ANDERSON MŌRI & TOMOTSUNE

CAPITAL MARKETS LEGAL UPDATE

2018 年 5 月

GDPR 導入の影響に関する考察

弁護士 福家 靖成 / 弁護士 中崎 尚

EU における General Data Protection Regulation(以下「GDPR」という。)は、2018 年 5 月 25 日に施行されたが、その資本市場に携わる日本の事業者への影響について検討した文献はあまり見られないように思われる。そこで、本ニュースレターでは、GDPR 導入が日本の資本市場に関係する事業者に及ぼし得る影響について検討してみたい。

1 GDPR の導入

GDPR が本年 5 月 25 日から施行された。従前有効であった EU データ保護指令(Directive 95/46/EC)と比べ、GDPR の特徴的な点としては、(i)加盟国の立法を待たずして直接適用の効力があること、(ii)EEA(European Economic Area)圏内在住者の個人データの処理に関して厳格なルールを設けていること、(iii)違反に対しては、巨額の制裁金条項を備えていること、(iv)明確な域外適用ルールが定められていること、といった点が挙げられる。

この点、EEA 圏内の投資家に対して行われる金融商品のオファリング等に関し、当該投資家の個人データが取り扱われる場合としては、大きく、①EEA 圏内の金融機関等の事業者が EEA 圏内の投資家の個人データを取り扱う場合、②日本を含む EEA 圏外の事業者が直接 EEA 圏内の投資家の個人データを取り扱う場合、及び③EEA 圏内の事業者が EEA 圏内の投資家の個人データを取得し、それが日本を含む EEA 圏外の事業者に移転される場合、が想定されるものと思われる。これらのうち、①の場合について EEA 圏内の事業者に GDPR が適用されることは当然であるが、②の場合の EEA 圏外の事業者については GDPR の域外適用の可能性が考えられ、また③の場合には個人データの越境移転に対する規制の適用の可能性が考えられるため、以下それぞれその規制の概要と共に検討する。

2 GDPR の概要

(1) 適用される主体及び個人データ

GDPR で保護の対象となる「個人データ(personal data)」とは、「識別された又は識別され得る自然人(=データ

主体)に関する、あらゆる情報」と定義されている(第 4 条第 1 号)。また、ここで「識別され得る自然人」とは、「当該自然人の氏名、識別番号、所在地データ、オンライン識別子又は身体的・生理的・遺伝子的・精神的・経済的・文化的・社会的固有性などの中から、いずれか一つ以上によって、直接又は間接的に識別される個人のことをいう」とされる(同号)。したがって、対象となり得る「個人データ」は非常に広範であり、例えば、個人投資家の氏名や連絡先情報はもちろん、機関投資家の担当者の連絡先情報も「個人データ」に含まれる。

GDPR が適用される主体は、「管理者(controller)」と「処理者(processor)」の二者に分類される。「管理者」とは、「単独で又は他と共同して、個人データの処理の目的及び手段を決定する自然人、法人、公的機関、行政機関又はその他の団体」(第 4 条第 7 号)、「処理者」とは、「管理者のために個人データの処理を行う自然人、法人、公的機関、行政機関又はその他の団体」(同第 8 号)とそれぞれ定義され、いずれも法人格の有無や営利性の有無は問われない。両者の区別は、個人データの処理を自らのためにするのか、委託を受けて委託元のために行うかによる違いにある。

(2) 域外適用

GDPR では、従前の EU データ保護指令に比べ、域外適用のルールが明確化された。すなわち、域内に拠点を有していない事業者であっても、「域内に所在するデータ主体に対する商品又は役務の提供」あるいは「域内で行われるデータ主体の行動のモニタリング」に関連して個人データを処理する場合には、GDPR が適用されることが明確に定められた(第 3 条第 2 項)。上記②の、日本を含む EEA 圏外の事業者が直接 EEA 圏内の投資家の個人データを取り扱う場合に、GDPR の域外適用があるか否かについては、「管理者」又は「処理者」として、「域内に所在するデータ主体」に対し、「商品又は役務の提供」を行っていると言えるか否かがポイントとなる。この点に関して考慮されるべきファクターの例としては、(i)EEA 圏内からのアクセス可能性、(ii)使用言語、(iii)決済に利用可能な通貨、(iv)その他のウェブサイト上の記載、が GDPR では列挙されている(前文第 23 項)。英語版のウェブサイトを用意していた場合には、形式的には(i)及び(ii)の要件を満たしてしまうものの、それだけで現地向けに「商品又は役務の提供」を行っていると評価される可能性は低いと考えられるが、(iii)の通貨や(iv)に関して特定の加盟国の投資家を意識した記述がされているような場合には、当該加盟国向けに「商品又は役務の提供」を行っていると評価される可能性も否定できない。

これに対し、「域内で行われるデータ主体の行動のモニタリング」という要件に関しては、典型的には、ウェブサイト閲覧履歴を追跡して、趣味嗜好や興味ある商品を分析して広告を表示するといったことが想定されているため、金融商品のオファリング等との関係では、問題になる場合は少ないように思われる。

EEA 圏外の事業者が GDPR の域外適用を受けることになった場合には、当該事業者は、EEA 圏内の事業者と同等以上の義務を負うことになる。すなわち、「管理者」の場合には、説明責任(第 5 条第 2 項)、同意の証明(第 7 条第 1 項)、データ主体の権利の尊重(第 12 条ないし第 22 条)、データ保護方針の策定・施行(第 24 条第 2 項)、管理者による処理活動の記録保持義務(第 30 条第 1 項)といった EEA 圏内の事業者と同様の諸々の義務に加え、EEA 圏内における代理人の選任義務(第 27 条)を負うことになる。代理人選任義務の違反には、最大 1000 万ユーロ又は年間世界売上高の 2 パーセントのいずれか高額な方を上限とする制裁金が科される可能性がある(第 83 条第 4 項(a))。

(3) 越境移転規制

上記③の、EEA 圏内の事業者が投資家の個人データを取得し、それが日本を含む EEA 圏外の事業者に移転される場合には、越境移転規制を遵守する必要がある。GDPR では、EU データ保護指令に基づく越境移転規制ルールが基本的に維持されており、個人データを EEA 圏内から圏外に移転することは、一定の要件を満たす場合にのみ許容される(第 44 条)。仮に第 44 条違反とされた場合には、最大 2000 万ユーロ又は年間世界売上高の 4 パーセントのいずれか高額な方を上限とする制裁金の対象となる他、社名の公表等の措置を受ける可能性がある。

個人データの越境移転が認められる場合としては、まず、移転先が「十分性」の認定を受けている場合、すなわち欧州委員会が特定の第三国・地域・国際機関等のデータ保護レベルを評価した結果として、十分な保護のレベルを確保していると認められる場合を挙げることができる(第 45 条)。しかし、本稿執筆時点では、日本はまだ十分性の認定を受けられておらず、日本の事業者が十分性の認定に依拠することはできない。

次に検討すべき例外として、管理者・処理者が以下のような適切な保護措置を提供しており、かつ、執行可能なデータ主体の権利及びデータ主体に関する効果的な司法救済が利用可能である場合には、EEA 圏内の管理者・処理者は、圏外の国等に個人データを移転することができるものとされている(第 46 条第 2 項)。すなわち、拘束的企業準則(Binding Corporate Rules、以下「BCR」という。)、標準データ保護条項(Standard Data Protection Clauses、以下「SDPC」という。)、行動規範(Codes of Conduct)、及びデータ保護認証(Certification)である。このうち、BCR は、主に企業グループ内での利用が想定され、EU の監督当局の個別の承認を受ける必要があり、導入のハードルが高い。SDPC は、移転元・移転先間で標準的条項に従って締結されるべき個別の合意であり、今後公表される予定の SDPC に従って契約を締結することで、個人データの移転が可能となるものであるが、移転元・移転先間において相対で個別に締結する必要がある。BCR 及び SDPC は、EU データ保護指令上も認められていたものである。これに対し、「行動規範」及び「データ保護認証」は、GDPR で初めて認められたより簡易な制度である。「行動規範」は、事業者団体により策定され、監督当局の承認を受けた後、当該事業者団体に属する事業者が利用可能となるものである。データ保護認証は、専門的な認証機関により、管理者・処理者のデータ保護措置が GDPR を遵守していることを認証する制度であり、認証の有効期間は最長 3 年とされる。場合によるものの、ある程度反復継続して EEA 圏外への個人データの移転が予定されているような場合には、SDPC の締結や行動規範又はデータ保護認証の利用も検討されるべきであると考えられる。

移転先が十分性の認定を受けておらず、かつ BCR、SDPC、行動規範又はデータ保護認証による適切なデータ保護措置のいずれも充足していない場合、圏外への個人データ移転のためには、データ主体の明示的な同意や、重要な公共の利益のために移転が必要な場合等の、第 49 条第 1 項に定められた特定の状況においてのみ認められる例外のいずれかに依拠することを検討することとなる。また、当該同意を得たとするためには、十分性認定及び適切な保護措置がないために当該移転によりデータ主体に生じ得るリスクについて情報が提供された後、データ主体から移転について明示的に同意を得る必要がある。日本の個人情報保護法では、データ主体から同意を得ることにより外国にいる第三者への個人データの提供ができることになり、また同意の取得に関する手続きは特に定められていないため、実務的にも同意を得ることで解決を図る傾向が強い。他方、GDPR については、同意はあくまで例外的な事由の一つと位置付けられていることに加え、同意の取得手続きについて前述のような厳格な要件が定められているため、事後的に監督当局から同意の手続きに問題があったとの指摘を受け(かつ他の適法化事由も充足していなければ)、越境移転が違法とされてしまうリスクに鑑みると、前述のデータ保護措置の導入についても検討されるべきであると思われる。

日本が十分性の認定を受けられた場合には、越境移転規制の適用は受けないことになるが、仮に監督当局から日本の十分性の認定が取り消された場合のビジネスの継続性・安定性にも鑑みると、重畳的に他のデータ保護措置を講じておくことも検討に値するものと思われる。

3 GDPR の違反の効果

GDPR の違反に対しては、警告や種々の命令等の是正措置が定められている(第 58 条第 2 項)。また、GDPR により新たに導入された措置として、高額な行政制裁金の制度がある。従前の EU データ保護指令の下では、各国の法令により制裁金の仕組み・金額が定められていたが、それらは GDPR が定める上限額よりもはるかに低額なものであった。すなわち、GDPR においては、違反する条項に応じて、(i)最大 2000 万ユーロ若しくは年間世界売上高の 4 パーセントのいずれか高額な方、又は(ii)最大 1000 万ユーロ若しくは年間世界売上高の 2 パーセントのいずれか高額な方、が上限額とされている。これらの制裁金は、他の是正措置に追加して、又はそれらの代わりとして課されるものとされている。

4 対応

日本の事業者が EEA 圏内の投資家に対するオファリング等に関して投資家の個人データを取り扱う場面は限定的であるかもしれないが、以上のとおり、仮に GDPR 違反とされた場合の効果は非常に厳格なものであるので、留意する必要があろう。すなわち、上記②の日本の事業者が直接 EEA 圏内の投資家の個人データを取り扱う場合には、GDPR の域外適用を受けないように留意する必要があるし、また仮に域外適用を受ける場合には、GDPR の厳格な様々なルールを遵守する必要が生じることになる。また、上記③の EEA 圏内の事業者が投資家の個人データを取得し、それが日本の事業者に移転される場合には、日本が十分性の認定を受けられていない現状に鑑みると、上記 2(3)のいずれかの適切なデータ保護措置の導入を含めた対応を検討する必要がある。

- 本ニュースレターの内容は、一般的な情報提供であり、具体的な法的アドバイスではありません。お問い合わせ等ございましたら、下記弁護士までご遠慮なくご連絡下さいますよう、お願いいたします。
  弁護士　福家　靖成（yasunari.fuke@amt-law.com）
  弁護士　中崎　尚（takashi.nakazaki@amt-law.com）

- ニュースレターの配信停止をご希望の場合には、お手数ですが、お問い合わせにてお手続き下さいますようお願いいたします。

- ニュースレターのバックナンバーは、こちらにてご覧いただけます。

- Capital Markets Legal Update 発行責任者
  弁護士　多賀大輔、広瀬卓生、吉井一浩、福田直邦

ANDERSON MŌRI & TOMOTSUNE

アンダーソン・毛利・友常 法律事務所

〒100-8136 東京都千代田区大手町1-1-1 大手町パークビルディング
TEL:03-6775-1000
www.amt-law.com