



シンガポール個人情報保護法の制定

執筆者：日比 慎（アソシエイト）

シンガポール個人情報保護法の制定

シンガポールでは従来、銀行法、通信法、コンピューター濫用防止法などの個別の法律において、一定の分野での個人情報の保護が定められていたものの、個人情報保護に関する一般的な法律は存在していなかった。この間、東南アジア各国でも個人情報保護法の制定が続いており、シンガポールでも個人情報保護に関する関心の高まりを受けて、個人情報保護法（Personal Data Protection Act、"PDPA"）が制定・施行されることとなった。2012年10月に国会にて可決され、監督官庁（Personal Data Protection Commission、"PDPC"）の設置などに関する一部の規定は、既に2013年1月2日から施行されている。そして、以下にて説明する Do-Not-Call 規制に関しては、1年の準備期間において2014年1月2日から、個人情報保護に関する規定については、1年半の期間において2014年7月2日からそれぞれ施行されることとなる。

Do-Not-Call 規制

Do-Not-Call 規制とは、登録機関（Do-Not-Call Registry）に登録されたシンガポールの電話番号に対してはマーケティング目的での電話、SMS（ショートメール）やファックスを送ってはならないという規制であり、日本では耳慣れない規制だが、イギリス、アメリカ、カナダなどでも同様の規制が行われている。マーケティング目的には、商品、サービス、ビジネスや投資の勧誘や宣伝などの目的が含まれる。この規制については、例えば、シンガポール所在の企業が、海外の業者に業務委託を行って、海外の業者を通じてシンガポールの電話番号に SMS などを送る場合にも適用があるものとされている。なお、個人の明確かつあいまいな点の無い書面等での同意があればこの規制は適用が無いものとされる。

個人情報保護に関する規制の適用対象

PDPA による個人情報保護に関する規制を受ける対象は、広くなっており、シンガポールにおいて個人情報を取得、利用又は開示するのであれば、その規模などを問わずあらゆる団体に適用があることとされている。すなわち、個人、企業、団体などの区別を問わず、またシンガポールで設立されたかどうか、シンガポールに事務所を有しているかなどを問わずに適用を受ける¹こととされており、日本所在の日本企業や個人にも理論上は適用が及ぶこととなる。なお、日本を含めた海外にも適用があるとの点については、PDPA 違反があったとして実際に罰則が適用され執行されるかといえば、現実的な可能性は低いと思われる。

対象となる個人情報

PDPA の対象となる個人情報は、真実か否かを問わず、当該情報それ自体から、または当該情報および企業等がアクセス可能か可能であると考えられるその他の情報との組み合わせから、個人が特定できる情報と定義されており、電子的なデータか否か、機微 (センシティブ) 情報か否かなどを問わずに該当するものとされており、広範な情報が対象となることとなる²。

個人情報の取得等に関する同意の必要性

PDPA においては、個人情報の取得、利用、開示に際しては、事前に当該個人から同意を得ることが必要とされている。この同意は有効に取得されなければならないが、明示の同意のほかに黙示の同意 (みなし同意) でも足りることとされている。みなし同意があるとされるための要件は、個人が自分の個人情報を特定の目的のために企業等に自発的に提供し、かかる自発的な提供がなされるのが合理的であることとされている³。

同意の取得にあたっては、企業等は、当該個人に個人情報の取得、利用、開示の目的を事前に伝えなければならないものとされている。また、個人情報を、当初取得した同意と異なる目的のために利用する場合には、改めて同意を取得することが必要となる。

なお、他の法律により許容されている場合や個人利用目的の場合⁴などについては、例外的に、個人の同意なく個人情報を取得、利用、開示できるとされている。

¹ 個人の資格で活動する個人や、企業のために活動する従業員など規制の適用を除外される者も存在する。

² ビジネスのためのコンタクト情報(個人の氏名、肩書、業務上の電話番号などの情報であり、個人的な目的で提供されたものでない情報であり、典型的には名刺記載の情報)など適用を受けない情報もある。

³ なお、みなし同意については、個人が A から B への個人情報の開示に同意した場合には、B による当該個人情報の取得についても同意したものとみなされる。

⁴ 個人の生命、健康、安全に関わる緊急事態や公の情報である場合などにも、例外的に個人の同意なくとも個人情報を取得、利用又は開示することが認められている。なお、企業買収の判断のための個人情報の開示と利用も一定の条件の下で個人の同意なく行えることとされている。

思想・信条や健康状態などに関するいわゆる機微（センシティブ）情報について

PDPAにおいて、特に機微（センシティブ）情報について他の情報と区別した取り扱いが必要となる旨は明示されていない。もっとも、PDPAは、個人情報の管理に際して合理的なセキュリティの確保をすることを企業等に対して求めているが、監督官庁であるPDPCが2013年9月に公表したガイドラインでは、適切なセキュリティの水準を決定する上で、対象となる個人情報の性質を考慮に入れる必要があるとされており、機微（センシティブ）情報に該当するか否かも考慮要素になるものと思われる。そのため、機微（センシティブ）情報に該当する個人情報に関しては、情報の管理に際して、一般の情報よりも厳格なセキュリティ手段を講じるなどの対応が必要になるものと思われる。

個人情報の正確性の担保

PDPAでは、個人情報を当該個人に影響を与える決定を行うために利用されうる場合や、他の企業等への開示が行われうる場合、取得する個人情報については正確かつ完全であることを担保するために合理的な努力をしなければならないものとされている。さらに、PDPCが2013年9月に公表したガイドラインでは、取得した個人情報を正確に記録すること、取得した個人情報に関連する部分をすべて含むこと（完全であること）、個人情報の正確性を担保するために適切かつ合理的な対策を講じること、個人情報を最新のものに更新するかを考慮することについても企業等は合理的な努力を行わなければならないものとされている。

個人情報の管理に関連するその他の義務

各企業等は、個人情報保護責任者（data protection officer）を選任しなければならない。この個人情報保護責任者は、最低1名選任する必要があるが、他の業務との兼任でもよいものとされているが、必ずしも当該企業等の従業員でなくともよいものとされている。個人情報保護責任者は当該企業等がPDPAを遵守するようにする義務があるが、これは、当該企業等において、個人情報保護責任者を選任したことによってPDPA遵守の義務を免れるということではない。

また、機微情報について言及したように、各企業等は、取得した個人情報の管理に関して合理的なセキュリティの手段を確保する必要がある。さらに、管理している個人情報の継続的な保持がその情報を取得した目的のためにもはや役に立たないか、法令順守やビジネスのためにもはや必要でないと判断することが合理的となった場合には、当該個人情報を含む書類などを破棄する必要がある。

第三国移転規制について

PDPA では、企業等が個人情報をシンガポール国外に移転させることを原則として禁止しており、例外的に、PDPA と同程度の個人情報の保護を企業等が与えることを確保するための PDPA の要件を満たす場合にのみ、国外への移転ができるものとされている。具体的に日本企業が問題となる場面としては、例えばシンガポール子会社の従業員の人事情報について日本本社で一元的に管理を行う場合が考えられる。現時点では、例外に該当する具体的な要件は明確にされていないが、EU などでの実例を踏まえて、EU データ保護指令 (EU Data Protection Directive) において採用されているモデル契約 (Model Contract Terms) 方式⁵や BCR (Binding Corporate Rules for international transfers) 方式⁶を例外要件とすることが議論されている⁷。今後の議論の進展次第だが、日本とシンガポールとの間で個人情報の移転を行う企業は、EU 域内の企業との関係で蓄積されてきた実務を参考として例外要件を満たすように対応する必要がある。

個人の情報コントロール権など

個人の情報コントロール権については明確な定めはないものの、PDPA は一定の権利を個人に認めている。まず、個人情報の取得、利用、開示に関して、何らかの目的で同意 (みなし同意を含む) を与えた個人には、かかる同意を取り消す権利が認められている。また、企業等が保持する個人情報について誤りや脱落がある場合には、かかる誤りや脱落を訂正するように企業等に請求することができることとされている。さらに、自らの個人情報を保有する団体が PDPA の個人情報取り扱いルールに違反したことによって直接的な損害を被った個人は、PDPC に不服申立てを行うことにより救済を求めることができるほか、PDPC の決定では救済を受けられないことが確定した場合には、当該企業等を被告として民事裁判上の請求を行うことができるものとされている。

⁵ EU が承認した、EU 域外の国への個人情報の移転に関するモデル契約を、個人情報を管理する EU 域内の企業と個人情報の移転を受ける EU 域外の企業との間で個別的に締結する方法。

⁶ 同一の企業グループ内で EU 域外のグループ企業に個人情報を移転させることについて、企業グループ内でルールを定め、これを拘束力のある企業ルールとして EU のデータ保護機関の承認を得る方法。

⁷ 第三国移転規制については、ガイドラインにて詳細な説明が加えられる予定であるが、本稿執筆時点においてはまだ公表されていない。なお、仮に EU データ保護指令第 25 条の国家単位での充分性認定の方法が採用されたとしても、日本の個人情報保護法は個人の同意、アクセス権、監督機関や司法救済の点などで PDPA よりも規制が緩いと評価される可能性が相当程度あり、国家単位では充分性認定を受けられないのではないかとと思われる。

PDPA 施行前に取得している個人情報に関する経過措置

PDPA の個人情報保護規定の施行前にシンガポールにて取得された個人情報については、特に当該個人に通知するなどの義務は課されておらず、個人の側から企業等による利用に同意しないという意思表示等が無ければ利用等を続けることができる。もっとも、当該個人情報を取得した当初の目的と異なる目的で利用、開示する場合には、改めて該当する個人から同意を取得する必要があるものと考えられる。また、Do-Not-Call 規制については、施行日前に取得された同意も有効であるとされているが、かかる同意についても「明確かつあいまいな点の無い」同意でなければならないとの考え方がガイドラインで示されていることに注意を要する。

罰則等

個人情報保護規定、Do-Not-Call 規定のいずれについても、PDPA に違反した企業等に対しては、違反内容に応じた罰金等の刑罰が課されるほか、PDPA 違反の態様での個人情報の取得、利用、開示の禁止などの行政処分が下されうる。PDPA 違反が取締役等の同意、黙認、任務懈怠等により生じた場合には、法人のみならず当該取締役等個人も責任を負う。また、従業員による違反は、使用者にて違反行為を防止する方策を採っていたことを証明できない場合には、使用者の責任となりうる。

本書は法的助言を目的とするものではなく、法的意見を構成するものではありません。
個別のお問合せ等ございましたら、下記執筆者までご連絡くださいますようお願い申し上げます。

<執筆者>

[日比 慎 \(アソシエイト\)](#)

E-Mail: makoto.hibi@aplaw.jp

〒100-0011 東京都千代田区内幸町2-2-2 富国生命ビル

URL: <http://www.aplaw.jp/>

© Atsumi & Sakai 2013
