シンガポールにおける
個人情報保護法について

（2022年3月）

日本貿易振興機構(ジェトロ)

シンガポール事務所

ビジネス展開支援課

本報告書の利用についての注意・免責事項

本報告書は、日本貿易振興機構（ジェトロ）シンガポール事務所が現地会計事務所RAJAH & TANN SINGAPORE LLPに作成委託し、2022年3月に入手した情報に基づくものであり、その後の法律改正などによって変わる場合があります。掲載した情報・コメントは作成委託先の判断によるものですが、一般的な情報・解釈がこのとおりであることを保証するものではありません。また、本報告書はあくまでも参考情報の提供を目的としており、法的助言を構成するものではなく、法的助言として依拠すべきものではありません。本報告書にてご提供する情報に基づいて行為をされる場合には、必ず個別の事案に沿った具体的な法的助言を別途お求めください。

ジェトロおよびRAJAH & TANN SINGAPORE LLP は、本報告書の記載内容に関して生じた直接的、間接的、派生的、特別の、付随的、あるいは懲罰的損害および利益の喪失については、それが契約、不法行為、無過失責任、あるいはその他の原因に基づき生じたか否かにかかわらず、一切の責任を負いません。これは、たとえジェトロおよびRAJAH & TANN SINGAPORE LLP が係る損害の可能性を知らされていても同様とします。

本報告書に係る問い合わせ先：

日本貿易振興機構（ジェトロ）
ビジネス展開・人材支援部　ビジネス展開支援課
E-mail：BDA@jetro.go.jp

ジェトロ・シンガポール事務所
E-mail：SPR@jetro.go.jp

JETRO

Copyright © 2022 JETRO. All rights reserved. **禁無断転載**

目次

Copyright © 2022 JETRO. All rights reserved. 禁無断転載

シンガポールにおける個人情報保護法について

Ⅰ．はじめに

シンガポールにおける個人情報保護に関する包括的な法律は Personal Data Protection Act 2012（以下「PDPA」という） である。PDPA は 2014 年 7 月 2 日に全面施行され、2021 年 2 月 1 日に改正が施行された。

シンガポールはアジア地域の経済・金融ハブとして発展し、集積される個人情報の保護についても配慮する必要性が高まったことを背景に PDPA は制定された。2014 年の施行当時は世界的にも厳格な法律として知られていたが、その後、EU の GDPR（EU 一般データ保護規則 General Data Protection Regulation）や日本での個人情報保護法改正、また東南アジア各国でも次々と厳格な個人情報保護法が成立しつつある。近年では、データアナリティクスを基盤とした巨大データ企業の発展やサイバー攻撃、情報漏洩事故などが多発する等の背景から、シンガポールでは多くの議論や幾度のパブリックコンサルテーションを経て、2021 年により厳格に改正された。

シンガポールの個人情報保護法制は、上記法律である PDPA のほか、下位規範である Personal Data Regulations が複数、また解釈・遵守に当たっての指針となる Advisory、Guidelines より構成されている。また、PDPA の遵守状況を包括的に監督する機関として設立された個人情報保護委員会(Personal Data Protection Commission、以下「PDPC」という） が、積極的な執行、処分を行っている。PDPC は、情報保護についての啓蒙活動、情報保護に関するアドバイス、PDPA の施行、実行などの役割を担う(PDPA5 条、6 条)とともに、各種ガイドラインの制定のほか、PDPA 違反の可能性がある者に対する直接的、具体的な改善策などの指示権限が与えられている上、令状なしの立入権限なども認められている(PDPA49 条、50 条)。さらに PDPA は、罰金、禁錮刑をはじめとする厳しい罰則を定めており、注意が必要である。

以下、PDPA のポイントについて解説する。

Ⅱ．PDPA の対象

１．PDPA の適用対象

PDPA は規模、法人格の有無を問わずすべての企業・団体（organisation）が適用対象となる。

PDPA2 条での organisation の定義：

any individual, company, association or body of persons, corporate or unincorporated, whether or not —

(a) formed or recognised under the law of Singapore; or

(b) resident, or having an office or a place of business, in Singapore

Copyright © 2022 JETRO. All rights reserved. 禁無断転載

そのため、外国企業であっても、現地法人・支店・駐在員事務所等のすべてが対象となる。すべての従業員情報は個人情報に当たることから、仮に事業の実態に乏しくとも、個人情報を有さない企業・団体はないことから、すべての企業・団体において遵守が必要となる。

なお、シンガポールの行政団体(public agency)については適用対象外である。個人については私的な活動の範囲あるいは企業等においても当該企業の従業員としての立場としての活動であれば適用されない。

２．個人情報の定義

PDPA における「個人情報」とは、情報からまたはその情報および保有する他の情報とあわせて識別することができる個人に関する情報のことであり、その情報が真実であるか否かを問わない。従って、氏名、住所、電話番号、身分証番号等のほか、顔写真、指紋、声紋、給与をはじめ人事情報等はすべて個人情報に含まれる。

なお、大きな例外としてビジネスコンタクト情報（Business Contact Information, BCI）については PDPA の適用が除外されている。ビジネスコンタクト情報とは、ビジネス上連絡をとるために用いる情報のことであり、具体的には名刺に記載されるような情報を言う。ただし、名刺に記載された情報であっても、あくまでビジネス目的で取得されたものに限られ、ビジネスと関係ない私的な目的での名刺交換、例えば個人でフィットネスジムに入会登録する際に名刺を連絡先登録情報として渡された場合などは含まれない。

Ⅲ．PDPA の義務・原則

１．企業の義務

PDPA は、企業に大きく三つの義務を課している。

まず、DPO（Data Protection Officer）と呼ばれる、個人情報保護に関する担当・責任者を選任しなければならない。DPO が誰かについては後述の公開原則の対象となり、企業の登記情報に相当する ACRA(Accounting and Regulatory Authority)に登記することができる。

また、後述する PDPA に定める各種原則に即した規程・手続きを整備、運用すること、そして定めた規程・手続きについて従業員に周知徹底・研修を行わなければならない。

２．PDPA の原則

PDPA には、以下の 10 の原則が定められており、企業はこれらを遵守し、遵守するための規程・手続きを整備運用しなければならない。

（1）同意原則：個人情報を収集、使用または開示する前には原則として当該個人から同意を取得しなければならない。なお、同意には明示の同意のほか、黙示の同意や、個人情報の提供からし

Copyright©2022 JETRO. All rights reserved. 禁無断転載

て同意しているとみなすのが合理的な場合など、みなし同意の形式をとることもある。また、個人は一度表明した同意を撤回することができ、企業は同意の撤回を禁止することはできない。ただし、PDPA において同意については一定の例外が定められている。例えば、身体生命等の危険がある場合や、捜査・調査目的の場合、従業員情報についても人事評価目的の場合は必ずしも同意が必要とされない。

（2）目的制限原則：個人情報は、特定の目的のためだけに収集、使用または開示されなくてはならない。使用する目的について、当該個人が当初同意した目的と異なる場合には、当該個人から新たな同意を得ることが必要となる。

（3）通知原則：個人情報を収集、使用もしくは開示するとき、またはその前に、個人情報の収集、使用または開示しようとする目的は当該個人に通知されなければならない。

（4）個人に対する開示および訂正原則：

開示（アクセス）：個人から要求があった場合、当該個人に関して保有する個人情報を当該個人に開示しなければならない。また、個人から要求があった場合には、過去 1 年間に個人情報が使用または開示された方法についても開示しなければならない。

訂正義務：個人は不正確な個人情報について訂正を求めることができる。訂正を求められた場合可能な限り速やかに訂正しなければならず、訂正後の個人情報を当該訂正請求前 1 年以内に開示した相手方にも伝えなければならない。

（5）正確性原則：保有する個人情報は正確かつ完全な状況を保たなければならない。

（6）保護原則：保有する個人情報は、不正アクセスや漏洩等のリスクを回避するための合理的な措置をもって保護されなければならない。いわゆるセキュリティー措置を講じる義務で、「合理的な水準」での措置が求められる。不正アクセスや情報漏洩事故が発生した場合、この保護原則を遵守して合理的な水準での措置がとられていたかが問題となり、不十分であれば罰則の対象とされうる。近時のサイバー攻撃や情報漏洩の増加に伴い保護原則の違反は特に多く、改正でも強化された点であり後述する。

（7）保持原則：個人情報の保持が、事業上または法律上の目的から必要でなくなった場合には、当該個人情報は廃棄または匿名化しなければならない。

（8）移転制限原則：取得した個人情報は、原則としてシンガポール国外に移転してはならず、移転が許されるのは、シンガポール国外に所在する移転先が PDPA に基づく保護と同等の保護基準を法的な拘束力をもって確保できる場合に限られる。これは海外の本社と共有する場合も含まれるた

Copyright©2022 JETRO. All rights reserved. 禁無断転載

め、シンガポールに子会社や支店を有する海外企業において、現地の従業員情報（個人情報）を本社やグループ会社と共有する場合、移転制限原則の遵守が問題となる。移転制限原則を遵守するには、上記のとおり、「法的な拘束力」をもって移転先に PDPA に基づく保護と同等の保護基準を確保する必要があるが、この「法的な拘束力」とは、法令や契約等を指す。日本への移転の場合、日本の個人情報保護法も改正により強化されているが、シンガポール PDPC は特定の国の法令がシンガポール PDPA と同等水準にあるかについて公式に発表している（ホワイトリスト）わけではないため、公式に日本の法令上の保護がシンガポールと同等とは言い切れない。そのため、日本を含むシンガポール国外に個人情報を移転する場合は、移転先と、移転元における PDPA と同等水準での保護を行うことを約する法的な合意書や会社間のルール(binding corporate rules)を定めておく必要があり、これらを無視して移転すると違反となるため注意が必要である。

（9）説明責任原則：企業は、PDPA に即したポリシーおよび手続きを整備・運用し、そのポリシーおよび手続きを一般の要請があれば入手可能な状態にしなければならない。これには DPO（データ保護担当者）を指名し、その連絡先を入手可能な状態にしておくことも含まれる。なお、2021 年改正を機に、本原則は公開原則から説明責任原則（Accountability）に名称変更され、企業において遵守の説明責任を負うという法の趣旨が明確化されている。

(10)データポータビリティー原則：企業において保有されている個人情報について、個人から要請があればほかの企業に移転させなければならない原則。この原則は 2021 年の改正時に新設され、今後実務での運用が待たれる。

Ⅳ．NRIC ガイドライン

PDPA の施行後、PDPC はさまざまなガイドラインを発表し、個別の問題に対処してきた。その中でも大きなインパクトがあったのが NRIC ガイドラインである。

シンガポールでは、全国民に NRIC（National Registration Identity Card）と呼ばれる固有の番号が発行され、居住・就労する外国人についても FIN（Foreign Identification Number）と呼ばれる番号が発行されている。これらの番号は従来個人の特定に広く使われてきたが、個人を特定する重要な個人情報であることから、悪用が懸念され、新たなガイドラインが 2019 年 9 月 1 日より施行されている。

同ガイドラインでは、基本的に NRIC 番号・パスポート番号等の身分証番号の取得を原則として禁止している。例外的にこれら身分証番号の取得が認められる場合として、①法令上必要な場合と、②高度の必要性(Fidelity)がある場合に限られる。ここで①法令上必要な場合とは、法令自体が身分証番号の確認を求めている場合（例えばホテルチェックイン時の確認はホテルライセンス規制で求められている）や、前述の PDPA が定める例外事由に該当する場合（例えば救急のため必要）を言う。他方、②高度の必要性とは、安全・セキュリティー上深刻なリスクがある場合（例えば幼稚園に入場する者の身元確認）あるいは、個人・組織に重大な影響・被害を与える場合（例えば、レピュテーションや詐欺のおそれがある場

Copyright©2022 JETRO. All rights reserved. 禁無断転載

合）をいう。

上記例外事由にかからない身分証番号の取得は一切禁止される。例えば、イベントへの参加や、特に現実的な危険のないような建物・企業への入館等においては、上記例外事由に該当するとは解されず、身分証番号の取得は控えなければならない。また、仮に本人確認が必要でも、上記に当たらない場合は別の方法によらざるを得ず、例えば、NRIC 番号の一部をマスキングするなどの措置が必要となる。

Ⅴ．同意原則の改正（2021 年改正）

１．データビジネス・イノベーションと個人情報

オンラインを通じた買物履歴、ブラウザ履歴、読書履歴、行動履歴、SNS 上のネットワークなど、膨大なデータを分析して特定の消費者嗜好に合わせたサービスの提供を行うビジネスモデルは近年国際的に著しく伸長している。データ分析・AI を用いた企業組織内のオペレーション・プロセス効率化にも大きな進展がみられる。

イノベーションハブを標榜するシンガポールでも同様で、これらのイノベーションには大きな経済上社会上のメリットもありサービスの利用者も便利さを享受できる反面、膨大かつ詳細な個人情報の収集・分析を前提とし、個人情報保護とのバランスが懸念される。PDPC は 2014 年の PDPA 施行以来、パブリックコンサルテーション等で改正に向けて検討を重ね、2021 年改正に至った。改正において、上記のようなイノベーション実現のためには、個人からの同意を厳格に求めるのが難しい場面もあるとして同意原則を緩和して取得しやすくする反面、その場合の個人情報保護を担保するための措置をとることを規定し、イノベーションを阻害しない対応と個人情報保護のバランスを図った。具体的には、「正当な利益（Legitimate Interests）」がある場合、または「事業改善（Business Improvement）」の目的がある場合には、企業にそれらが認められることや不利益に関する説明責任を課した上で、一定の要件のもと同意の取得を免除している。

２．正当な利益・事業改善

「正当な利益」とは、たとえば金融機関が不正を検知・防止する目的、会社が支給するデバイスのデータ喪失を防止する目的（例えばデータ漏洩や不正アクセスを検知するソフトの導入）、不正顧客を防止する目的（例えばブラックリストの共有）などをいう。企業は、「正当な利益」があることを根拠に、同意要件の適用除外を受けるためには、定められたインパクトアセスメントを実施し、正当な利益のためであるか、公共の利益が個人の不利益を上回るか、不利益を緩和する手段がとられているかを自己評価した上で、この例外要件に依拠することを開示し、かつ評価結果を保存しなければならない。

「事業改善」の目的とは、消費者の嗜好分析、新サービス開発、機械学習のラーニングモデルの構築、社内プロセスの自動化・効率化等の目的をいう。企業は、「事業改善」の目的を根拠に同意要件の適用除外を受けるためには、当該個人情報を用いなければ事業改善の目的が達成できないかを自己評価したうえで、合理的な者であれば適切と考えられる範囲での個人情報を共有し、かつ書面により個人情報保護措

Copyright©2022 JETRO. All rights reserved. 禁無断転載

置を整備し運用しなければならない。

３．オプトアウト

2021 年の改正では、前述のみなし同意の解釈を拡張した。当該個人情報の使用の目的を通知され、拒否をするための合理的な期間が与えられたにもかかわらずに拒否しない場合には、個人の不利益や必要性を考慮した上で、異議を述べることができる期間を明示した明確な通知がなされていることを条件に、同意したとみなすことを許すようになった。いわゆるオプトアウト方式で、従来はオプトアウト方式による同意については厳しい姿勢であったのを緩和したものである。例えば、ある銀行が顧客の同意を得て顧客の音声データを取得し、当該音声データを本人確認に使用しようと考えた場合、銀行は当該音声データを本人確認に利用することは信憑性が高く安全で、顧客に不利益を及ぼす恐れがないかを評価した上で、顧客に対して、音声データを使用することと質問がある場合の連絡先、異議がある場合にはメールにあるハイパーリンクを利用し 14 日以内に異議を通知することを求めるといった内容のメールを送信し、14 日間に異議がない場合には、同意があったものとみなすことができる。

Ⅵ. 罰則・通知義務

１．罰則

PDPC は前述のとおり強力な捜査権限を有し、実際に厳しい捜査・摘発を行っている。PDPC は毎週のように摘発した企業をウェブサイト上で公表しており、報道されるような大きな違反でなくとも公表の対象となり、企業のレピュテーション上リスクとなる。

PDPA の違反の罰則としては、PDPA の義務・原則に違反に対する是正命令等および 100 万シンガポールドル以下の罰金が科されうるとされていたが、施行後の情報漏洩事故の国際的な増加もふまえ、2021 年改正で罰則がさらに強化されている。具体的には、100 万シンガポールドル以下の罰金または、直近の監査済み財務報告書に基づき年間売上高の 10%までの罰金を科すことができるとされ、会社規模によってはさらに高額の罰金を科されうる。

また、個人に対する刑事罰も定められており、改正前も PDPC の調査妨害等に対する罰則が定められていたが、さらに、2021 年改正により、権限なく、故意または無関心（reckless）によって個人情報を使用または開示した場合も刑事罰を科すこととされた。

２　通知義務

また、情報漏洩事故(data breach)が生じた場合、漏洩の内容・規模によって PDPC および影響を受けた個人に対する通知義務が定められている。

具体的には、影響を受ける個人の数が 500 人以上の場合は、PDPC にできるだけ速やかに、遅くとも 3 日以内に、通知しなければならないと定められている。また、漏洩した個人情報により影響を受ける個

Copyright©2022 JETRO. All rights reserved. 禁無断転載

人の数は上記 500 人未満でも重大な害をもたらしうる個人情報が漏洩した場合には、同様に PDPC、また当該個人にも通知することが義務として定められている。なお、ここで「重大な害をもたらしうる」個人情報とは、医療情報といった機微情報に限られず、身分証番号等も広く含まれるため、注意が必要である。

3　サイバーセキュリティー

前述のとおり、PDPA の遵守原則の一つに保護原則があり、情報漏洩事故が生じた場合、PDPC により調査がされ、十分なセキュリティー措置を講じていないと判断されれば保護原則違反として PDPA の罰則の対象となる。なお、2021 年 10 月時点の集計では、全違反事案の 64%が保護原則の違反であり、いかに同原則の遵守が重要かを示している（なお、その他の違反は説明責任原則。つまり必要な規程・手続きや DPO を選任・公開していないことによる違反が 16%、通知・同意の原則つまり個人情報の取得・使用について十分な通知・同意がないことによる違反が 12%であった）。

PDPA 施行以後の摘発事例において、とくに高額の罰金を科された事案も保護原則にかかわるものであり、2018 年にシンガポール公共医療機関 Singapore Health Service Pte Ltd (SingHealth)に対する大規模なサイバー攻撃がなされ、その結果 150 万人分もの個人情報が流出し、中には首相の個人情報も含まれているとして大々的に報道された事案があった。同事案について調査がなされた結果、2019 年 1 月、保護原則違反があったと認められ、SingHealth に対して 25 万シンガポールドル、同社の IT を担当していた Integrated Health Information Systems Pte Ltd （IHiS）に対して 75 万シンガポールドル[1]と合計 100 万シンガポールドルの罰金が科された。

同事案は、グループの利用していたワークステーションに対して悪意を持った外部者がサイバー攻撃を行い、マルウェアを通じてさらにほかのワークステーションにアクセスしユーザーアカウントをコントロール、さらにコーディングの脆弱性を悪用した高度なものであり、SingHealth、IHiS は被害者ではあるのだが、調査においてサイバー攻撃防止の措置が十分でなかったとし、PDPC の決定の中でもシンガポール史上最悪の情報漏洩（worst breach of personal date in Singapore's history）と断じられた。

フィッシングメールやマルウェアを含むサイバー攻撃は近時頻繁になされ、どのような事業の会社でも被害者となり得るが、仮にサイバー攻撃の被害者であっても PDPC の調査の対象となり、罰則の対象となりうることは注意しなければならない。また、この事案が示すように、多くの企業では外部の専門の IT 会社にセキュリティー措置を委託していることが多い。しかし、外部専門家に委託しても、サイバー攻撃が発生すると委託した企業側も責任を問われないわけではなく、十分に高度な専門性ある会社に委託したか、委託後も任せきりとせず十分なチェック、監督をしていたかなどが問われ、これらの措置が十分でなければ保護原則違反として罰則の対象となる。上記 SingHealth 社以外の違反事例の多くでも同様にサイバー攻撃による情報漏洩において、委託した企業側も罰則の対象となっている。

近時のサイバー攻撃の横行、前述の通知義務とあいまって、今後ますます保護原則に従いサイバーセキュリティー措置の重要性は高い。なお、PDPC も、ガイドライン Guide on Managing and Notifying Data

[1] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Commissions-Decisions/Grounds-of-Decision---SingHealth-IHiS---150119.pdf?la=en

Copyright©2022 JETRO. All rights reserved. 禁無断転載

Breaches Under the PDPA を定めており、同ガイドラインではセキュリティー措置や漏洩時のプランニングについて平時から定めておくことを求めている。実際の摘発事例でも、情報漏洩が発生した場合、当該漏洩の原因はもとより、漏洩に対していかに迅速・適切に対応したか、また平時より漏洩時に備えてどのようなプランニングや規程・手続ききが定められていたかについても調査、また罰則決定における考慮の対象となる。

Ⅶ. 終わりに

以上のとおり、シンガポール PDPA は規制対象が広く、厳しい罰則が定められている上、執行・摘発も厳しくなされている。個人情報は石油にも相当する新時代の通貨とまでいわれることも多く、ビジネス、イノベーション上重要性はますます高まっている。他方、個人情報が重要となる反面、サイバー攻撃、不正アクセスや情報漏洩事故のリスクも高まっている。こうした現状を反映し、シンガポールも PDPA についてイノベーションにも配慮した改正を行うとともに、違反の摘発を強化するとともに改正でも情報漏洩について通知義務を課し、また罰則を強化している。なお、こうした流れはシンガポールのみならず国際的にもみられ、東南アジア各国でも個人情報保護法の整備が進んでいる。企業においても個人情報保護について法令の内容・義務を十分に理解して遵守するための規程・手続ききを整備するとともに、漏洩事故が生じた場合迅速な対応をとれる措置を十分とることは一層重要である。

Copyright©2022 JETRO. All rights reserved. 禁無断転載