及び被害の拡大防止、②事実関係の調査及び原因の究明、③影響範囲の特定、④再発防止策の検討及び実施のそれぞれについて、可能な範囲で必要な措置を取るという理解で良いでしょうか。 また、「漏えい等事案の内容等に応じて、二次被害の防止、類似事案の発生回避等の観点から、当該事案等の事実関係及び再発防止策等について、速やかに公表することとする。」とありますが、貴庁において公表が必要となると考える「漏えい等のおそれのある事案」について、何か目安等基準があれば、ご教示ください。	前段について、金融分野における個人情報取扱事業者は、本人の権利利益の保護の観点から、漏えい等事案の内容に応じて、①～④の各事項について、必要な措置を講じる必要があります。 後段について、金融分野における個人情報取扱事業者が取り扱う情報の性質等に鑑みれば、基本的には全ての漏えい等事案について速やかに公表することが望ましいと考えられます。 なお、例えば、インターネット上の掲示板等に漏えいした個人データがアップロードされており、金融分野における個人情報取扱事業者において当該掲示板等の管理者に削除を求める等、必要な初動対応が完了しておらず、事実関係等を公表することで、かえって被害が拡大することが想定される場合等においては、当該時点（必要な初動対応が完了していない時点）において公表を行う必要はないと考えられます。
34	金融分野ガイドライン 第11条第3項	第11条第3項が設けられた趣旨について教えていただきたい 第11条第3項について、改定前第17条第2項では、「早急に公表」とあったが、改定後は「速やかに公表」と変更された趣旨について教えていただきたい。	通則ガイドラインと表記を揃えたものであり、改正前後で実質的な変更はありません。

No	該当条項	御意見	御意見に対する考え方
35	金融分野ガイドライン 第11条第3項	<p>第2文の「また、」と「漏えい等事案の内容等に応じて」の間に、「施行規則第7条各号に定める事態を知ったときは、」との文言を追加するべきではないか。</p> <p>個人情報保護委員会等への報告、本人への通知、公表いずれも、義務の対象を、「施行規則第7条各号に定める事態を知ったとき」にあわせる必要があるのではないか。</p>	<p>金融分野ガイドライン第11条第4項後段について、金融分野ガイドライン第11条第1項又は第2項に規定する事態が生じた場合には、当該事態の内容等に応じて、当該事態の事実関係等を公表することが望ましいことから、原案で御理解いただけるものと考えます。</p>
36	金融分野ガイドライン 第12条	<p>改正前の第11条1の「第三者に提供される情報の内容」と「第三者に提供される個人データの項目」の関係性を明らかにしていただきたい。</p> <p>同じ意味で単なる言い換えをするための改正か、それとも、異なる意味を有しているのか。また、仮に異なる意味を有しているのであれば、どういう違いが改正前後の文言の間にあるかご教示いただきたい。</p> <p>[理由]</p> <ul style="list-style-type: none"> <li>概念的には、「情報」には、産業データや個人データではない個人情報も含まれる。また、個人データの内容は、(1)項目と(2)その項目の具体的情報が含まれる。</li> <li>そのため、今回の改正で文言が変わったことにより、本人から同意を得る際に得るべき情報は、減ったように読むのが自然である。しかし、改正法の趣旨にかんがみると本人からの同意取得時に提供すべき情報が減ったという解釈はやや違和感がある。そこで、上記の[意見]の点について伺いたい次第です。</li> </ul>	<p>改正前の金融分野ガイドライン第11条第1項の「第三者に提供される情報の内容」は、第三者に提供される個人データの項目を意味するものであったところ、今回の改正では、これを分かりやすく示す観点から、「第三者に提供される個人データの項目」と表現を修正しております。改正前後で実質的な変更はありません。</p>



No	該当条項	御意見	御意見に対する考え方
37	金融分野ガイドライン 第 12 条	「個人データの提供先の第三者」に代わる本人に参考となるべき情報の記載方法は、本人が金融機関のウェブサイトなどで当該金融機関のグループ会社や提携先を把握することができるのであれば、例えば「当社のグループ会社」、「当社の提携先」といった記載でもよいか。	<p>本人の同意を得ようとする時点において、個人データの提供先の第三者が特定できない場合には、個人データの提供先の第三者に代わる本人に参考となるべき情報を本人に認識させた上で同意を得ることとされています。当該参考となるべき情報としては、提供先の第三者の範囲や属性に関する情報が考えられます。</p> <p>個別の事案ごとの判断となりますが、金融機関が、ウェブサイトなどにおいて、合理的かつ適切な方法で当該金融機関のグループ会社や提携先を示すことにより、本人がこれを把握することができるのであれば、「当社のグループ会社」、「当社の提携先」といった情報を本人に認識させた上で同意を取得することでも可能であると考えられます。</p>
38	金融分野ガイドライン 第 12 条第 1 項	点線囲み部分の「本人の同意を得ようとする時点において、①に掲げる事項が特定できない場合」について、具体例をお持ちでしたらご教授ください。	<p>個別の事案ごとの判断となりますが、例えば、保険会社が保険引受リスクの分散等の観点から再保険会社に再保険を行う場合において、保険会社による顧客からの保険引受及び同意取得の時点では、最終的にどの再保険会社に再保険を行うかが未確定であり、当該顧客の個人データの提供先を特定できない場合が考えられます。</p>
39	金融分野ガイドライン 第 13 条	日本の保険会社 A が、外国にあるグループ会社の再保険会社から、再保険にかかる業務の代理又は事務の代行を引き受け、行っている場合、当該外国の再保険会社の代理人として、日本の保険会社 B から保険契約者の個人データを受領し、当該外国の再保険会社に提供すること	<p>保険会社 A が外国にある再保険会社に個人データを提供する場合、原則として、保険会社 A において、個人情報保護法第 28 条に基づき必要な情報を提供した上で、本人の同意を取得する必要があります。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>が考えられる。この場合、日本の保険会社 B が、保険契約者から、当該外国の再保険会社への個人データの提供を認める旨の同意を得ているのであれば、日本の保険会社 A は、改めて、保険契約者から、当該外国の再保険会社への個人データの提供を認める旨の同意を得る必要はないことを確認したい。</p> <p><b>【理由】</b>            解釈の明確化のため。保険契約者にとって、既に同意したことであり、改めて同意を取得しないとしても、不利益は発生しない。また、保険会社 A が、保険契約者から同意を取得することは実務的に困難であり、煩雑な手続となる。</p>	<p>もっとも、個別の事案ごとの判断となりますが、御指摘のような事案においては、保険会社 B が、保険会社 A に代わって、本人に対して同条に基づき必要な情報を提供し、保険会社 A の氏名・名称等を明示した上で、保険会社 A の再保険会社への個人データの提供に係る同意を取得することも認められると考えられます。なお、この場合、保険会社 B 及び保険会社 A の双方が、保険会社 B が保険会社 A に代わって本人の同意を取得する旨を認識している必要があります。</p>
40	金融分野ガイドライン 第 13 条	<p>第 13 条外国にある第三者への提供の制限（法第 28 条関係）の前提として、法第 28 条 1 項の同意が必要となるか否かについて、金融機関はすべての委託先、提携先等に対して調査をする必要はあるか、という点について伺います。例えば、個人データの移転が予定される業務委託の委託先その他、ビジネス・マッチング契約による提携先や投資信託の販売会社の立場から受託会社（信託銀行）等について、個人データを管理するデータサーバがすべて国内に設置されているか、一部またはすべてが外国に設置されているかについて調査する等をして、同意の要否を把握する必要はありますか。あるいは、国内に所在する個人情報取扱事業者であれば、法第 28 条 1 項</p>	<p>個人情報取扱事業者は、外国にある第三者に個人データを提供する場合（ただし、我が国と同等の水準にあると認められる外国にある第三者若しくは基準適合体制を整備している者に提供する場合、又は個人情報保護法第 28 条第 1 項で準用する同法第 27 条第 1 項各号に該当する場合を除く。）、同法第 28 条第 2 項に基づく情報提供を行った上で同条第 1 項に基づく同意を取得する必要があります。これは当該第三者が管理・運営するサーバが国内にある場合でも同様です。</p> <p>なお、個人情報取扱事業者が、外国にある第三者に個人データの取扱いを委託する場合や外国にある支店・営業所に個人データを取り扱わせる場合等、外国</p>

No	該当条項	御意見	御意見に対する考え方
		<p>に関するような事実はないものと推定し、法第 28 条 1 項の同意が必要となる事実について端緒が掴めたときに、初めて調査を行うという対応で差し支えはないでしょうか。</p> <p>仮に、調査をし、当該同意の要否に関して把握することが必要であるとする場合、金融機関がすべてを調査するには相当の負荷がかかりますし、令和 4 年 4 月 1 日の法施行までに終わらせることは困難です。この場合において、個人情報取扱事業者は、個人データを保管するデータサーバが一部またはすべてが外国に設置されている等、法第 28 条 1 項の同意が必要となるような事実があれば自ら公表をするという規制とした方が、個別に問い合わせをする手間がなくなる点で当該調査の負荷が軽減されることにはなるものと思われま。金融機関にかかる負荷に関して、貴庁の見解をご教示ください。</p>	<p>において個人データを取り扱う場合には、事業の規模及び性質、個人データの取扱状況（取り扱う個人データの性質及び量を含む。）、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て、当該第三者が所在する国のほか、当該個人データが保存されるサーバの所在国の個人情報の保護に関する制度等を把握した上で、安全管理措置を講じるとともに、個人情報保護法第 32 条第 1 項第 4 号に基づき、当該措置を本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置く必要があります。</p>
41	金融分野ガイドライン 第 13 条	<p>第 13 条外国にある第三者への提供の制限（法第 28 条関係）の前提として、外国送金について（預金取扱金融機関の他にも資金移動業、仮想通貨交換業を含むものと思われまが）、法第 28 条 1 項に該当するものと整理された場合、令和 4 年 4 月 1 日の法施行までに対応することはおそらく困難です。外国の個人情報保護法制の有無、その内容について個別の金融機関が個々に調査するにも限界があります。</p> <p>令和 4 年 1 月 11 日付金融審議会「資金決済ワーキング・グループ」報告における AML/CFT 業務の共同化の議</p>	<p>個別の事案ごとの判断となりますが、一般論として、本人の同意を事前に取得して外国にある第三者に個人データを提供する場合、提供元の個人情報取扱事業者は、原則として、改正後の個人情報保護法施行規則第 17 条第 2 項に基づき、当該外国の名称や適切かつ合理的な方法により得られた当該外国における個人情報の保護に関する制度に関する情報等を本人に提供する必要があります。</p> <p>なお、個人情報保護委員会では、一定の国又は地域における個人情報の保護に関する制度について調査</p>

No	該当条項	御意見	御意見に対する考え方
		<p>論のように、例えば、個人情報保護委員会や預金保険機構等適切な機関がすべての国・地域の個人情報保護法制の有無、その内容について調査、公表し、定期的に更新を続け、個人情報取扱事業者がその結果を利用するという方式が合理的かと思いますが、外国送金業務が滞るおそれを含め、貴庁の見解をご教示ください。</p>	<p>し、我が国の個人情報保護法との間の本質的な差異の把握に資する一定の情報を公表しています。個人情報保護法第 28 条第 2 項の趣旨には、外国にある第三者に対する個人データの提供に伴うリスクについて、本人の予見可能性を高めるという点のほか、外国にある第三者に対して個人データを提供する個人情報取扱事業者においても、従前以上に、提供先の外国にある第三者における事業環境等を認識することを促すという点が含まれます。また、個人情報取扱事業者が同項に基づいて本人に対して提供すべき情報の具体的内容は、個別の事案に応じて異なり得ます。したがって、外国における個人情報の保護に関する制度に関する情報の確認は、外国にある第三者に対して個人データを提供する個人情報取扱事業者の責任において行うべきものであり、当委員会が提供する上記参考情報は、あくまで補助的なものとして参照する必要があります。</p>
42	<p>金融分野ガイドライン 第 13 条第 1 項</p>	<p>第 13 条で、「外国にある第三者への提供に関する条項が他の個人情報の取扱いに関する条項等と明確に区別され、本人に理解されることが望ましい。」とある部分についての質問です。</p> <p>インターネットで同意を得る場合については、「個人情報の取扱いに関する方針」（又は、プライバシーポリシー等、名称は各社により異なる。）の条項について一体として、クリックによる同意を得て、その条項の中で、「外国</p>	<p>金融分野ガイドライン第 13 条第 1 項では、外国にある第三者への個人データの提供に関する本人の同意を得るにあたり、あらかじめ作成された同意書面を用いる場合には、外国にある第三者への提供に関する条項が他の個人情報の取扱いに関する条項等と明確に区別され、本人に理解されることが望ましいとしています。</p> <p>御指摘のインターネットで本人の同意を得る場合について、外国にある第三者への提供に関する条項を他</p>

No	該当条項	御意見	御意見に対する考え方
		<p>にある第三者への提供に係る条項」が目立つようになっていけば足りるという趣旨かお伺いしたいです。</p>	<p>の個人情報の取扱いに関する条項等と明確に区別するという観点からは、個人情報保護宣言の中に記載されている外国にある第三者への提供に関する条項を目立たせるだけではなく、他の個人情報の取扱いに関する条項とチェックボックスを分けること等が望ましいと考えます。</p>
43	<p>金融分野ガイドライン 第13条第1項</p>	<p>金融分野における個人情報保護に関するガイドライン第13条第1項で、あらかじめ作成された同意書面を用いる場合の望ましい対応として、「文字の大きさ及び文章の表現を変えること等により」とありますが、具体例をお示しいただけないでしょうか。例えば、色を変えたり、下線を引くといったことをご想定でしょうか。</p>	<p>金融分野ガイドライン第13条第1項では、外国にある第三者への個人データの提供に関する本人の同意を得るにあたり、あらかじめ作成された同意書面を用いる場合には、外国にある第三者への提供に関する条項が他の個人情報の取扱いに関する条項等と明確に区別され、本人に理解されることが望ましいとしています。</p> <p>このための具体的な工夫としては、例えば、文字の大きさや色、フォント等を変えるほか、下線を引くことが考えられます。また、Web ページで本人の同意を得る場合、外国にある第三者への提供に関する条項を他の個人情報の取扱いに関する条項等と明確に区別するという観点からは、他の個人情報の取扱いに関する条項とチェックボックスを分けること等が望ましいと考えます。</p>
44	<p>金融分野ガイドライン 第13条第1項</p>	<p>第1項において、個人情報保護法施行規則第17条第2項から第4項までの規定により情報提供が求められる事項に加えて、「1個人データの提供先の第三者」についての情報提供が求められている。</p>	<p>金融分野ガイドライン第12条第1項及び第13条第1項では、本人が同意の可否を適切に判断できるようにする観点から、第三者への個人データの提供に関する本人の同意を得る際は、「個人データの提供先の第</p>

No	該当条項	御意見	御意見に対する考え方
		<p>個人情報取扱事業者自身の企業秘密保持の観点や、当該第三者との間の守秘義務契約の観点により、1に掲げる事項を特定できているもの、開示が困難な場合がありうる。</p> <p>このような場合には、「1に掲げる事項が特定できない場合」と同様の対応で差し支えないか（2、3については、本人に認識させた上で同意を得ることとする）</p> <p>このため、記載を以下のように修文して頂きたい。</p> <p>「本人の同意を得ようとする時点において、1に掲げる事項が特定できない場合、または、1に掲げる事項を開示することが困難な場合には、1に掲げる事項に代わる本人に参考となるべき情報を当該本人に認識させた上で同意を得ることとする。」</p>	<p>三者」等を本人に認識させた上で、同意を得ることとしています。</p> <p>個別の事案ごとの判断となりますが、金融分野における個人情報取扱事業者が当該第三者との間に守秘義務契約を締結しており、秘密情報の保護につき、本人が事業者間での個人データの流通を把握する必要性を上回る特別な事情がある場合として、当該第三者の会社名等を本人に提供することにより、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は、「個人データの提供先の第三者」の代わりに、当該第三者の範囲や属性に関する情報など、本人に参考となるべき情報を本人に認識させた上で、同意を得ることが望ましいと考えます。</p>
45	金融分野ガイドライン 第13条第1項	<p>法第28条では、外国第三者提供の同意を得ようとする場合には、予め施行規則第17条2項から4項までに定められた「情報提供」をすることが義務付けられている。他方で、本ガイドライン第13条1項によれば、前記の情報提供について、同意書面の中に記載の上で同意を得ることが（法令上は必ずしも求められてはいない追加的な措置として）定められていると理解している（努力義務）。以下の場合についてご教示いただきたい。</p> <p>①法令上の情報提供の方法としては、「「個人情報の保護に関する法律についてのガイドライン」に関するQ&amp;A」のQ12-10及びA12-10にあるように、必要な情報が掲載されたウェブサイトのURLを本人に提供する</p>	<p>① 個別の事案ごとの判断となりますが、例えば、外国にある第三者への個人データの提供に関する本人の同意を得る際に、必要な情報が掲載された自社のWebページのURLを紙媒体の同意書面に掲載し、当該Webページに掲載された情報を本人に閲覧させる方法も、個人情報保護法施行規則第17条第1項における「適切な方法」に該当します。ただし、この場合であっても、例えば、当該URLを同意書面の本人にとって分かりやすい場所に掲載するほか、紙媒体の同意書面を用いる場合には当該URLの近くにQRコードを掲載すること等により、同意可否の判断の前提として、本人に対して当該情報の確認を明示的</p>

No	該当条項	御意見	御意見に対する考え方
		<p>ことも一定範囲で認められていると理解しているが、本ガイドライン第13条1項も踏まえて考えた場合、金融分野における個人情報取扱事業者としては、例えば、紙の同意書面（同意書面と一体と評価できる書面を含む）に必要な情報が記載されたウェブサイトのURLを分かりやすい形で記載するなどした上で同意を得るということであれば、努力義務を果たしていると考えてよいか。また、電話録音の場合には、URLを口頭で伝達することになるが、この場合でも、適切にアクセスが可能になるように伝達しておくことであれば、努力義務を果たしていると考えてよいか。</p> <p>②情報提供項目の一つである法第17条2項2号の事由については、個人情報保護委員会においても、事業者の参考となる一定の情報を取りまとめて公表される予定と理解しているが、①の同意書面（または当該同意書面に記載されたウェブサイトのURL先）に、当該個人情報保護委員会の公表するウェブサイトのURLを記載した上で、同意を得るという方法も認められるか。</p>	<p>に求めるなど、本人が当該情報を閲覧すると合理的に考えられる形で情報提供を行う必要があると考えられます。</p> <p>他方、当該URLを本人に口頭で伝達することのみでは、「適切な方法」とは認められません。</p> <p>② 個人情報保護法第28条第2項の趣旨には、外国にある第三者に対する個人データの提供に伴うリスクについて、本人の予見可能性を高めるという点のほか、外国にある第三者に対して個人データを提供する個人情報取扱事業者においても、従前以上に、提供先の外国にある第三者における事業環境等を認識することを促すという点が含まれます。また、個人情報取扱事業者が同項に基づいて本人に対して提供すべき情報の具体的内容は、個別の事案に応じて異なり得ます。したがって、個人情報保護法施行規則第17条第2項第2号に基づく「適切かつ合理的な方法」による確認は、外国にある第三者に対して個人データを提供する個人情報取扱事業者の責任において行うべきものであり、個人情報保護委員会が提供する情報は、あくまで補助的なものとして参照する必要があります。</p> <p>個別の事案ごとの判断となりますが、当該事業者が当該外国における個人情報の保護に関する制度に関する情報について一般的な注意力をもって適切か</p>

No	該当条項	御意見	御意見に対する考え方
			<p>つ合理的な方法により確認を尽くした結果、当該事業者として本人に提供すべき情報が、上記のとおり個人情報保護委員会が補助的なものとして提供する情報（以下「委員会提供情報」といいます。）と同じであった場合には、当該委員会提供情報を個人情報保護法施行規則第 17 条第 2 項 2 号の「適切かつ合理的な方法」により得られた情報として本人に提供することは考えられます。なお、当該事業者が、当該委員会提供情報以外にも同施行規則第 17 条第 2 項に基づいて本人に対して提供すべき情報を保有している場合には、当該情報も本人に対して提供する必要があります。</p> <p>また、その場合、当該事業者は、当該委員会提供情報の掲載された Web ページの URL を自社のホームページに掲載し、当該 URL の指定する Web ページに掲載された情報を本人に閲覧させる方法も、同施行規則第 17 条第 1 項における「適切な方法」に該当すると考えられます。ただし、この場合であっても、例えば、当該 URL を同意書面の本人にとって分かりやすい場所に掲載するほか、紙媒体の同意書面を用いる場合には当該 URL の近くに QR コードを掲載すること等により、同意の可否の判断の前提として、本人に対して当該情報の確認を明示的に求めるなど、本人が当該 URL の指定する Web ページに掲載された情報を閲覧すると合理的に考えられる形で、情報提</p>



No	該当条項	御意見	御意見に対する考え方
			供を行う必要があると考えられます。
46	金融分野ガイドライン 第13条第2項	<p>「金融分野における個人情報取扱事業者は、事後的に提供先の第三者を特定できた場合は、遅滞なく、・・・情報を提供することとする。」に変更すべきと考える。</p> <p>[理由]</p> <ul style="list-style-type: none"> <li>・まず、本来的に、個人情報取扱事業者は、提供先の第三者に関する情報を本人に提供すべきであるところ、上記の文言の箇所は、かかる提供を猶予されているという状況を想定している。本人に対する説明義務及び透明性の観点、並びに金融機関が有する個人情報が本人もたらす影響の大きさから鑑みると、「提供先の第三者が特定できた場合は、本人の求め」を待つまでもなく、事業者は自ら自発的に情報を提供すべきである。</li> <li>・実際、金融分野における個人情報取扱事業者が「提供先の第三者が特定できた」かどうかを本人は知りようがない以上、そもそも「本人は求め」を当該事業者に対して行うきっかけが得られない。ゆえに、「本人の求めに応じて」という文言を挿入することは、事業者の情報提供義務を死文化させることにつながる懸念が大きい。</li> <li>・そして、金融機関の管理部門（法務部、コンプライアンス部等）が一般の事業会社に比べて充実していることを踏まえると、金融機関であれば特段の負担なく対</li> </ul>	<p>個人情報取扱事業者は、外国にある第三者への個人データの提供時に、原則として個人情報保護法第28条第2項、同法施行規則第17条第2項に基づく情報提供を行うことが求められます。もともと、同施行規則第17条第2項第1号又は第3号に定めるいずれかの事項が特定できない場合には、例外的な対応として、それぞれ同施行規則第17条第3項又は第4項に基づく情報提供（提供先が定まる前に、本人の同意を得る必要性を含みます。）を求めています。</p> <p>御指摘の状況は、そのような例外的な場合であって、さらに事後的に同施行規則第17条第2項各号に定める事項の情報提供が可能となった場合に、情報提供することを努力義務として定めているものであり、一般的に現状の案で御理解いただけるものと考えています。頂いた御意見は、今後の執務の参考といたします。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>応じうると考えられ、金融機関における個人情報取扱事業者以外とは異なる取扱いを金融機関における個人情報取扱事業者に求めたとしても、過度な負担を課すことにはならないと考える。</p> <ul style="list-style-type: none"> <li>・そのため、金融機関が有する個人情報が本人もたらず影響の大きさに伴う情報提供の必要性に基づき、金融機関における個人情報取扱事業者以外とは異なる取扱いを金融機関における個人情報取扱事業者に本ガイドラインに求めるべきと思料する。</li> </ul>	
47	金融分野ガイドライン 第13条第2項	<p>第13条第2項について、「第20条に定める「個人情報保護宣言」と一体としてインターネットのホームページへの常時掲載又は事務所の窓口等での掲示・備付け等により、公表することとする。」ことが追加された。当該公表義務は「本人の同意を得ようとする時点において、個人データの提供先の第三者が所在する外国が特定できない場合」がある場合に限定され、外国にある第三者への個人データの提供を行わない場合や、外国にある第三者への個人データの提供を行う場合であっても、「本人の同意を得ようとする時点において、個人データの提供先の第三者が所在する外国が特定できない場合」がない場合には、上記の公表は不要という理解でよいか。</p>	<p>金融分野ガイドライン第13条では、提供先の第三者が所在する外国が特定できない場合（第2項）と提供先の外国にある第三者が基準適合体制を整備していることを根拠として当該第三者に個人データを提供した場合（第3項）において、金融分野における個人情報取扱事業者は、本人が事後的に情報提供の求めが可能である旨を自社のホームページ等への常時掲載等により公表することとして、努力義務として定めています。</p> <p>このため、外国にある第三者に個人データを提供しない場合や、本人の同意を得る際に、個人情報保護法施行規則第17条の規定に従って、提供先の第三者が所在する外国の名称や当該外国における個人情報の保護に関する制度に関する情報等の情報提供を行っている場合は、本人が事後的に情報提供の求めが可能である旨を公表する必要はありません。</p>

No	該当条項	御意見	御意見に対する考え方
48	金融分野ガイドライン 第 13 条第 2 項	<p>13 条 2 項第 2 段落では、「このような情報提供の求めが可能である旨を前項に定める書面における記載を通じて本人に認識させる」とされており、「前項に定める書面」（越境移転に関する同意を取得する書面）に 13 条 2 項第 2 段落記載の情報提供の求めが可能であることを記載するよう求めているように読めます。</p> <p>この点について、「前項に定める書面」（越境移転に関する同意を取得する書面）に、個人情報保護宣言（この個人情報保護宣言には、上記情報提供の求めが可能である旨が記載）が掲載された URL を記載し、その URL を閲覧することを本人に求めている場合には、「前項に定める書面」（越境移転に関する同意を取得する書面）には、13 条 2 項第 2 段落記載の情報提供の求めが可能であることを記載しなくても、差し支えないという理解でよろしいでしょうか。</p>	<p>提供先の第三者が所在する外国が特定できない場合（金融分野ガイドライン第 13 条第 2 項）において、金融分野における個人情報取扱事業者は本人が事後的に情報提供の求めが可能である旨を同意書面における記載を通じて本人に認識させるとともに、個人情報保護宣言に記載の上自社のホームページ等への常時掲載等により公表することとしています。</p> <p>個別の事案ごとの判断となりますが、個人情報保護宣言の中に本人が事後的に情報提供の求めが可能である旨を明記するとともに、外国にある第三者への個人データの提供に関する本人の同意を得るための書面に個人情報保護宣言の Web ページの URL を掲載することで、当該情報を本人に閲覧させる方法も、「前項に定める書面における記載を通じて本人に認識させる」方法の一つとして認められるものと考えられます。</p> <p>この場合であっても、例えば、当該 URL を同意書面の本人にとって分かりやすい位置に掲載するとともに、紙媒体の同意書面を用いる場合には当該 URL の近くに QR コードを掲載する等により、本人に対して事後的に情報提供の求めが可能である旨の確認を明示的に求めるなど、本人が当該情報を容易に閲覧できるような工夫が望まれます。</p>
49	金融分野ガイドライン 第 13 条第 2 項	<p>外国にある第三者への第三者提供に関し、個人情報取扱事業者が、「同意取得時に個人データの提供先の第三者が所在する外国が特定をできない場合には、外国にある</p>	<p>金融分野ガイドライン第 13 条第 2 項及び第 3 項は、金融分野における個人情報取扱事業者は、①提供先の第三者が所在する外国が特定できない状態で本人</p>

No	該当条項	御意見	御意見に対する考え方
		<p>第三者への個人データの第三者提供は行わない」という運用する場合には、金融分野ガイドライン第13条第2項に記載の「事後的に提供先の第三者を特定できた場合」の情報提供の求めが可能である旨に関する公表等については不要との理解でよいか。</p>	<p>の同意を根拠として第三者に個人データを提供した場合（同条第2項）、及び、②提供先の外国にある第三者が基準適合体制を整備していることを根拠として当該第三者に個人データを提供した場合（同条第3項）には、本人が事後的に情報提供の求めが可能である旨をホームページへの常時掲載等により公表することとする、との努力義務を課しています。</p> <p>御指摘の事案は個別の判断になりますが、提供先の第三者が所在する外国を特定できない場合に、外国にある第三者への個人データの提供を行わないのであれば、金融分野ガイドライン第13条第2項に基づき、本人が事後的に情報提供の求めが可能である旨を公表する必要はないと考えられます。</p> <p>ただし、この場合であっても、提供先の外国にある第三者が基準適合体制を整備していることを根拠として当該第三者に個人データを提供する場合は、同条第3項に基づき、本人が事後的に情報提供の求めが可能である旨を公表する努力義務を負います。</p>
50	金融分野ガイドライン第13条第2項	<p>2で「個人データの提供先の第三者が所在する外国が特定できない場合には、特定できない旨及びその具体的な理由（提供先が定まる前に本人同意を得る必要性を含む。）を情報提供するとともに、外国の名称に代わる本人に参考となるべき情報の提供が可能である場合には、当該情報を提供しなければならない。」とあるが、この場合の情報提供は、顧客に自社のウェブサイト等の掲載場所</p>	<p>個別の事案ごとの判断となりますが、外国にある第三者への個人データの提供に関する本人の同意を得る際に必要な情報を自社のホームページに掲載した上で、その掲載箇所のWebページのURLを書面に掲載することで、当該情報を本人に閲覧させる方法も、適切な情報提供の方法の一つとして認められるものと考えられます。</p>

No	該当条項	御意見	御意見に対する考え方
		を案内し、当該ウェブサイトにおいて必要な情報を記載することで上記の要件を満たすと考えてよいか。なお、上記情報を記載したリーフレット等の書面を交付する方法も考えられるが、記載する情報の内容（想定される第三者提供の対象となる国等の範囲等）は変化することも考えられるため、情報更新が比較的容易なウェブサイトへの掲載が合理的であると考えます。	ただし、この場合であっても、例えば、当該 URL を本人にとって分かりやすい位置に掲載した上で、同意の可否の判断の前提として、本人に対して当該情報が掲載された Web ページの確認を明示的に求めるなど、本人が当該情報を閲覧すると合理的に考えられる形で情報提供を行う必要があります。
51	金融分野ガイドライン 第 13 条第 2 項	第 2 段落冒頭の「事後的に提供先の第三者を特定できた場合」とされているが、「事後的に提供先の第三者が所在する外国を特定できた場合」ではないか確認したい。	御意見を踏まえ、提供先の第三者が所在する外国を特定できた場合と提供先の第三者が講ずる個人情報の保護のための措置についての情報提供が可能となった場合とを区別して、それぞれの情報提供について明確となるよう修正いたします。
52	金融分野ガイドライン 第 13 条第 2 項	事後的に提供先の所在する外国を特定できた場合、本人の求めに応じて、施行規則第 17 条第 2 項各号に定める情報を提供する必要があるが、当該情報提供方法は、書面によらない方法も認められるという理解でよいか。	事後的に提供先の第三者が所在する外国が特定できた場合の情報提供も、電磁的記録の提供による方法、書面の交付による方法その他の適切な方法で提供することが認められます。
53	金融分野ガイドライン 第 13 条第 3 項	ガイドライン第 13 条第 3 項にある「その後、当該第三者に個人データを提供した場合に施行規則第 18 条第 1 項第 1 号の規定により当該第三者による相当措置の実施状況を確認する際には、個人データを取り扱う場所に赴く方法又は書面による報告を受ける方法により確認を行うこととする。これらの方法は、外国にある第三者に提供する個人データ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」という点について、	相当措置の実施状況の定期的な確認とは、例えば、次のようなことをいいます。 ①外国にある事業者個人データの取扱いを委託するケース 提供元及び提供先間の契約を締結することにより、当該提供先の基準適合体制を整備している場合は、当該契約の履行状況を確認すること ②同一の企業グループ内で個人データを移転するケース

No	該当条項	御意見	御意見に対する考え方
		<p>たとえば外国にあるクラウドサービス事業者のサービスを利用する場合などで、取扱場所に赴くことができず、個別の調査書面への回答を得られない場合、当該事業者のホワイトペーパーやプライバシーポリシーなどの公表事項をもとに相当措置の実施状況を判断することが認められるかをご教示いただきたい。</p>	<p>提供元及び提供先に共通して適用されるプライバシーポリシーにより、当該提供先の基準適合体制を整備している場合は、当該プライバシーポリシーの履行状況を確認すること</p> <p>確認の方法としては、「赴く方法」（「テレビ会議システム等（映像と音声の送受信により相手の状態を相互に認識できる方法をいう。）を利用する方法」を含む。金融分野ガイドライン第10条第3項①参照。）又は書面により報告を受ける方法によって行うこととされています。御指摘の事案は個別の判断になりますが、当該第三者からホワイトペーパー等の形で回答を受け、それを参照することにより、当該第三者による相当措置の実施状況を確認できる場合も「書面により報告を受ける方法」の一つとして認められるものと考えられます。</p>
54	金融分野ガイドライン 第13条第3項	<p>第13条第3項について、「法第28条第3項及び施行規則第18条に基づき、本人の求めに応じて事後的に情報を提供する旨を第20条に定める「個人情報保護宣言」と一体としてインターネットのホームページへの常時掲載又は事務所の窓口等での掲示・備付け等により、公表することとする。」ことが追加された。個人データの外国にある第三者（法第28条第1項に規定する体制を整備している者に限る）への提供を行わない場合には、上記の公表は不要という理解でよいか。</p>	<p>金融分野ガイドライン第13条第2項及び第3項は、金融分野における個人情報取扱事業者は、①提供先の第三者が所在する外国が特定できない状態で本人の同意を根拠として当該第三者に個人データを提供した場合（同条第2項）、及び、②提供先の外国にある第三者が基準適合体制を整備していることを根拠として当該第三者に個人データを提供した場合（同条第3項）には、本人が事後的に情報提供の求めが可能である旨をホームページへの常時掲載等により公表することとする、との努力義務を課しています。</p>

No	該当条項	御意見	御意見に対する考え方
			<p>御指摘の事案は個別の判断になりますが、提供先の外国にある第三者が基準適合体制を整備していることを根拠として当該第三者に個人データの提供を行わない場合は、金融分野ガイドライン第13条第3項に基づき、本人が事後的に情報提供の求めが可能である旨を公表する必要はないと考えられます。</p> <p>ただし、この場合であっても、提供先の第三者が所在する外国が特定できない状態で本人の同意に基づき個人データを提供する場合には、同条第2項に基づき、本人が事後的に情報提供の求めが可能である旨を公表する努力義務を負います。</p> <p>なお、御指摘の金融分野ガイドライン第13条第3項の記載は、本意見募集の意見を踏まえて修正を行います。</p>
55	金融分野ガイドライン第13条第3項	<p>「相当措置の実施状況を確認する際には、個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法により確認を行うこととする。」としています。「リスクに応じた」ものとされています。</p> <p>提供先がグループ間のエンティティの場合であって、グループ間において相当措置の要件を満たす共通のポリシーを遵守している場合は、当該ポリシーの遵守の実施状況を各国の個人情報保護法のコンプライアンス担当者電子メールで確認する方法で宜しいでしょうか。また、提供先が外部のベンダーである場合、現地のグループ企</p>	<p>相当措置の実施状況は、外国にある第三者に提供する個人データの内容や規模に応じて適切かつ合理的な方法によって確認される必要があります。</p> <p>御指摘の事案は個別の判断になりますが、提供先である同一グループ内の別法人にも共通して適用されるポリシーにより当該提供先の基準適合体制を整備している場合には、当該ポリシーの履行状況（履行に問題が生じた場合の当該問題の内容やそれに対して講じた対応策等を含む。）を、当該別法人の所在する外国に係るコンプライアンス担当者に対して電子メールで確認することや、現地のグループ企業が提供先の第三者</p>

No	該当条項	御意見	御意見に対する考え方
		業担当の者がベンダーを訪問し、訪問記録が共有されていけばよいでしょうか。	を訪問して契約等の履行状況等を確認し、当該グループ企業から書面により相当措置の実施状況の共有を受けて確認することも、「適切かつ合理的な方法」の一つとして認められるものと考えられます。
56	金融分野ガイドライン 第13条第3項	基準適合体制を整備していることを根拠として外国にある第三者に個人データを提供する際、提供時点で、当該第三者による相当措置の実施に影響を及ぼすおそれのある当該外国の制度がある場合、「当該第三者による相当措置の継続的な実施の確保」の可否の確認をすることとされているが、「相当措置の継続的な実施の確保」に係る具体的に求められる対応事項及びその水準等に関する考えがあればご教示いただきたい。	<p>相当措置の継続的な実施を確保するために必要な措置として、第三者による相当措置の実施状況並びに相当措置の実施に影響を及ぼすおそれのある外国の制度の有無及びその内容の定期的な確認を行うこと、第三者による相当措置の実施状況に支障が生じたときに必要かつ適切な措置を講ずること、相当措置の継続的な実施の確保が困難となったときに提供の停止を行うことが求められます（個人情報保護法施行規則第18条第1項）。</p> <p>当該相当措置の実施に影響を及ぼすおそれのある外国の制度の有無及びその内容の確認については、一般的な注意力をもって適切かつ合理的な方法により確認する必要があり、例えば、当該第三者に対して照会する方法や、我が国又は外国の行政機関等が公表している情報を確認する方法が考えられます。</p> <p>なお、相当措置の実施に影響を及ぼすおそれのある外国の制度とは、例えば、事業者に対し政府の情報収集活動への広範な協力義務を課すことにより、事業者が保有する個人情報について政府による広範な情報収集が可能となる制度や事業者が本人からの消去等の請求に対応できないおそれがある個人情報の国内保存義</p>



No	該当条項	御意見	御意見に対する考え方
			務に係る制度をいいます。
57	金融分野ガイドライン 第13条第4項	<p>「提供先の第三者が所在する外国の名称を・・・公表するとともに、特定の都度更新することが望ましい」または「提供先の第三者が所在する外国の名称を・・・公表するとともに、定期的に、少なくとも四半期に1回の頻度で更新することが望ましい」に変更すべきと考える。</p> <p>[理由]</p> <ul style="list-style-type: none"> <li>・まず、本来的に、個人情報取扱事業者は、提供先の第三者の所在する国がわかり次第、速やかに公表して本人に対する説明義務及び透明性の観点、並びに金融機関が有する個人情報が本人もたらす影響の大きさから鑑みると、特定でき次第、本人に対して最新の情報を公表すべきものである。</li> <li>・逆に、更新しない場合、古い情報を公表したままになっており、不十分又は不正確な情報を本人に提供し続けることになり、本人保護に欠ける。</li> <li>・そして、金融機関の管理部門（法務部、コンプライアンス部等）が一般の事業会社に比べて充実していることを踏まえると、金融機関であれば特段の負担なく対応しうると考えられ、金融機関における個人情報取扱事業者以外とは異なる取扱いを金融機関における個人情報取扱事業者に求めたとしても、過度な負担を課すことにはならないと考える。</li> </ul>	<p>提供先の第三者が所在する外国が特定できない状態で本人の同意を根拠として個人データを第三者に提供する場合には、同意を取得するに際して、特定できない旨及びその具体的な理由、外国の名称に代わる本人に参考となるべき情報について（金融分野ガイドライン第13条第2項）、提供先の外国にある第三者が基準適合体制を整備していることを根拠として個人データを当該第三者に提供する場合には、本人の求めに応じて提供先の第三者が所在する外国の名称等について（同条第3項）、本人に情報提供する必要があります。</p> <p>上記のほか、同条第4項では、個人データの越境移転に係るリスクに対する本人の予見可能性を高めることを目的として、提供先の第三者が所在する外国の名称を公表するとともに、定期的に更新することが望ましいとしており、一般に現状の案で御理解いただけるものと考えます。なお、同条第4項の「定期的に更新」とは、年に1回程度又はそれ以上の頻度で確認し、更新することをいいます。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>・そのため、金融機関が有する個人情報本人もたらす影響の大きさに伴う情報提供の必要性に基づき、金融機関における個人情報取扱事業者以外とは異なる取扱いを金融機関における個人情報取扱事業者の本ガイドラインに求めるべきと思料する。</p>	
58	金融分野ガイドライン 第13条第4項	<p>4で「提供先の第三者が所在する外国…の名称をインターネットのホームページへの掲載等により、公表する」とあるが、事業者が、個別サービスを提供している顧客の個人データを外国の第三者に提供している場合において、対象となる個別の顧客に、逐一、書面で、当該第三者が所在する外国の名称を通知している場合には、インターネットでのホームページへの掲載は不要と考えてよいか。その場合は、「等」には、個別の書面通知も含まれると考えてよいか。なお、文中「前2項の定めるところにより、」とあるが、「前2号の」の誤りではないのか。</p>	<p>金融分野ガイドライン第13条第4項は、個人データの越境移転に係るリスクに対する本人の予見可能性を高めることを目的として、提供先の第三者が所在する外国の名称を公表するとともに、定期的に更新することが望ましいとしています。</p> <p>御指摘の事案は個別の判断になりますが、外国にある第三者に個人データを提供している場合に、その対象となる本人に当該外国の名称を逐一通知することも、本人の予見可能性を高めるために適切な情報提供の方法の一つとして認められるものと考えられます。</p>
59	金融分野ガイドライン 第12条、第13条	<p>金融分野における個人情報保護に関するガイドライン第12条第1項と第13条第1項で、「提供先の第三者の範囲や属性に関する情報」を認識させたうえで本人から同意をとる方法が言及されていますが、これは特定の程度についての問題ではなく、特定の程度が低ければ同意が取り難いというだけで、同意の有効性についての議論を想定していないとの理解で間違いないでしょうか。仮に、「提供先の第三者の範囲や属性に関する情報」として、一定程度の特定が、同意の有効性の前提になるようであ</p>	<p>金融分野ガイドライン第12条第1項及び第13条第1項では、本人が同意の可否を適切に判断できるようにする観点から、第三者への個人データの提供に関する本人の同意を得る際は、「個人データの提供先の第三者」等の情報を本人に認識させた上で、同意を得ることとしており、個人データの提供先の第三者が特定できない場合には、これに代わる本人に参考となるべき情報として「提供先の第三者の範囲や属性に関する情報」を提供することとしており、本人が同意の可否を適切に判断できるようにするため、適切かつ合理的</p>

No	該当条項	御意見	御意見に対する考え方
		<p>れば、どの程度の特定が必要とされるのか、具体的な記載例をお示しいただけないでしょうか。</p>	<p>な方法で特定に努めていただくことが望ましいといえます。</p> <p>なお、「提供先の第三者の範囲や属性に関する情報」としては、個別の事案ごとの判断となりますが、例えば、「グループ会社」等の情報が考えられます。</p>
60	金融分野ガイドライン 第13条	<p>個人データを自社で保管、利用するために使用するシステムが第三者の環境にあること（例えば SaaS、IaaS、PaaS 等）や、自社システムの運用を外部委託することは「第三者への個人データの提供」にはあたらないと理解しています。よって、そうしたシステムが外国に所在しても、この第13条による制限は受けないもの、との理解でよろしいでしょうか。</p>	<p>個人データの第三者への「提供」に該当するかどうかは、当該個人データが保管されるシステムが第三者の環境にある場合において、当該システムを提供する事業者が、個人データを取り扱うこととなっているかどうか判断の基準となります。この点、個人データを取り扱わないこととなっている場合とは、契約条項等によってシステムを提供する事業者が当該システムに保存された個人データを取り扱わない旨が定められており、適切にアクセス制御を行っている場合等が考えられます。</p> <p>そして、当該システムを提供する事業者が、上記において当該個人データを取り扱うこととなっている場合には、個人データの「提供」に該当するものの、個人データの取扱いの委託に伴う提供の場合（個人情報保護法第27条第5項第1号）、当該委託先は同法第27条第1項から第4項の規定の適用については「第三者」には該当しません。</p> <p>また、当該システムを提供する事業者が外国にある場合であって、当該システムのサーバに保存されている個人データを取り扱うこととなっている場合には、</p>

No	該当条項	御意見	御意見に対する考え方
			当該サーバの所在地にかかわらず、金融分野ガイドライン第13条が適用されます。なお、これは個人データの取扱いの委託に基づく場合でも同様です。
61	金融分野ガイドライン第14条	<ul style="list-style-type: none"> <li>・「本人に対して通知又は公表」をするだけでは、「本人に認識させた」ことにはならないという理解でよいか。</li> <li>・「本人に対して明示」をするだけで、「本人に認識させた」ことになるとの理解でよいか。</li> <li>・「本人が認識させるようにする」（改正後通則編ガイドライン3-7-2-2）だけで、「本人に認識させた」の要件を満たすという理解でよいか。</li> </ul> <p>[理由]</p> <ul style="list-style-type: none"> <li>・まず、個人情報の保護に関する法律においては、書面に記載された個人情報を取得する場合は、利用目的を単に通知又は公表するのでは足りず、本人に「明示」することが求められている（以下に抜粋した、法第18条第2項）。</li> </ul> <p>本ガイドラインの上記の箇所も個人関連情報を取得するに際して書面により同意を取る場合であるため、同法が想定した場面に類似した場面と考え、「明示」（法第18条第2項）をすれば「本人に認識させた」ことになるとの理解になると思うが、その点が明らかではないので確認を求めたい。</p> <ul style="list-style-type: none"> <li>・また、改正後の通則編ガイドラインでは、「本人が認</li> </ul>	金融分野ガイドライン第14条の「書面における記載を通じて・・・本人に認識させた上で同意を得る」とは、所定の事項を記載した書面を本人に示す方法により、当該事項を本人に明確に示した上で、本人の同意を得ることを意味します。

No	該当条項	御意見	御意見に対する考え方
		<p>識できるようにする」ことまでは事業者に義務付けられているが、「本人が認識した」ことまでは義務づけられていない。そこで、改正後の通則編ガイドラインの「本人が認識できるようにする」ことで、本ガイドライン上の「本人に認識させた」を満たすことの確認を求めたい。</p> <p>[参考条文]</p> <p>1) 現行の個人情報に関する法律の抜粋  第十八条 個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。</p> <p>2 個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他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、その利用目的を明示しなければならない。ただし、人の生命、身体又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。</p> <p>2) 令和4年4月1日に施行される通則編ガイドラインの抜粋</p>	

No	該当条項	御意見	御意見に対する考え方
		<p>3-7-2-2 同意を取得する主体  &lt;中略&gt;</p> <p>提供先の第三者による同意取得の場合であっても、提供元の個人関連情報取扱事業者による同意取得の代行の場合であっても、個人関連情報の提供を受けて個人データとして取得する主体、対象となる個人関連情報の項目、個人関連情報の提供を受けて個人データとして取得した後の利用目的等について、本人が認識できるようにする必要がある。</p>	
62	金融分野ガイドライン 第14条第1項	<p>通則ガイドライン（令和4年4月1日施行版）3-7-2-1では、「本人の同意は、必ずしも第三者提供のたびに取得しなければならないものではなく、本人が予測できる範囲において、包括的に同意を取得することも可能」とされている。</p> <p>他方で、本改正案では、1個人関連情報の項目、2個人データとして取得した後の利用目的を認識させた上で同意を取得することが規定されているが、これは、通則ガイドラインの上記内容を否定するものではなく、1、2を認識させることで、包括的に同意を取得することも可能との理解でよいか確認したい。</p>	御理解のとおりです。提供先は、必ずしも各提供行為について個別に本人の同意を取得しなければならないわけではなく、本人の意思を明確に確認できる限り、書面における記載を通じて、所定の事項を本人に認識させた上で、各提供行為について一括して同意を取得することもできると考えられます。
63	金融分野ガイドライン 第14条第1項	個人関連情報の提供先（金融分野における個人情報取扱事業者）が、法第31条第1項第1号の本人同意を取得する際に、本条項に従い「個人関連情報の提供を受けて個人データとして取得した後の利用目的」を書面における記載を通じて本人に認識させた場合には、当該利用目	御理解のとおりです。

No	該当条項	御意見	御意見に対する考え方
		<p>的についてあらかじめ公表している場合でなくても、当該個人関連情報の取得後に改めて、法第 21 条の対応（当該利用目的を本人に通知し、又は公表すること）を行う必要はないという理解でよいか（上記のとおり認識させた場合には、法第 21 条に定める利用目的の通知も満たしていると考えられるため）。またこの理解が正しい場合、本条項のなお書きはあくまでも法第 21 条に関する一般的な注意喚起を示したにすぎないものと理解してよいか。</p>	
64	<p>金融分野ガイドライン 第 14 条第 1 項</p>	<p>「書面による記載を通じて、①対象となる個人関連情報の項目、②個人関連情報の提供を受けて個人データとして取得した後の利用目的を本人に認識させた上で同意を得ることとする。」とされている。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）3-7-2-2（2）によると、「提供元の個人関連情報取扱事業者が同意取得を代行する場合には、本人は利用の主体を認識できないことから、提供元の個人関連情報取扱事業者において、個人関連情報の提供を受けて個人データとして取得する提供先の第三者を個別に明示」することが求められているが、提供元に同意取得を代行させた場合に、提供先を必ずしも書面上に記載する必要まではない（口頭での提供先の明示でも可）という理解でよいか。</p>	<p>提供元の個人関連情報取扱事業者は、提供先の金融分野における個人情報取扱事業者による同意取得を代行する場合は、通則ガイドライン 3-7-2、金融分野ガイドライン第 3 条及び第 14 条第 1 項に従って、本人の同意を取得する必要があります。この場合、提供元の個人関連情報取扱事業者は、提供先の第三者についても、他の事項と同様、書面による記載を通じて本人に認識させることが望ましいと考えます。</p>
65	<p>金融分野ガイドライン 第 14 条第 1 項</p>	<p>金融庁「マネー・ローンダリング及びテロ資金供与対策に関するガイドライン」の【対応が求められる事項】にある、顧客管理の実施を目的として、改正法施行前に</p>	<p>本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>

No	該当条項	御意見	御意見に対する考え方
		取得している電話番号の疎通確認、使用状況の確認をするため、外部事業者から当該電話番号の使用履歴の情報提供を受けることは、個人情報保護法第19条「個人データを正確かつ最新の内容に保つ」こと、および同法第23条第1項第1号「法令に基づく場合」に該当し、書面による同意は不要との理解でよいか。	
66	金融分野ガイドライン 第14条第1項	書面による顧客同意が必要とした場合、電話番号の使用履歴を確認することが、「お客さまとの取引を円滑に行うこと」など、既存の個人情報の取扱い等に対する同意によって確認済みと評価できるとの理解でよいか。すなわち、改正法附則第5条第1項の「同意があったものとみなす」ことができるとの理解でよいか。	本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。
67	金融分野ガイドライン 第14条第1項	銀行等、金融分野における個人情報取扱事業者がインターネットバンキングへの不正アクセス/不正送金や預金口座のマネー・ローンダリングの利用の検知、未然防止を目的に個人関連情報取扱事業者から端末情報等個人関連情報の提供を受ける場合は個人情報保護法第23条第1項2号「人の生命、身体また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場合」に該当し、当該顧客からの書面による同意は不要との理解でよいか。	個人情報保護法第31条第1項において、同法第27条第1項第2号の例外事由に該当するか否かは、個別の事案ごとの判断となります。
68	金融分野ガイドライン 第14条第2項	本改正案14条2項の「必要に応じて」の具体的な意味は、本改正案13条3項第2段落と同様に、「外国にある第三者に提供する個人データの規模及び性質並びに個	御理解のとおりです。



No	該当条項	御意見	御意見に対する考え方
		<p>人データの取扱状況等に起因するリスクに応じて」ということでよいか確認したい。</p>	
69	<p>金融分野ガイドライン 第14条第2項</p>	<p>法第31条第2項において読み替えて準用する法第28条第3項に従い、外国にある第三者による相当措置の実施状況を定期的に確認することについて、金融分野における個人関連情報取扱事業者がこれを行う場合であっても、本ガイドライン第14条2項では「必要に応じて」とあることや外国にある第三者への提供編ガイドライン（令和3年10月一部改正）6-1（1）の記載に沿って考えると、必ずしも「個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法」による必要はなく、適切かつ合理的な方法である限り、口頭により確認することも可能という理解でよいか。</p>	<p>金融分野における個人情報取扱事業者が、金融分野ガイドライン第14条第2項に基づき、外国にある第三者による相当措置の実施状況を定期的に確認する際には、「必要に応じて個人データを取り扱う場所に赴く方法又は書面により報告を受ける方法によること」が努力義務として求められており、これらに代わる合理的な方法が認められないものではありませんが、「赴く方法又は書面により報告を受ける方法」によることが望ましいといえます。</p>
70	<p>金融分野ガイドライン 第14条</p>	<p>不正アクセス検知サービスの導入を検討している。サービスの特徴は、リスクベースだけでなく他の導入企業から不正アクセス（実際に不正取引の被害にあった等）と認定されたIPアドレスを共有し、当該IPアドレスが当社会員サービスへログインを試行した際、追加認証等を求めるなど本人性を確認するもの。</p> <p>サービスの利用にあたっては、個人関連情報の第三者提供が発生。</p> <p>しかしながら、第三者提供についての同意を取得するにはシステム開発負荷や顧客利便性の低下につながることから、不正アクセス検知サービスのような、顧客保護を念頭に置いたサービスについては第三者提供に関する</p>	<p>個人情報保護法第27条第1項各号について、ガイドラインやQ&amp;Aにおける事例の追加等については、今後とも引き続き検討してまいります。</p>

No	該当条項	御意見	御意見に対する考え方
		<p>同意を不要と整理をガイドラインにてお示しいただきたい。</p> <p>金融に関するガイドライン（証券等）では、不正検知のモニタリングなどの導入を求める一方、法令に基づく対応ではないことから通常のサービスと同様の取扱いとなっている現状である。</p>	
71	金融分野ガイドライン第15条	<p>法第32条第1項第4号、政令第10条第1項で、保有個人データの安全管理措置を本人の知る得る状態としなければならないとあり、本ガイドライン第20条第1項③に「法第32条における開示等の手続き等」とあるが、プライバシーポリシーや法律に基づく公表事項に記載する必要はあるか（安全管理措置に関する相談窓口は記載済）。</p>	<p>金融分野における個人情報取扱事業者が、個人情報保護法第32条に従い、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際には、自らの金融商品の販売方法等の事業の態様に応じて適切な方法による必要があり、継続的に公表を行う方法として、例えば、金融分野ガイドライン第20条に定める「個人情報保護宣言」と一体としてインターネットのホームページでの常時掲載を行うこと（保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。）、又は事務所の窓口等での常時掲示・備付けを行うこと等が考えられます（金融分野ガイドライン第15条）。</p>
72	金融分野ガイドライン第15条	<p>「保有個人データに関する事項の公表等保有個人データに関する事項の公表等」において、継続的に公表を行う方法の例に、「インターネットのホームページでの常時掲載を行うこと（保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含</p>	<p>個人情報の保護に関する法律等の一部を改正する法律（令和2年法律第44号）による個人情報保護法改正に伴い、保有個人データに関する公表等を行わなければならない事項として、個人情報取扱事業者の住所及び（法人にあっては）法人の代表者の氏名等が追加されました。住所及び法人の代表者の氏名に関して</p>

No	該当条項	御意見	御意見に対する考え方
		<p>む。)」とあるが、この記載内容が意図するところとしては、プライバシーポリシーを含む「個人情報保護宣言」のページから、更に1回程度の操作で遷移するようなリンクを設置したプライバシーポリシー等とは別のページ内に、当該内容を記載することを許容する意図と理解してよいか。</p> <p>プライバシーポリシー等のページは様々な企業において個人情報保護法で定められ必要とされている同意等の内容があり、そのページ内容の変更については容易に変更ができないことがある。このため、プライバシーポリシー等のページに設置したリンクから、本項目が求める公表事項等が記載された別ページへの遷移することが許容されるという内容であることを確認したい。</p>	<p>は、多くの事業者が、事業者概要を示す Web ページを別途作成していることが想定されることから、個人情報保護宣言の Web ページ自体に、当該住所及び法人の代表者の氏名が記載されている事業者概要を示す Web ページに1回程度の操作で遷移するように設定したリンクを掲載することを可能とすることを明確化する趣旨で記載を追加したものです。</p>
73	<p>金融分野ガイドライン 第16条</p>	<p>第16条(例)「企業秘密が明らかになる恐れがある場合」</p> <p>上記(例)を「企業秘密の保護の必要性が、本人が事業者間での個人データの流通を把握する必要性を上回る特別の事情がある場合」に変更すべきと考える。</p> <p>[理由]</p> <ul style="list-style-type: none"> <li>「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、外国にある第三者への提供編、第三者提供時の確認・記録義務編及び匿名加工情報編)の一部を改正する告示」等に関する意見募集において(以下注)、日本証券業協会からの第三者提供記録の不開示</li> </ul>	<p>御意見を踏まえ、次のとおり修文いたします。</p> <p>「企業秘密の保護の必要性が、本人が個人情報取扱事業者における保有個人データの取扱い等を把握する必要性を上回る特別の事情がある場合」</p>

No	該当条項	御意見	御意見に対する考え方
		<p>事由等に関する質問に対して、個人情報保護委員会は、「個別の判断となりますが、秘密情報の保護につき、本人が事業者間での個人データの流通を把握する必要性を上回る特別の事情がある場合には、当該第三者提供記録の全部又は一部を開示しないことができると考えられます。」との回答をしている（通則編ガイドラインの意見募集結果 No. 514）。</p> <ul style="list-style-type: none"> <li>・ かかる回答の趣旨からすれば、単に「企業秘密が明らかになるおそれがある場合」ではなく、「企業秘密の保護の必要性が、本人が事業者間での個人データの流通を把握する必要性を上回る特別の事情がある場合」に限って初めて、本人の開示請求を事業者は拒めるというのが改正法の趣旨に合致していると考えます。</li> <li>・ そのため、上記のガイドラインの文言について令和2年度改正を機に変更することを求める次第である。</li> </ul> <p>[参照] 注) <a href="https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000223334">https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000223334</a></p>	
74	金融分野ガイドライン 第20条	ガイドライン第20条の例にある「階層構造」について、例えば利用目的にかかる事項や開示等の手続きなど、一部の項目を個別のページにとりまとめ、個人情報保護宣言内にそのリンクを掲載することも、「階層構造」とい	金融分野ガイドライン第20条第3項は、金融分野における個人情報取扱事業者の個人情報保護に関する考え方及び方針を適切に理解した上で、自らの判断により選択の機会を行使することができるよう、個人情

No	該当条項	御意見	御意見に対する考え方
		えるでしょうか。あるいは、見出しに「+」ボタンなどを設け、押下すると同一ページ内に表示されるような仕組みのみを指すのかを示していただきたい。	<p>報保護宣言の内容を本人がより理解できるようにするための工夫の事例を示したものです。</p> <p>ここでの階層構造としては、個人情報保護宣言の各項目の見出しの横に「+」のボタン等クリックで展開できるメニュー等を設け、当該「+」のボタンをクリックすると、当該項目の詳細な内容が同じ Web ページに表示されるようなデザインを想定しています。</p>
75	金融分野ガイドライン 第 20 条第 3 項	「消費者等、本人がこれを適切に理解した上で」と本人の例示として消費者を第一に挙げていますが、本ガイドラインの対象となる本人には、個人事業主や自然人である法人代表者といった消費者ではない属性の方も多数いて、本ガイドライン（及び個人情報保護法等）が消費者保護を第一に掲げるものでもないため、改正後第 20 条 2（改正前第 18 条 2）の記載と併せて単に「個人顧客等、本人がこれを適切に理解した上で」と表現した方が良いと思います。この点につきまして、貴庁の見解をご教示ください。	御指摘を踏まえ、「消費者等、」を削除することといたします。
76	金融分野ガイドライン 第 20 条第 3 項	第 20 条第 3 項が設けられた趣旨について教えていただきたい。	金融分野ガイドライン第 20 条第 3 項は、金融分野における個人情報取扱事業者の個人情報保護に関する考え方及び方針を適切に理解した上で、自らの判断により選択の機会を行使することができるよう、個人情報保護宣言の内容を本人がより理解できるようにするための工夫の事例を示すものです。

No	該当条項	御意見	御意見に対する考え方
77	金融分野ガイドライン 第 20 条第 3 項	個人情報保護宣言の望ましい工夫例として、「ポップアップによる同意取得」が記載されているが、どのようなときを想定しているか教えて頂きたい。	<p>金融分野ガイドライン第 20 条第 3 項は、金融分野における個人情報取扱事業者の個人情報保護に関する考え方及び方針を適切に理解した上で、自らの判断により選択の機会を行使することができるよう、個人情報保護宣言の内容を本人がより理解できるようにするための工夫の事例を示したものです。</p> <p>「ポップアップによる同意取得」については、インターネットで本人の同意を取得する場合において、金融分野における個人情報取扱事業者の Web ページで商品やサービス等を申し込む時に、当該ページの中に個人情報の取扱いに係るチェックボックスを掲載した上で、それをチェックすることで本人の同意を取得するのではなく、例えば、商品やサービス等の申込みを決定するボタンをクリックした時に、個人情報保護宣言の URL を掲載されたウィンドウが自動的に表示され、その内容の確認を明示的に求めるようなことを想定しています。</p>
78	金融分野ガイドライン 第 13 条、第 15 条、 第 18 条、第 20 条	<p>第 13 条の「インターネットのホームページでの常時掲載を行うこと」を「インターネットのホームページでの常時掲載を行うこと（保有個人データに関する事項が示された画面に 1 回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。以下同じ。）に変更すべきと考える。</p> <p>[理由]</p>	<p>金融分野ガイドライン第 15 条において、1 回程度の操作で遷移するよう設定したリンクを掲載することを含むとした趣旨は、No. 72 のとおりです。</p> <p>同第 13 条において、本人が、提供先の第三者が特定された場合に事後的に当該第三者の情報等を求めることができる旨の記載は、個人情報保護宣言から遷移することなく、同一ページ内で確認できるようにすべきものとするため、その旨明確となるよう、『「個人</p>

No	該当条項	御意見	御意見に対する考え方
		<p>第15条には、「インターネットのホームページでの常時掲載を行うこと」を「インターネットのホームページでの常時掲載を行うこと（保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。）と記載されているところ、第13条、第18条及び第20条では、「インターネットのホームページでの常時掲載を行うこと」に「保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む」とのかっこ書が付されていない。</p> <p>そのため、反対解釈をすると、第15条でのみ「保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む」ことになり、第13条、第18条及び第20条ではそれを含まないことになってしまう。</p> <p>本ガイドラインの趣旨に照らすと、第13条、第15条、第18条及び第20条で同様に解釈するようにすべきである。そこで、第13条に第15条のカッコ書きを加えたくて、「以下同じ。」と追記すべきと考える。</p>	<p>「個人情報保護宣言」と一体として』とあるのを『「個人情報保護宣言」に記載の上』と修文いたします。</p> <p>なお、同第15条においては、「第20条に定める「個人情報保護宣言」と一体としてインターネットのホームページでの常時掲載を行うこと」について、「保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。」としています。</p>
79	金融分野ガイドライン 第15条、第13条、 第18条	<p>15条に「保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。」という記載が追記されましたが、13条、18条にお</p>	<p>No. 78のとおり、金融分野ガイドライン第13条と第15条では、規定の趣旨が異なります。</p> <p>一方、同第18条の開示請求等の手続に関しては、開示請求等の手続を別途定めている旨を「個人情報保護</p>

No	該当条項	御意見	御意見に対する考え方
		<p>いては、リンクの設定についての特段の記載がありません。</p> <p>15条と13条、18条との間に取扱いの差異はないという理解でよろしいでしょうか。</p>	<p>宣言」自体のWeb ページに記しているのであれば、詳細な手続に関しては別ページにより丁寧に解説することを否定するものではないため、同第15条の「保有個人データに関する事項が示された画面に1回程度の操作で遷移するよう設定したリンクを「個人情報保護宣言」に継続的に掲載することを含む。」について「第18条第1項において同じ。」とすることとします。</p>
80	実務指針	<p>実務指針では、金融分野における個人情報取扱事業者は個人データの取扱状況を確認できる手段の整備として次に掲げる事項を含む台帳等を整備しなければならない、との定めがあるため当社では個人データ管理台帳を整備しております。</p> <p>今回の改正で保有個人データの定義が変更となり当社では個人データは保有個人データであるために、短期的に保管する個人データについても台帳に記載する必要があると想定しており、どのような対応が効率的か検討しているところです。</p> <p>例えば以下のような対応は可能でしょうか。</p> <p>例1 短期的に保管する個人データで当社の定める保管期限を超過したものは開示請求対応のためのみには保管せず、当社の定めに従って記録を残して廃棄する。顧客から開示請求があったとしても廃棄済みであり開示不能と回答する。半年を超えて保管する個人データも同様の対応としておりますので、可能と考えます。</p>	<p>個人情報の保護に関する法律等の一部を改正する法律（令和2年法律第44号）による個人情報保護法改正により、6か月以内に消去する短期保存データも「保有個人データ」に含まれることとなりましたが、開示等の請求等に応じるためだけに保存する必要はなく、利用目的を達成した場合には、遅滞なく消去するよう努める必要があります（個人情報保護法第22条）。そのため、例1に記載のような対応は可能と考えます。</p> <p>保有個人データに関する状況を確認できる手段として、「台帳等」を整備するよう求めています。必ずしも台帳である必要はなく、必要な事項が明示された状態で取得状況等の管理に資するものであれば良いと考えられます。例2のように、1週間以内程度で廃棄するような短期的な保有個人データに関しては、台帳等を分け、別途適切な形で保管することも認められます。</p>



No	該当条項	御意見	御意見に対する考え方
		<p>例2 1週間以内程度で廃棄するような短期的な保管の個人データは、個々に台帳に記載し廃棄後に台帳から抹消するのは煩雑であるために、社内ルールを定め、例えば6カ月などの一定期間後に廃棄が見込まれるものは台帳には記載不要とし、どのようなものが廃棄されたか適切に記録することとする。</p> <p>その他、効率的な方法があればお示しください。</p>	
81	実務指針 2-6-1	<p>同指針「金融分野における個人情報保護に関するガイドライン第8条に定める安全管理措置の 実施について」の2-6-1が今般の改正により削除されているが、その趣旨について教えていただきたい。</p> <p>また、金融機関における個人情報（個人データ）の漏えい等発生時には、「金融機関における個人情報保護に関するQ&amp;A」の別紙様式1又は2により金融庁宛に報告することになっているが、今般の上記改正（2-6-1の削除）により当該様式も改定されることになるのか、さらに同Q&amp;Aも改定されることになるのか、教えていただきたい。</p>	<p>改正前の実務指針2-6-1においては、漏えい等事案が発生した場合に、金融分野における個人情報取扱事業者が、監督当局等への報告・本人への通知・事案の公表を実施しなければならない旨定めていたところ、今般、金融分野ガイドライン第11条において個人データ等の漏えい等事案の際に必要な対応を定めることとしたため、実務指針での改めでの規定は不要と考え、削除したものです。改正前後で実質的な変更はありません。</p> <p>なお、後段については、本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、本意見募集の対象外と考えます。</p>
82	実務指針 2-6-1	従来金融機関は、「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」2-6-1に基づき原則として全件当局報告や本人への	金融分野ガイドライン第11条でお示ししているとおり、金融分野における個人情報取扱事業者は、個人情報保護法に基づき漏えい等報告等の義務を負うのみなら

No	該当条項	御意見	御意見に対する考え方
		<p>通知を行ってきたものと思いますが、今般 2-6-1 が削除されたことにより、全件につき当局報告や本人への通知を行うことは求められなくなり、「金融分野における個人情報保護に関するガイドライン」11 条に基づき、個人情報保護法施行規則 7 条各号に該当する場合のみ当局報告及び本人への通知の対象となるという理解でよいでしょうか。</p>	<p>ず、各業法に基づき漏えい等報告等の義務や努力義務を負うこととなります。</p>
83	<p>実務指針 2-6-3</p>	<p>実施体制の整備に関する物理的安全管理措置に規定される「取扱区域」及び「管理区域」はどのような区域を指すのか、定義を明らかにされたい。現行の「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）」8-5 においては、「管理区域」を「個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域」、「取扱区域」を「その他の個人データを取り扱う事務を実施する区域」としているが、これと同義か。また、「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）（案）」に関する意見募集結果（平成 28 年 11 月 30 日）の 665 番の「御意見等に対する考え方」において、「個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域を「管理区域」としているため、例えば、パソコンで個人情報データベース等を閲覧している場合、そのことのみをもって直ちに当該区域が管理区域に該当するものではないと考えます。」との考え方が示されているが、実務指針（案）に</p>	<p>「物理的安全管理措置」に係る規定は、通則ガイドラインに合わせて金融分野ガイドライン及び実務指針においても明確化させたものであり、用語の定義は通則ガイドラインと同様です。</p>

No	該当条項	御意見	御意見に対する考え方
		おける「管理区域」、「取扱区域」についてもこれと同様に考えて良いか。	
84	実務指針 4-3	<p>「1. 持ち運ぶ個人データの暗号化、パスワードによる保護等」の措置を講じなければならないとあるが、この規定は、スマートフォンを用いて屋外で電子メールその他の顧客情報を利用する場合、スマートフォンにインストールされたアプリに暗号化やパスワードによる保護を義務付けるものか。</p> <p>(理由)</p> <p>スマートフォンを含む技術的安全管理措置の一般論としては、現行の同実務指針 6-2-2 等の「個人データの利用者の識別及び認証」がパスワードに該当し、センシティブ情報に関する同 7-1-3-1 が暗号化について定めているが、本改正案 4-3 がスマートフォンにインストールされたアプリに影響するのを確認したい。</p>	<p>スマートフォンで個人データを持ち運ぶ場合、当該スマートフォンに対する認証等のセキュリティ対応がなされている場合には、「①持ち運ぶ個人データの暗号化、パスワードによる保護等」の措置を講じているものと考えられます。</p> <p>より強固な安全管理措置を講じる観点で、スマートフォンにインストールされたアプリに暗号化やパスワードによる保護等がなされることは望ましいものと考えます。</p>
85	実務指針 4-3	<p>「2. 書類等の封緘、目隠しシールの貼付等」の措置を講じなければならないとあるが、この規定は電子媒体ではなく紙媒体を想定したものか。</p>	<p>例示したものに関しては、紙媒体を想定したものはあるものの、電子媒体の場合は紙媒体の場合の封緘や目隠しシールと同様の効果を生じさせる対応を想定しています。</p>
86	実務指針 6-3④	<p>「漏えい等事案が発生した際の委託先の責任」とありますが、漏えい等のおそれのある場合において、委託先にどのような責任を負わせるのが具体的に妥当であると考えていますでしょうか。</p> <p>また、委託先に漏えい等のおそれのある事案が発生した際に、委託元である金融機関がそれを把握するために</p>	<p>前段について、例えば、委託契約において、委託先の講ずべき安全管理措置の内容を定め、これを遵守しなかった場合の委託先の損害賠償責任の規定を設けること等が考えられます。</p> <p>後段について、例えば、委託契約において、委託先は個人データの漏えい等事案が発生した場合には当該</p>

No	該当条項	御意見	御意見に対する考え方
		<p>は、委託先から適切に報告をさせるための方策を別途考える必要があると思います。この具体的な方策について、貴庁として何か具体案がありますでしょうか。また、委託先に漏えい等のおそれのある事案が発生した際に、適切に報告がなされることを始めから期待せず、形式的に安全管理措置について契約に謳っていただければ良いものとお考えでしょうか。</p> <p>貴庁の見解をご教示ください。</p>	<p>事案が生じた旨を速やかに委託元に通知する義務を負うといった規定を設けること等が考えられます。</p>
87	<p>実務指針 7-2-1-1</p>	<p>個人情報データベース等を取り扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域である「管理区域」外への持出しに関しては実務指針（案）7-2-1-1（現行実務指針 6-2-1-1）に基づき上乗せ措置を講じる必要があるが、その他の個人データを取り扱う事務を実施する「取扱区域」外への持出しに関しては上乗せ措置を講じる必要がないという理解で良いか。</p>	<p>御理解のとおりです。</p>
88	<p>実務指針 7-6-1</p>	<p>自社内外への報告に関する手続きとして、「個人情報保護委員会又は監督当局等への報告」とあります。「法律施行規則第7条各号に定める事態を知ったときは個人情報保護委員会の通則編ガイドライン3-5-3及び3-5-4に従い」個人顧客に関する</p> <p>「個人データ」の漏えい等の報告は監督当局に行い、そのほか、会社の「雇用管理情報」および「株主情報」が対象となる漏えい等の事案（例えば、会社の従業員の個人データの漏えい）は、個人情報保護委員会への報告を行う、という理解でよろしいでしょうか。</p>	<p>御理解のとおりです。</p>

No	該当条項	御意見	御意見に対する考え方
89	実務指針 7-6-1	施行規則第7条の「個人の利益を害するおそれの大きいもの」に該当しない、軽微な漏えい事象についての報告はこれまで同様に四半期の報告を監督当局に対して行えばよろしいでしょうか。	各業法に基づく漏えい等報告（金融分野ガイドライン第11条第1項後段）については、原則として、都度速やかに報告が必要となります。 なお、例えば、FAXの誤送信、郵便物等の誤送付及び電子メール誤送信などについては、個別の事案ごとに、漏えい等した情報の量、機微（センシティブ）情報の有無及び二次被害や類似事案の発生の可能性などを検討し直ちに報告を行う必要性が低いと判断したものであれば、業務上の手続の簡素化を図る観点から、四半期に一回程度にまとめて報告いただいても差し支えありません。
90	実務指針 7-6-1	速報、確報はどのような方法で報告すればよろしいでしょうか、報告様式をお示してください。	個人情報保護法に基づく漏えい等報告に係る報告様式は、個人情報保護法施行規則の別記様式第一となります。 各業法に基づく漏えい等報告（金融分野ガイドライン第11条第1項後段）及び金融分野ガイドラインに基づく漏えい等報告（金融分野ガイドライン第11条第2項。努力義務。）に係る報告様式については、参考となるものを別途公表する金融分野Q&Aに示しております。 これらの様式を用いて電子申請・届出システムにより報告をお願いいたします。
91	その他	「金融分野における個人情報保護に関するQ&A」について改訂版の公表は予定されていますでしょうか。	本意見募集は、金融分野ガイドライン及び実務指針の一部改正（案）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。

以下の欄は、1月27日より開始した意見募集の際にお寄せいただいた御意見のうち、金融分野ガイドラインに関するもののみについて記載しております。

No	該当箇所	御意見の概要	御意見に対する考え方
1	全般	<p>金融機関、とりわけ銀行は日本の経済の血液ともいえるお金の流れに関わる重要な機関である。そこで扱われる情報の取り扱いには、厳重かつ慎重であるべき。監督官庁である金融庁においては、その指揮監督能力において、十分に金融機関に対して行き届いていることが重要だと捉える。</p>	<p>金融機関の業務の公共性にかんがみ、金融機関の情報の取扱いに関しては適切に監督してまいります。</p>
2	全般	<p>本改正に賛成である。適切な改正と思われた。しかし、各種金融機関（ゆうちょ銀行なども含む）については、インターネット上のサービス利用者向けサイト等においてセキュリティ的に不適切となる部分が存在したりする事がそれなりにあったりするので、金融庁は各種金融機関のセキュリティがより高いものになるよう指導等をより積極的に行っていただきたいと考える。（なお、市民としては金融関係サービスについてはすべからく高いセキュリティが必要であると考え。金融庁はCRYPTRECにおける最高レベルとなるような暗号スイートの選択他の措置が行われていない場合は指導を行うようにしていただきたいと考える。）</p> <p>（本改正案は事故発生後の対応についてのものであったが、そもそも事故が発生しにくいような体制である事が望ましいものである。）</p>	<p>貴重な御意見として承ります。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
3	保険業法施行規則第 53 条の 8 の 2、金融分野ガイドライン第 11 条第 1 項	<p>監督当局への漏えい等報告について、仮名加工情報である個人データは報告対象であるか。</p>	<p>金融分野における個人情報取扱事業者は、保険業法施行規則等に基づき、個人である顧客等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、監督当局に報告をする義務を負います（金融分野ガイドライン第 11 条第 1 項後段）。これは、仮名加工情報である個人データの漏えい等であっても同様です。</p>
4	保険業法施行規則第 53 条の 8 の 2、金融分野ガイドライン第 11 条第 1 項	<p>個人データ又は仮名加工情報（以下「個人データ等」という）の共同利用を行っている場合、個人データ等の取得者は保険会社等金融分野の個人情報取扱事業者であり、提供先の共同利用者は金融分野以外の個人情報取扱事業者であるケースも考えられる。</p> <p>共同利用者である金融分野以外の個人情報取扱事業者が個人データ等の漏えい等が発生させた場合、個人データの取得者である金融分野の個人情報取扱事業者に報告義務はないとの理解でよいか。</p> <p>【理由】</p> <p>上記は改正事項以外にも関わるが、今般「仮名加工情報」制度が導入され、共同利用での利活用が広がると考えられ、漏えいの発生も懸念されるため確認するもの。</p>	<p>御理解のとおり、保険会社が取得した個人データを金融分野以外の個人情報取扱事業者と共同利用（個人情報保護法第 27 条第 5 項第 3 号）している場合に、当該他の事業者（共同利用者）において個人データの漏えい等が発生し、又は発生したおそれがある事態が生じたときは、当該保険会社は監督当局に報告をする義務を負いません。</p> <p>なお、個人データの共同利用を実施する場合には、個人データの漏えい等防止に関する事項について、あらかじめ取り決めておくことが望ましいと考えます。</p>
5	金融分野ガイドライン第 1 条第 1 項	<p>金融分野ガイドライン第 1 条第 1 項「関係法令を踏まえ」の関係法令は、今回のパブリックコメントに付されている銀行法施行規則等（及び委任元の法令）が該当するという認識でよいか。これ以外に、該当する法令があれば教えてほしい。</p>	<p>金融分野における個人情報取扱事業者が服する法令が該当します。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
6	金融分野ガイドライン第5条	<p>今回の改正対象ではないが、金融分野ガイドラインで規定されている「機微情報」には、平成29年の改正個人情報保護法の施行に伴って規定された「要配慮個人情報」には含まれない項目が残置されている。これらは、他省庁が策定している「特定分野におけるガイドライン」には見られないものである。</p> <p>平成29年の改正個人情報保護法が施行されて4年以上が経過した今日、金融庁のみが採用する当否、あるいは逆に、他省庁や個人情報保護委員会でも採用すべき要否など、調整検証は行われていないのか。</p> <ul style="list-style-type: none"> <li>・労働組合への加盟</li> <li>・門地</li> <li>・本籍地</li> <li>・性生活</li> <li>・その他（例えば、医師等の診断等によらず、自己判断により市販薬を服用しているといったケース）（出典 現行金融分野Q&amp;A 8頁）</li> </ul>	<p>本意見募集は、「銀行法施行規則等の一部を改正する内閣府令（案）」等（金融分野ガイドラインの一部改正（案）赤字部分を含む）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>
7	金融分野ガイドライン第11条	<p>個人情報保護法や、他の主要先進国の金融規制当局が求めている漏えい報告に比べて、金融分野ガイドライン、金融分野Q&amp;Aが求める漏えい報告の対象範囲が広過ぎるため、過重な負担が生じている。</p> <p>金融分野ガイドライン第11条第1項及び第3項では、「金融分野における個人情報取扱事業者は、施行規則第7条各号に定める事態を知ったときは、（中略）報告しなければならない」、「本人への通知等を行わなければな</p>	<p>個人情報等の漏えい等事案に関しては、一般に、金融機関の取り扱う顧客情報は経済的価値が高く、漏えい等による不正利得のおそれ大きいことも踏まえ、漏えい等事案が発生した場合に金融機関が監督当局に漏えい等事案を漏れなく報告し、監督当局においてそれらを分析し原因への対処を行うことで、重大な漏えい等事案を未然に防ぐ観点で、努力義務として監督当局への報告を求めることとします。</p>



No	該当箇所	御意見の概要	御意見に対する考え方
		<p>らない」と記載しているのであるから、報告義務及び通知義務が発生するのは、個人情報保護法施行規則第7条において規定されている「個人の権利利益を害するおそれ大きいもの」として定める四類型に限定していただきたい。</p> <p>したがって、第2項「金融分野における個人情報取扱事業者は、次に掲げる事態(前項に規定する事態を除く。)を知ったときは」、第3項「金融分野における個人情報取扱事業者は、次に掲げる事態(施行規則第7号各号に定める事態を除く。)を知ったときも」のような無限定な規定は見直していただきたい。</p>	
8	金融分野ガイドライン第11条	<p>金融分野Q &amp; Aは今回のパブリックコメントに付されていないが、現行の金融分野Q &amp; Aの問IV-5の答④において、「個人データ」の「漏えい」とは「個人データが外部に流出すること」と定義されている。個人情報保護法施行規則第7条に規定されている四類型に止まることなく漏えい報告の対象が広範に規定されているため、他の主要先進国における漏えい報告の範囲に比べて、日本の対象範囲が広過ぎる結果となっている。</p> <p>例えば、オーストラリアの金融監督当局APRAの漏えい報告ルール Prudential Standard CPS 234 の section35 においては、金融機関に課される報告義務は、ア) material なインパクトを持つ漏えい、及びイ) 海外の当局に報告した漏えい、と規定されている。</p>	<p>本意見募集は、「銀行法施行規則等の一部を改正する内閣府令(案)」等(「金融分野ガイドラインの一部改正(案)赤字部分を含む)の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>このため、日本に拠点を持つオーストラリアの金融機関は、金融庁に報告した漏えい事案についても、全てAPRAに報告を行っているが、ア)に比較してイ)の事案が軽微なものが多いことが際立ってしまっている。</p>	
9	金融分野ガイドライン第11条第1項	<p>金融分野ガイドライン第11条第1項によると、顧客等に関する個人データの漏えい等が個人情報保護法施行規則第7条各号に定める事態に該当する場合、個人情報保護委員会と監督当局の双方に報告することとなるように見受けられるが、報告先を一本化していただきたい。</p>	<p>金融分野における個人情報取扱事業者は、個人情報保護法第26条第1項に基づき、個人情報保護法施行規則第7条各号に該当する漏えい等事案について報告する場合、（個人情報保護委員会より報告受理権限の委任を受けた）監督当局へ報告することとなります。詳細は、金融分野Q&amp;Aにおいて示す予定です。また、個人情報保護委員会のホームページにおいて、漏えい等報告の報告先（権限委任関係）について示す予定です。</p>
10	金融分野ガイドライン第11条第1項	<p>金融分野ガイドライン第11条第1項後段について、「取り扱う個人である顧客等に関する個人データ」を追加した理由について、同項前段の個人情報保護法施行規則第7条各号と重なり合う部分があるのか、相互排他的なのか、その関係性について教えてほしい。</p>	<p>金融分野ガイドライン第11条第1項後段（業法に基づく報告義務）においては、その取り扱う「個人である顧客に関する個人データ」の漏えい等が発生し、又は発生したおそれがある事態が生じたときに、金融分野の個人情報取扱事業者に報告義務が生じます。他方、同項前段（個人情報保護法第26条第1項に基づく報告義務）においては、「個人である顧客に関する」ものに限定されず、その取り扱う個人データについて個人情報保護法施行規則第7条各号に定める事態が生じたときに、個人情報取扱事業者に報告義務が生じます。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
			<p>個人データの漏えい等事案について、個人情報保護法第 26 条第 1 項の定める報告対象事態（個人情報保護法施行規則第 7 条各号）に該当するとともに、業法の定める報告対象事態にも該当する場合には、双方の法令に基づく報告を行う必要があります。詳細は、金融分野 Q &amp; A において示す予定です。</p>
11	金融分野ガイドライン第 11 条第 1 項	<p>金融分野ガイドライン第 11 条第 1 項後段を追加するにあたり、当該立法事実、制度趣旨について教えてほしい。</p>	<p>銀行法施行規則等の一部を改正する内閣府令等の改正に伴い、当該改正の内容を明示的に示すものです。</p>
12	金融分野ガイドライン第 11 条第 1 項、第 2 項	<p>金融分野 Q &amp; A は、今回のパブリックコメントに付されていないが、金融分野 Q &amp; A IV 4 - 5 の答④に以下の記載がある。</p> <p>「個人データ」の「漏えい」とは「個人データが外部に流出すること」であり、たとえ流出した媒体において暗号化処理がされていたとしても、「個人データ」の「漏えい」に当たります。また、暗号化処理ではなく、パスワードが設定されている場合も同様です。なお、暗号化処理やパスワード設定がされていることは、「漏えい」後に公表や本人への通知等を行うべきか否かを判断する際の判断要素の一つになると考えられます。」</p> <p>他方、個人情報保護委員会の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）の「3 - 5 - 3 - 1 報告対象となる事態」では、以下のとおり規定されている。</p>	<p>本意見募集は、「銀行法施行規則等の一部を改正する内閣府令（案）」等（金融分野ガイドラインの一部改正（案）赤字部分を含む）の内容に関するものであるため、御意見は、本意見募集の対象外と考えます。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>「なお、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合については、報告を要しない。」</p> <p>金融分野Q &amp; Aにおける漏えいの解釈の方が広い結果、社外流出した個人データを第三者に閲覧されないうちに全て回収した場合や、パスワードでプロテクトされた携帯電話やスマートフォン等を紛失したがパスワードでプロテクトされていた又は遠隔操作で直ちにデータを消去した場合なども漏えい報告が求められることとなっている。</p> <p>個人情報保護委員会と同一の解釈を採用規定していただきたい。</p>	
13	金融分野ガイドライン第11条第1項、第2項	<p>「意見公募要領」より、今回の改正の目的は個人である顧客に関する情報の漏えい等が発生し、又は発生するおそれがある事態が生じた場合の当局への報告を義務付けることだと示されている。この改正趣旨を踏まえ、金融分野ガイドライン第11条第1項及び第2項に定める監督当局への報告義務は、あらゆる個人情報についてではなく、銀行等が取り扱う個人顧客に関する個人情報を対象としていることを再確認させてほしい。</p>	<p>金融分野ガイドライン第11条第1項前段（個人情報保護法第26条第1項に基づく報告義務）について、その対象となる個人データは、個人である顧客等に関する個人データに限定されません。</p> <p>金融分野ガイドライン第11条第1項後段（銀行法施行規則等に基づく報告義務）について、その対象となる個人データは、個人である顧客等に関する個人データに限定されます。</p> <p>金融分野ガイドライン第11条第2項については、第1項に該当するものを除き、適切な監督を行う観点から、努力義務として、広く個人情報等の漏えい等につい</p>

No	該当箇所	御意見の概要	御意見に対する考え方
			<p>て報告を求めるものであり、その対象となる個人情報等は個人である顧客等に関するものに限定されません。</p>
14	金融分野ガイドライン第 11 条第 1 項、第 2 項	<p>金融分野ガイドライン第 11 条第 1 項及び第 2 項に定める監督当局への報告義務について、下記のようなケースにおいては本人の権利利益の侵害は実質的に発生していないと考えられると思うが、それぞれのケースについて同項に基づく監督当局への報告義務があるか、見解を聞かせてほしい。</p> <p>A. 会社の環境にアクセスできるアプリケーションをインストールした携帯端末を紛失したが、当該アプリケーション中のデータは暗号化されており、またその利用には ID/パスワードによる認証が必要であるため、当該携帯端末を拾得した第三者によるアクセスが困難であり、当該アプリケーション中の個人情報は実質的に外部に漏えいしていないと考えられる場合。さらに、同日中もしくは翌日に当該端末が発見・返却され、第三者によるアクセスのリスクがなくなっている場合。</p> <p>B. 個人情報が保存されている携帯端末を紛失したが、当該携帯端末の利用には ID/パスワードによる認証が必要であることに加え、アクセスがモニタリングされており、当該携帯端末の紛失・発見・返却までの期間に第三者によるアクセスが発生していないことが確認できた場合</p>	<p>「個人データ」の「漏えい」とは「個人データが外部に流出すること」をいいます。</p> <p>A について、個別の事案ごとの判断となりますが、携帯端末を社外で紛失した場合に、当該端末から個人データを格納しているサーバにアクセス可能な場合には、当該端末を紛失した時点で、個人データの「漏えい」が発生した「おそれ」が認められると考えます。これは、当該端末にパスワード等を設定している場合も同様です。このため、金融分野ガイドライン第 11 条第 1 項の要件を満たす場合には、漏えい等報告の義務を負うこととなります。</p> <p>なお、個人情報保護法第 26 条第 1 項に基づく報告義務（金融分野ガイドライン第 11 条第 1 項前段）との関係では、漏えい等した個人データに「高度な暗号化その他の個人の権利利益を保護するために必要な措置」が講じられている場合には、報告を要しません。他方、業法に基づく報告義務（金融分野ガイドライン第 11 条第 1 項後段）との関係では、漏えい等した個人データに上記措置が講じられているとしても、報告が必要となります。</p> <p>B について、個別の事案ごとの判断となりますが、紛失した携帯端末を直ちに発見した場合において、紛</p>

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>C. 個人情報を含むメールをグループ会社の従業員に誤送信してしまったが、グループ会社間では情報管理に関する共通のポリシーを適用していることから当該グループ会社の従業員による当該個人情報の不正利用のリスクは低く、また当該メールを削除することで当該個人情報のさらなる拡散のリスクを低減しており、実質的に本人の権利・利益の侵害が発生していないと考えられる場合</p>	<p>失中に、第三者が当該端末から個人データを閲覧していないことがアクセスログ等から確認された場合には、「漏えい」に該当しないと考えます。</p> <p>Cについて、個人データが外部に流出しているため、個人データの「漏えい」に該当すると考えます。このため、金融分野ガイドライン第11条第1項の要件を満たす場合には、漏えい等報告の義務を負うこととなります。</p>
15	金融分野ガイドライン第11条第1項、第2項	<p>金融分野ガイドライン第11条第1項前段「施行規則第7条各号に定める事態」、同項後段「取り扱う個人である顧客等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態」、同条第2項①「その取り扱う個人情報の漏えい等が発生し、又は発生したおそれがある事態」、同項②「その取り扱う仮名加工情報に係る削除情報等（省略）又は匿名加工情報に係る加工方法等情報の漏えいが発生し、又は発生したおそれがある事態」との記載があるが、令和3年12月22日付公表の金融分野ガイドラインの一部改正案の第8条第7項(2)⑥の「漏えい等事案（漏えい等又はそのおそれのある事案をいう。以下同じ。）」及び第11条第3項柱書の「漏えい等事案」とでは表現を異にしている。</p> <p>改正案（及び引用先の個人情報保護法施行規則）における「発生したおそれがある事態」と令和3年12月22日付公表の金融分野ガイドラインの一部改正案における「漏えい等の恐れのある事案」では、例えば、個人デー</p>	<p>金融分野における個人情報取扱事業者は、一定の個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、漏えい等報告の義務を負います（金融分野ガイドライン第11条第1項）。漏えい等の「おそれ」は、その時点で判明している事実関係からして、（漏えい等が発生した確証まではないものの、）漏えい等が発生したことが疑われる場合に認められません。</p> <p>個別の事案ごとの判断となりますが、個人データを含む書類を誤って送付しかけたが、送付前に気が付いて防止できた（送付しなかった）という場合には、個人データが外部に流出しておらず、また流出したことが疑われる状況でもないことから、個人情報取扱事業者は漏えい等報告の義務を負わないと考えます。</p>

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>タを含む書類を誤って送付しようとしたところ、自らが付いて防止できたという事例で、漏えい等の結果は発生しなかったものの漏えい等が発生するおそれが生じたという場合について、文理上前者はこれを含まず、後者は含むものと理解しているが、この理解で差し支えないか。それとも、募集要項では「本件は、銀行等に対し、個人である顧客に関する情報の漏えい、滅失若しくは毀損が発生し、又は発生するおそれがある事態が生じた場合の当局への報告を義務付けるための改正を行うものです。」とあるため、募集要項の「発生するおそれがある事態」という表現を踏まえ、報告の対象となる事態には「漏えい等の結果は発生しなかったものの漏えい等が発生するおそれが生じた場合」を含むということになるのか。貴庁の見解を伺う。</p> <p>なお、「発生したおそれがある事態」に「漏えい等の結果は発生しなかったものの漏えい等が発生するおそれが生じた場合」が含まれるとするならば、その想定される具体例、特におそれの程度について教えてほしい。</p> <p>仮に「発生したおそれがある事態」に「漏えい等の結果は発生しなかったものの漏えい等が発生するおそれが生じた場合」が含まないとする理解でよい場合、令和3年12月22日付公表の実務指針の一部改正案で、2-6の柱書及び②並びに7-6に「漏えい等事案」と記載されている部分は、報告の対象（事態）よりも組織的安全管</p>	

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>理措置の対象（事案）の方が広いという認識になるが、それでよいか。</p> <p>また、令和3年12月22日付公表の金融分野ガイドラインの一部改正案に第10条第3項②の「漏えい等事案が発生した場合の委託先の責任」とあるが、委託先の管理についても同様の理解でよいか。</p>	
16	金融分野ガイドライン第11条第2項	<p>金融分野ガイドライン第11条第2項柱書及び同項①を追加するにあたり、当該立法事実、制度趣旨について教えてほしい。</p>	<p>金融分野ガイドライン第11条第2項については、一般に、金融機関の取り扱う顧客情報は経済的価値が高く、漏えい等による不正利得のおそれ大きいことも踏まえ、漏えい等事案が発生した場合に金融機関が監督当局に漏えい等事案を漏れなく報告し、監督当局においてそれらを分析し原因への対処を行うことで、重大な漏えい等事案を未然に防ぐ観点で、努力義務として広く報告を求めるものです。</p>
17	金融分野ガイドライン第11条第2項	<p>金融分野ガイドラインにおける漏えい等への対応に関して、従前、金融機関においては実務指針2-6-1により監督当局への報告が義務とされていたと理解している。</p> <p>今回の改正では、実務指針2-6-1が削除され、かつ、金融分野ガイドライン第11条第2項で、個人情報保護法施行規則第7条各号の事態に該当しない個人情報の漏えい等の場合は監督当局への報告が努力義務とされている。</p> <p>そうすると、改正後は、個人情報保護法施行規則第7条各号の事態に該当しない個人データの漏えい等につい</p>	<p>金融分野における個人情報取扱事業者は、銀行法施行規則等に基づき、個人である顧客等に関する個人データの漏えい等が発生し、又は発生したおそれがある事態を知ったときは、監督当局に報告をする義務を負います（金融分野ガイドライン第11条第1項後段）。これは、当該漏えい等事案が、個人情報保護法施行規則第7条各号に該当しない場合であっても同様です。</p> <p>なお、金融分野における個人情報取扱事業者は、個人情報等の漏えい等が発生し、又は発生したおそれがあ</p>



No	該当箇所	御意見の概要	御意見に対する考え方
		ては、金融機関においても、義務ではなく、努力義務にとどまるとの理解でよいか。	る事態を知ったときは、監督当局に報告をする努力義務を負います（金融分野ガイドライン第11条第2項）。
18	金融分野ガイドライン第11条第2項	金融分野ガイドライン第11条第1項では、報告対象が「その取り扱う個人である顧客等に関する個人データ」とされているのに対して、第2項①では、単に「その取り扱う個人情報」とされているが、こちらも「個人である顧客等に関する」個人情報であると考えてよいか。	金融分野ガイドライン第11条第2項については、第1項に該当する場合を除き、適切な監督を行う観点から、努力義務として、広く個人情報等の漏えい等について報告を求めるものであり、その対象となる個人情報等は、個人である顧客等に関するものに限定されません。
19	金融分野ガイドライン第11条第2項	金融分野ガイドライン第11条第2項柱書及び同項①において、「個人情報」について規模や性質について特段の限定はなされていないが、同条第1項前段及び後段との対比において、報告の対象が過度に広範ではないか。貴庁の見解を伺う。	金融分野ガイドライン第11条第2項については、一般に、金融機関の取り扱う顧客情報は経済的価値が高く、漏えい等による不正利得のおそれ大きいことも踏まえ、漏えい等事案が発生した場合に金融機関が監督当局に漏えい等事案を漏れなく報告し、監督当局においてそれらを分析し原因への対処を行うことで、重大な漏えい等事案を未然に防ぐ観点で、努力義務として広く報告を求めるものであり、同条第1項は義務規定であることと比し、過度に広範なものではないと考えます。
20	金融分野ガイドライン第11条第2項、第3項	金融分野ガイドライン第11条第2項第1号において「その取り扱う個人情報」、第3項第1号において「その取り扱う個人データ」とあるが、これらは、従前より金融分野Q&A IV-6で、金融分野ガイドライン及び実務指針の対象外とされていた「金融機関自身の雇用管理情報、株主情報」まで、上記の「その取り扱う個人情報」「その取り扱う個人データ」に含むものとして上記第11	金融機関自身の雇用管理情報や株主情報の中に含まれる個人データの漏えい等については、業法、金融分野ガイドライン及び実務指針の対象外であるため、金融分野ガイドライン第11条第1項後段（業法に基づく報告義務）及び金融分野ガイドライン第11条第2項の対象とはなりません。

No	該当箇所	御意見の概要	御意見に対する考え方
		<p>条第2項及び第3項の対象に含めるというものではないとの点を確認したい。</p>	<p>なお、金融機関自身の雇用管理情報や株主情報の中に含まれる個人データの漏えい等について、個人情報保護法施行規則第7条各号に該当する場合には、個人情報保護法第26条第1項に基づき、個人情報保護委員会に対して報告を行う必要があります。</p>
21	<p>金融分野ガイドライン第11条第2項、第3項</p>	<p>金融分野ガイドライン第11条について、第2項①に「その取り扱う個人情報（以下略）」、第3項②に「その取り扱う個人情報（以下略）」とあるが、今回同じくパブリックコメントに付されている銀行法施行規則第13条の6の5の2（個人顧客情報の漏えい等の報告）では、「銀行は、その取り扱う個人である顧客に関する情報（個人情報の保護に関する法律（中略）第16条第3項に規定する個人データに該当するものに限る。）」と明記されている。したがって、「個人データに該当しない個人情報」は報告の対象ではなく、本人通知の対象でもないとの理解でよいか。</p>	<p>金融分野の個人情報取扱事業者は、個人データに該当しない個人情報の漏えい等が発生し、又は発生したおそれがある事態を知ったときは、監督当局への報告や本人への通知等の努力義務を負います（金融分野ガイドライン第11条第2項、同条第3項後段）。</p>
22	<p>金融分野ガイドライン第11条第3項</p>	<p>金融分野ガイドライン第11条第3項「また、金融分野における個人情報取扱事業者は、次に掲げる事態（施行規則第7条各号に定める事態を除く。）を知ったときも、これに準じて、本人への通知等を行うこととする。」とあるが、個人情報取扱事業者が、個々の漏えい等事案の内容を鑑みて、本人の権利利益を害するおそれが低いと判断する場合（例えば、漏えい先が金融庁から免許・登録を受けている金融機関等であって、個人情報保護の態勢管理が適切な先であり、二次漏えいや不正利用の可能性</p>	<p>金融分野における個人情報取扱事業者は、個人情報等の漏えい等が発生し、又は発生したおそれがある事態を知ったときは、本人への通知等を行う努力義務を負います（金融分野ガイドライン第11条第3項後段）。この点、金融機関が取り扱う情報の性質を鑑みれば、基本的には全ての事案について本人への通知等を行うことが望ましいと考えます。なお、本人の権利利益が侵害されておらず、今後も権利利益の侵害の可能性がない</p>

No	該当箇所	御意見の概要	御意見に対する考え方
		が相当程度低い場合等) には、本人への通知は必ずしも義務ではないという理解でよいか。	又は極めて小さい場合等には、本人への通知を省略するケースもあります。