② 個人データの適正な取扱いのための取扱規程の策定を通じた従業者の役割・責任の明確化及び従業者への安全管理義務の周知徹底、教育及び訓練を行うこと。

③ 従業者による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び従業者における個人データの保護に対する点検及び監査制度を整備すること。

第10条 委託先の監督（法第22条関係）

1 金融分野における個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、法第22条に従い、委託を受けた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。

当該監督は、個人データが漏えい、滅失又は毀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。

2 「委託」には、契約の形態や種類を問わず、金融分野における個人情報取扱事業者が他の者に個人データの取扱いの全部又は一部を行わせることを内容とする契約の一切を含む。

3 金融分野における個人情報取扱事業者は、個人データを適正に取り扱っていると認められる者を選定し委託するとともに、取扱いを委託した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。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。

具体的には、金融分野における個人情報取扱事業者は、例えば、以下を実施すること。

① 個人データの安全管理のため、委託先における組織体制の整備及び安全管理に係る基本方針・取扱規程の策定等の内容を委託先選定の基準に定め、当該基準を定期的に見直さなければならない。

なお、委託先の選定に当たっては、必要に応じて個人データを取り扱う場所に赴く又はこれに代わる合理的な方法による確認を行った上で、個人データ管理責任者等が適切に評価することが望ましい。

② 委託者の監督・監査・報告徴収に関する権限、委託先における個人データの漏えい・盗用・改ざん及び目的外利用の禁止、再委託に関する条件及び漏えい等が発生した場合の委託先の責任を内容とする安全管理措置を委託契約に盛り込むとともに、定期的に監査を行う等により、定期的又は随時に当該委託契約に定める安全管理措置等の遵守状況を確認し、当該安全管理措置を見直さなければならない。

なお、委託契約に定める安全管理措置等の遵守状況については、個人データ管理責任者等が、当該安全管理措置等の見直しを検討することを含め、適切に評価することが望ましい。

委託先が再委託を行おうとする場合は、委託元は委託を行う場合と同様、再委託の相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、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、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、再委託先が法第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が望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

第11条 第三者提供の制限（法第23条関係）

以下の事項の他は通則ガイドラインの例による。

1 金融分野における個人情報取扱事業者は、法第23条に従い、第三者提供についての同意を得る際には、原則として、書面によることとし、当該書面における記載を通じて、

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

を本人に認識させた上で同意を得ることとする。

2 個人信用情報機関に対する提供

個人信用情報機関に対して個人データが提供される場合には、個人信用情報機関を通じて当該機関の会員企業にも情報が提供されることとなるため、個人信用情報機関に個人データを提供する金融分野における個人情報取扱事業者が本人の同意を得ることとする。

本人から同意を得るに当たっては、本人が、個人データが個人信用情報機関を通じて当該機関の会員企業にも提供されることを明確に認識した上で、同意に関する判断を行うことができるようにすることとする。このため、事業者は、同意を得る書面に、前項に定める事項のほか、個人データが当該機関の会員企業にも提供される旨の記載及び当該機関の会員企業として個人データを利用する者の表示を行うこととする。

「当該機関の会員企業として個人データを利用する者」の表示は、「当該機関の会員企業として個人データを利用する者」の外延を本人に客観的かつ明確に示すものであることが必要であり、会員企業の名称を記載する方法若しくは当該機関の規約等及び会員企業名を常時公表しているインターネットのホームページ（苦情処理の窓口の連絡先等、第18条の内容を記載したもの）のアドレスを記載する方法等により、本人が同意の可否を判断するに足りる具体性をもって示すことをいう。また、本人に表示する個人信用情報機関の規約等においては、機関の加入資格及び会員企業の外延が明確に示されるとともに、個人データの適正管理、情報の目的外利用の防止等の観点から、安全管理体制の整備、守秘義務の遵守及び違反に対する制裁措置等を明確に記載することが適切である。

なお、金融分野における個人情報取扱事業者は、個人信用情報機関から得た資金需要者の返済能力に関する情報については、当該資金需要者の返済能力の調査以外の目的に使用することのないよう、慎重に取り扱うこととする。

3 与信事業における法第23条第２項（オプトアウト）の規定の適用

金融分野における個人情報取扱事業者は、与信事業に係る個人の返済能力に関する情報を個人信用情報機関へ提供するに当たっては、法第23条第２項の規定を適用しないこととし、前項に従い本人の同意を得ることとする。

4 法第23条第５項第３号に定める通知等（共同利用の際の通知等）

金融分野における個人情報取扱事業者は、法第23条第５項第３号に定める「通知」については、原則として、書面によることとする。

金融分野における個人情報取扱事業者による「共同して利用する者の範囲」の通知等については、共同して利用する者を個別に列挙することが望ましい。また、共同して利用する者の外延を示すことにより本人に通知等する場合には、本人が容易に理解できるよう共同して利用する者を具体的に特定しなければならない。外延を示す具体例としては、

・ 当社及び有価証券報告書等に記載されている、当社の子会社

・ 当社及び有価証券報告書等に記載されている、当社の連結対象会社及び持分法適用会社

といった方法が適切である。

なお、同号は、同号に定める「個人データの管理について責任を有する者」以外の共同して利用する者における安全管理責任等を免除する趣旨ではないことに留意する。

第12条 保有個人データに関する事項の公表等（法第27条関係）

以下の事項の他は通則ガイドラインの例による。

金融分野における個人情報取扱事業者が、法第27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、第18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、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る。