Asia Focus Team
Tokyo

Newsletter

15 October 2019

目次

Asia Focus Newsletter vol. 6

ベーカー＆マッケンジー法律事務所 アジア・フォーカスチームは、アジア・太平洋地域の 17 の事務所からなる、ベーカーマッケンジーのネットワークを最大限に活かし、アジア全域へ進出・事業拡大を検討する日本企業に対し、コーポレート、M&A、ファイナンス、紛争解決等、幅広い分野においてシームレスなリーガルサービスを提供しております。

今号では、個人情報保護に関する規制についてご紹介します。

個人情報保護に関する規制

個人情報・プライバシーデータを保護するための法制度は、EU 一般データ保護規則（GDPR）をはじめとして近年世界的に急速に発展している。ASEAN 諸国でも、個人情報・プライバシーデータ保護に関する法制が整備・強化される傾向にあり、例えばタイでは GDPR をベースとした個人情報保護法が近時制定され 2020 年に施行されることが予定されており、インドネシアにおいても GDPR のコンセプトを導入し従前よりも要件を厳格化するための新たな保護法制が検討されている。

個人情報・プライバシーデータの取扱いについて問題が生じた場合、その結果として制裁金などの行政罰や市場における評価の低下など著しい損害が生じるリスクが年々高まっており、日本企業においても、各国での個人情報・プライバシーデータの取扱いについてより一層注意を払う必要がある。個人情報・プライバシーデータの保護法制は、国ごとに具体的な法律の内容は異なることから、子会社所在国の保護法制の概要を把握し、国ごとに適切な管理体制の整備・実施を行うことが求められる。この関連で、個人情報・プライバシーデータ保護法制は会社従業員の情報にも等しく適用されることが多いため、顧客の個人情報とともに、子会社従業員の個人情報の収集・処理にあたっても適切な措置を取る必要があることに注意を要する。

以下では、ASEAN 諸国の個人情報保護制度の概要について、個別の質問に対する回答の形でまとめている。

本ニューズレターに関するお問い合わせ先

asia.tokyo@bakermckenzie.com

ベーカー＆マッケンジー
法律事務所（外国法共同事業）

〒106-0032
東京都港区六本木 1-9-10
アークヒルズ仙石山
森タワー28F
Tel 03 6271 9900
Fax 03 5549 7720
www.bakermckenzie.co.jp

(1) 個人情報保護に関する法規制はどのようなものか。

ベトナム	主要な個人情報保護に関する法律及び規則は以下のとおりである。 • 民法（No. 91/2015/QH13） • IT 法（No. 67/2006/QH11） • サイバー情報セキュリティに関する法律（No. 86/2015/QH13）（LOCIS） • サイバーセキュリティ法（No. 24/2018/QH14） • 消費者保護法（No. 59/2010/QH12） • 子ども法（No. 10/2016/QH13） • インターネットサービス及びオンライン情報の管理、提供及び使用に関する政令（No. 27/2018/ND-CP）を修正・補足する政令（No. 72/2013/ND-CP）（政令 72 号） • 電子商取引に関する政令（No. 52/2013/ND-CP）（政令 52 号） • 郵便、通信、情報技術及び無線周波数領域に関する行政上の違反の罰則を定める政令（No. 174/2013/ND-CP） • 国家のサイバー情報セキュリティを確保するための緊急時対応計画を定める決定（No. 05/2017/QD-TTg）（決定 5 号） • 全国の情報セキュリティインシデントの調整及び対応に関する規定である通達（No. 20/2017/TT-BTTTT）（通達 20 号）
マレーシア	個人情報保護法（Personal Data Protection Act 2010 （PDPA））のほか、PDPA の関連法規として以下のものがある。 • Personal Data Protection Regulations 2013（PDPR） • Personal Data Protection Standards 2015 • Personal Data Protection (Class of Data Users) Order 2013 • Personal Data Protection (Registration of Data User) Regulations 2013 • Personal Data Protection (Fees) Regulations 2013
タイ	個人情報保護に関する法令は、個人情報保護法（Personal Data Protection Act （PDPA））である。
フィリピン	個人情報保護に関する法令は以下のとおりである。 • データプライバシー法（Data Privacy Act （DPA）） • DPA の施行規則（DPA IRR） • フィリピン国家プライバシー委員会（Philippine National Privacy Commission （NPC））の規則
インドネシア	主要なデータプライバシー、セキュリティに関する法律及び規則は以下のとおりである。 • 2008 年電子情報及び電子取引に関する法第 11 号及び同改正法 2016 年第 19 号（EIT 法） • 2012 年電子システム及び電子取引に関するインドネシア共和国規則（GR82） • 2016 年電子システムの個人データ保護に関する情報通信省（MOCI）規制第 20 号（データ保護規制） なお、現在、GDPR のコンセプトを導入し従前よりも要件を厳格化すべく、GR82 に代わる新たな規制及び個人データ保護法の制定が進められている。2020 年前半頃までに公布される見込みではあるが、具体的な予定は確定していない。

シンガポール	個人情報保護法（2012 年法律第 26 号）（The Personal Data Protection Act 201（PDPA））及び PDPA に基づく行政委任立法が存在する。 PDPA のほか、銀行金融関連法令をはじめとする特定の分野に係る法令において、一定の個人情報（銀行口座番号、顧客情報等）に係る保護規定が存在する。

(2) 個人情報の取得に関する法律上の要件はどのようなものか。

ベトナム	基本的な考え方として、ベトナムの個人情報に関する法律は、個人を個別に識別できる個人（及び小規模組織）に関する又は属する情報（総称して以下「個人情報」という。）を保護するものである。法律及び規則は、どの情報が個人情報を構成するかについて一貫した定義を採用しておらず、規則／法律が適用される分野によって異なる。 また、個人情報の取得には、データ主体である個人から、個人情報の収集、使用及び移転に関する事前の告知に基づき、同意を取得する必要がある。上記の同意の形式に関する特定の規定はない。実務的には、オンライン上でチェックボックスにチェックを入れる形での同意の取得は一般的に受け入れられる一方で、事前に自動的にチェックボックスにチェックされたような形での同意の取得は避けるべきである。特に、消費者保護法は、顧客情報の収集、使用及び／又は移転の前に、事業者は、当該顧客に収集の目的及び顧客情報の使用について明確に及びオープンに通知することを要求する。IT 法は、ネットワーク環境で他者の個人情報を収集する組織又は個人は、データ主体の同意を取得することを要求する。 政令 52 号及び政令 72 号は、(1)データ主体によって電子取引ウェブサイト上で公表された情報、(2) (i)ネットワーク環境での情報、製品又はサービスの使用のために契約の署名、変更又は履行する場合、(ii) ネットワーク環境での情報、製品又はサービスの使用のために料金の設定又は計算する場合、又は(iii)法律に従い他の契約上の義務を履行するときのために使用される場合には、事前の同意なく個人情報を収集できる例外を設けている。 また、個人情報を収集する組織は、組織の属性、収集される個人情報の種類、個人情報を収集する目的、組織が個人情報を開示する第三者、データ主体の権利、どのように個人情報を維持するか、どこに個人情報を移転するか、どこで個人情報を保管するか、及びデータ主体の個人情報のアクセス及び／又は収集方法についての情報をデータ主体に提供しなければならない。
マレーシア	PDPA 上、個人情報の処理（取得を含む）を行う場合には、データ主体の同意が必要となる。なお、データ使用者は、当該同意について、記録、管理を行う必要がある。 もっとも、データ使用者は、データ主体が当事者となっている契約の履行のために必要となる場合など、一定の場合には、個人情報の処理が可能である。 個人情報の取得の際、データ使用者は、データ主体に対して、法令上規定された事項を含むデータプライバシー通知（以下「通知」という）を書面（英語及びマレー語の両方）により提供する必要がある。 その他、データ使用者は、個人情報を処理するにあたり、第三者への開示の際の同意取得（(4)参照）、適切なデータセキュリティ措置の実施、不要となった個人情報の破棄／削除の実施、個人情報の完全性を確保するための合理的措置の実施、データ主体の権利への対応（(6)参照）等を行う義務を有する。
タイ	PDPA は、一定の例外（例：調査又は研究目的等、当該個人情報の匿名性が担保され、かつ、個人の生命、身体又は健康に対する危害を防ぐ又は排除することのみを目的として利用される場合）を除いて、データ管理者は個人情報を収集・利用・開示（以下「収集等」という。）するに際して当該個人情報のデータの主体から収集等と同時又は事前にこれらに関する同意を得ない限り、収集等を行うことができな

	いと規定している。データ管理者は、収集の対象となる当該個人情報が PDPA において規定される一定の詳細な情報（例：収集の目的、個人情報の開示先となる人又は組織の種類、データの主体の権利）を含む場合には、データの主体に対して収集と同時又は事前に通知を行わなければならない。
フィリピン	DPA の下では、個人情報は公正かつ合法的に収集する必要がある。データの収集対象となる個人に対して、データが収集されていることを通知し、同意を得て（契約上の義務を履行する場合を含む特定の例外を除く）、個人情報の修正又は誤った情報を削除する権利を与えることが必要となる。データは特定の正当な目的のために収集する必要があり、収集されるデータの量はその目的に比例する必要がある。また、データは安全に保管される必要があり、その目的に必要な期間に限って保持することが認められる。データ主体は、データ管理者への要求に応じて収集された情報にアクセスできなければならず、データの不正確さについて異議を唱えたり、データを修正又は削除したり、不正確又は不完全なデータ収集による損害を被った場合に補償を受ける権利がある。 上記の一般規則には、国家の緊急事態及び公的機関が関与する場合のデータの収集及び保持に関する例外がある。さらに、DPA は、外国の居住者に関して、当該国の法律に従って収集された個人情報には適用されない。
インドネシア	個人データの使用（個人データの取得及び収集を含む）は、データ主体の事前の書面によるインドネシア語での明確な同意が必要である。 また、事前の同意を取得する前に、電子システムのオペレーターはデータ主体に対して個人データの詳細な使用目的を明確にしなければならない。
シンガポール	一般的に、個人情報の収集、使用又は開示は、当該個人の同意を得た場合、又は法令上の要件を満たした場合に行うことができる。例えば、PDPA の別表 2 (Second Schedule) に掲げる一定の事由（ある個人情報が、①公開されている場合、②公共の利益のために必要とされる場合及び③法令遵守のため必要となる場合等が含まれる。）に該当する場合には、個人の同意なく個人情報の収集、使用又は開示を行うことができるとされている。 一定の例外を除き、個人情報の収集に関して当該個人の同意を得なければならない場合には、当該個人に対して通知を行う必要がある。かかる場合、事業者は、個人情報の収集、使用又は開示の目的を、当該収集、使用又は開示と同時又はこれらに先立って当該個人に通知しなければならない。

(3) センシティブ情報の処理に関する規制はどのようなものか。

ベトナム	センシティブ情報は、ベトナム法上明確な定義はない。さらに、「センシティブ情報」は、ベトナムのデータ保護に関する法律上、特段の厳格な保護基準は置かれていない。
マレーシア	PDPA 上、センシティブ情報とは、データ主体の身体的又は精神的健康又はその状態、政治的見解、宗教的信条又はその他の類似の信条、犯罪行為又は疑われる犯罪行為、その他当局が公報において公表する規則により指定した個人情報を指すと定義されている。 PDPA 上、データ主体の明示的な同意がない限り、センシティブ情報を収集し、保持し、処理し、使用することは禁止されている。ただし、司法行政において必要な場合、又は医療目的の場合は例外とされている。
タイ	センシティブ情報の処理に関する法的根拠は（通常の個人情報と）異ならないものの、以下の追加の要件が必要となる。 • データの主体が処理について明確に同意を与えている場合 • データの処理がデータの主体若しくはデータの主体が物理的又は法的に同意を

	与えることが不可能な自然人の重大な利益を保護するために必要な場合 • データの処理が、政治、哲学、宗教又は労働組合としての目的又はこれらの更なる条件のための財団、団体等の非営利組織によって、適切な予防措置のもとで正当な活動の過程の中で行われる場合 • データの主体によって明白に公にされている当該個人情報に関するデータの処理である場合 • 法的主張の立証、行使又は弁護のためにデータの処理が必要な場合 上記に加えて、PDPA は、付加的基準に応じて、センシティブ情報のデータの処理についての他の追加要件を定めている。 センシティブ情報は PDPA 上で特に定義されていないものの、PDPA 第 26 条によれば、以下のような項目が含まれる。 • 人種、民族的出自、政治的意見、宗教的又は哲学的信条、労働組合員であることを明らかにする個人情報 • 遺伝子情報 • 自然人を特定する目的の生物学的情報 • 健康や医療情報に関する情報 • 性生活又は性的趣向に関する情報 • 犯罪歴 • 障害 • 上記と同様の影響をデータの主体に与える情報で、個人情報保護委員会（Personal Data Protection Committee）により規定されるもの
フィリピン	特定の例外を除き、センシティブ情報の処理は一般に禁止されている。センシティブ情報は、データ主体が同意した場合、法律で許可されている場合、データ主体又は第三者の生命と健康を保護する必要がある場合、医療措置又は法的手続きのために必要な場合には、収集及び処理することができる。 センシティブ情報には、以下のような項目が含まれる。 • 個人の人種、民族、婚姻状況、年齢、肌の色、宗教、哲学、又は政治的所属に関する個人情報 • 個人の健康、教育、遺伝子、性的生活、又は個人が犯したとされる又は実際に犯した犯罪に関する訴訟についての情報 • 政府機関が個人に固有のものとして発行したもの（例：社会保障番号、以前又は現在の健康記録、ライセンス又はその拒否、一時停止、失効、納税申告書） • 大統領令又は議会によって機密性の高い個人情報と指定されたもの
インドネシア	センシティブ情報に関する規制は存在しない。もっとも、新しい個人データ保護法では導入される予定である。
シンガポール	PDPA では、センシティブ情報に関する規定は存在しない。一方で、特定の分野に係る法令においては、特定の情報（国民登録番号、国民登録番号カード、パスポート番号等）の取扱いに関し、特別の定めが置かれている場合がある。

(4) 第三者への個人情報の提供に関する法律上の要件はどのようなものか。

ベトナム	第三者に個人情報を移転する組織又は個人は、通常データ主体の同意を取得しなければならない。上記(2)の回答で説明したとおり、同様の例外が個人情報の移転の際にも適用される。 ベトナム法は、同意を取得する形式についての特定のガイドラインを規定していないが、積極的な行為（オプトイン等）の形式であることが望ましい。黙示的な同意としてのオプトアウトの枠組みは、当局から承認されない可能性が高く、事業者は、オプトアウト等を利用しないことが望ましい。
マレーシア	原則として、データ主体の同意なく第三者に個人情報を提供／開示することはできな

	い。 もっとも、例外として、犯罪の防止・捜査のため、若しくは調査のために必要な場合、法律上認められている場合、裁判所の命令に従う場合、データ使用者が自己に開示を行う権限がある若しくはデータ主体が同意している（データ主体が開示の状況について認識している場合に限る）との合理的考えに基づき開示を行う場合、当該開示が当局により指定された公益のためになされる場合のいずれかに該当する場合については、開示が認められている。ただし、オプトアウトや委託の場合の例外は認められていない。 データ使用者は、第三者への個人情報の開示に関する事項（目的及び開示する第三者を含む）を、通知に規定する必要がある。 また、データ使用者は、第三者への提供／開示を行った場合、当該提供／開示の相手方について記録の作成、管理を行う必要がある。 なお、マレーシア個人情報保護局（the Malaysian Personal Data Protection Department）は、センシティブ情報が存在しない限り、通知において、「データ主体が通知に対し問題を指摘し又は異議を述べない場合、同意があったとみなされる」旨の規定が明確に含まれている場合、黙示の同意を認める余地があることを認めている。もっとも、黙示の同意の概念が PDPA 上明示的に規定されているわけではないことには注意が必要である。
タイ	PDPA は、適用除外となる場合を除いて、第三者に対する個人情報の開示には同意が必要であると定めている。開示によって個人情報を受領する第三者は、当該個人情報をデータの主体が通知を受けた目的以外の目的のために利用・開示してはならない。 PDPA は、上記の要件に関して事業者に対する例外的な規定を特には定めていない。
フィリピン	データ主体には、データの共有に関する権利も認められている。これは、DPA IRR のセクション 3（f）で、データの管理者又は処理者から第三者への個人データの開示又は転送（開示又は転送がデータの処理者によって行われる場合は、データの管理者の指示に従う必要があります）として定義されている。これには、データのアウトソーシングや、管理者から処理者への個人情報データの開示又は転送は含まれない。データの管理者又は処理者が第三者へのデータの共有を行う場合、当該第三者が管理者又は処理者の関連会社であっても、事前に関連するデータ主体に通知し、同意を得る必要がある。さらに、データ共有が商業目的（ダイレクトマーケティングなど）である場合は、当該データを対象とするデータ共有契約を締結する必要がある。データ共有契約は、NPC の独自のイニシアチブによる調査や、データ主体から提出される苦情の対象となる。 また、データの管理者が個人データの処理を外部に委託するには、関連するデータ処理法の要件に基づいて処理が実行されることを保証する契約その他の法的行為の下でのみ行う必要がある。そのような契約又は法的行為は、NPC の独自のイニシアチブによる調査や、データ主体から提出される苦情の対象となる。
インドネシア	個人データの第三者提供は、原則としてデータ主体の事前の書面によるインドネシア語での明確な同意が必要である。ただし、裁判所の命令や捜査機関の要請があった場合には例外として同意が不要となる。なお、新しい個人データ保護法には GDPR に定められているようなデータ主体の同意が不要となる例外規定が導入される見込みである。 また、第三者に提供する際には個人データの正確性を検証し、データ主体にはどの個人データが機密情報であるかを特定する機会を付与しなければならない。
シンガポール	PDPA の別表 4 (Fourth Schedule) に掲げる例外事由（ある個人情報が、①公開されている場合、②公共の利益のために必要とされる場合及び③法令遵守のため必要となる場合等が含まれる。）に該当する場合を除いて、第三者に対する個人情報の開示には原則として当該個人の同意が必要となる。

(5) 個人情報の海外への移転に関する法律上の要件はどのようなものか。

ベトナム	国際的なデータ移転を明示的に定める規定はない。一般的に、第三者にデータを移転する要件は、上記(4)の回答で説明したとおりに適用される。
マレーシア	PDPA 上、以下の場合を除き、データ主体の個人情報を海外に移転することはできない。 • 当局が指定し公報に公表した地域に対して移転する場合（現時点で、当局が公式に指定している国は存在しない。） • データ主体の同意がある場合 • データ使用者が、以下の事項について信頼する合理的理由がある場合 ○ 当該海外移転が、データ主体に対する不利益行為を避け又は軽減するために行われること ○ 海外移転の際に、書面でデータ主体の同意を取得することが不可能であること ○ 同意を取得することが可能な場合、データ主体の同意があること • データ使用者が、PDPA に反した形での処理がなされないことを確保するために、必要なすべての合理的な予防策をとり、かつ調査を行った場合 • 海外移転がデータ主体の生命に関わる利益を保護するために必要な場合 • 海外移転が公益のために必要な場合
タイ	データ管理者が第三国に個人情報を送信又は移動する場合には、法令上の要件の遵守、契約上の義務の履行、法的主張の証明、行使又は弁護のための必要性等の法的な適用除外が存在する場合を除いて、当該個人情報の送信又は移動先となる当該第三国が個人情報保護に関して十分な基準を有していなければならない。
フィリピン	DPA 及び DPA IRR は、国外への個人データの送信及び処理を禁止していないものの、個人情報の処理がフィリピン国外で行われる場合であっても、DPA の規制は及ぶ。そのような場合、関係する個人情報管理者及び処理者は、上記(2)~(4)で述べた、DPA、DPA IRR 及び NPC の規則に従わなければならない。 さらに、DPA IRR のセクション 50 は、国外の第三者への外部委託によって処理される個人データに対して、データの管理者が適切な域外移転手続きを行う責任があることを強調している。
インドネシア	データ保護規制上、国外に個人データを移転する場合、電子システムのオペレーターは、データ移転に関する計画及びその結果の報告を行うなどして、MOCI と連携する必要がある。
シンガポール	個人情報の外国への移転は、①当該外国において個人情報の取扱い及び移転に関する法令が整備されており、かつ、②以下のいずれかに該当する場合に限って許容されている。 • 承認された標準契約条項が存在すること • 拘束力のある会社規則が存在すること • APEC 越境プライバシールール（CBPR：Cross Border Privacy Rules）システムの認証がなされていること • 同意、契約の履行、法律上の要求に係る履行又は防御等に係る逸脱行為が存在しないこと

(6) 事業者が保有する個人情報に関してデータ主体である個人が有する権利はどのようなものか。

ベトナム	データ主体は、データ管理者に自らの個人情報を提供するよう要求する権利を有する。また、データ主体は、自らの個人情報の収集、削除及び／又は破棄を要求する一般的な権利を有する。

マレーシア	一定の例外に当たる場合を除き、データ主体は、自己の個人情報へのアクセス権、訂正請求権、個人情報の処理に対する同意の撤回権を有する。 データ使用者は、所定の期間内にデータ主体からの要求に対応しなければならない。
タイ	PDPA は、データ主体がデータ管理者に対して自身の情報を精緻に、最新に、完全に、そして誤解を招かないようにするよう求めた場合で、データ管理者がこれらの要求に応えることができない場合には、データ管理者はデータの主体からの要求及びその要求へ対応しない理由を記録しなければならないと規定している。データの主体は、データ管理者の不応答について、個人情報保護委員会に対して、更なる行政手続を求めて不服を申し立てることができる。
フィリピン	(2)で述べたとおり、DPA の下では、データを提供した個人に対して、個人情報の修正又は誤った情報を削除する権利を与える必要がある。データ主体は、データ管理者への要求に応じて収集された情報にアクセスできなければならず、データの不正確さについて異議を申し立て、データを修正又は削除し、不正確又は不完全なデータ収集による損害を被った場合に補償を受ける権利がある。 さらに、データ主体はデータポータビリティの権利を有する。これは、データ主体が、個人データの管理者から、電子的又は構造化された形式（つまり、一般的に使用され、データ主体によるさらなる使用を可能にする形式）で、管理者によって処理中又は処理された個人データのコピーを得る権利である。
インドネシア	データ保護規則上、データ主体は下記の権利を有するため、事業者はこれに対応する必要がある。 • 個人データにアクセスし、又は個人データを修正若しくは更新する機会の取得 • 収集された個人データに関する履歴情報のリストの取得 • 個人データの削除の要請（ただし、関連性が失われた個人データに対してのみ認められ、これを証する裁判所の命令が必要である）
シンガポール	各個人は、事業者等に対して以下の事項を請求する権利を有する。 • 自己の個人情報へのアクセス権の付与 • 自己の個人情報に係る誤り又は不足の修正 • 自己の個人情報に係る収集、使用及び開示の中止 なお、個人情報の「開示」に係る請求に関して、シンガポールの個人情報保護法令では、現在のところデータ可搬性に係る権利は認められていない。ただし、プライバシー・データ保護委員会 (Privacy and Data Protection Commission) では、現在 PDPA にデータ可搬性に係る規定を導入することが検討されている。

(7) 個人情報の漏洩又は不正利用に関する報告義務はあるか。

ベトナム	データセキュリティ違反は、「サイバー情報セキュリティ事由」として LOCIS 上で広く定義されており、通達 20 号では、情報又は情報のシステムが攻撃され又は損害を受け、情報又は情報のシステムの整合性、機密性、有用性に影響する事由として定義される。サイバー情報セキュリティ事由が生じた場合、情報通信省及び他の関連する当事者は、緊急時対応を調整する必要がある。決定 5 号は、国の関連する情報システムが影響を受ける深刻なサイバー情報セキュリティ事由の報告及び対応の基本的な枠組み及び手続を規定している一方で、通達 20 号では、非サイバー情報セキュリティ事由への対応の手続を規定している。 通達 20 号において、関連する情報システムの事業者は、他者、関連するインターネットサービスプロバイダー及びベトナムコンピュータ緊急時対応チーム（VNCERT）に報告しなければならない。また、攻撃の兆候を発見した他の主体（情報システムの事業者ではない組織及び個人等）も他者、情報システム事業者及

	び VNCERT に速やかに通知しなければならない。
マレーシア	現時点では当局への通知義務はない。 もっとも、マレーシア個人情報保護局は、情報漏洩の際に、関係当局及び影響を受けるデータ主体に対して通知を義務付ける制度の新設に向けて準備を進めており、今後通知義務が課される可能性がある。なお、当該通知制度は 2018 年末には実施されると見込まれていたが、遅れており、現時点ではいつ実施されるのか不透明な状況である。
タイ	PDPA は、ある個人の権利若しくは自由に対して高度の危険性を課するものではない限り、データ管理者はデータの主体に対して当該個人情報の漏洩に関して漏洩から 72 時間以内に通知しなければならないと規定している。個人情報保護委員会により規定される数を超える特定個人の個人情報の漏洩がおきた場合には、データ管理者は個人情報保護委員会に対して当該破損及び適時に取られた回復措置を通知しなければならない。
フィリピン	DPA のセクション 20（f）に基づき、センシティブ情報又はその他のデータに関連するデータ侵害により、権限のない人物が特定の不正行為を犯す可能性があり、それによって影響を受ける個人への深刻な被害のリスクがあるとデータ管理者又は NPC が判断した場合には、当該個人への通知を行う必要がある。DPA IRR のセクション 38（a）に基づき、当該通知は、不正行為の発見又は不正行為が発生したと合理的に判断可能となった時点から 72 時間以内に行う必要がある。 DPA IRR のセクション 41 は、データ侵害が発生した場合、データの管理者に対して、上記の個人への通知の要件を満たしていない場合であっても、すべてのセキュリティインシデント及びデータ侵害の内容を詳細に説明する報告を行うことを要求している。当該レポートは、NPC からの要求に応じて提供する必要があり、レポートの概要を NPC に毎年提出する必要がある。
インドネシア	特に存在しない。
シンガポール	現在のところ、当局に対する情報漏洩又は個人情報の不正利用に係る報告義務は存在しない。しかし、近々当該規定の導入が見込まれている。

(8) ダイレクトマーケティングに関する個人情報保護の観点からの法規制はあるか。

ベトナム	データ主体とダイレクトマーケティングに従事することを計画するデータ使用者は、データ主体の事前の同意を取得しなければならない。事前の同意の要求は、明確に表明されなければならない。同意は、広告された情報、製品及びサービスの種類、特定の期間内に送信される広告メール／テキストメッセージの最大数と広告の送信時間を特定しなければならない。データ使用者は、データ主体が返答しないことから同意を推測することはできない。
マレーシア	ダイレクトマーケティングを行う場合、データ主体の同意が必要である。また、データ主体は、合理的な期間の経過後は、いつでも、データ使用者に対し、書面により、ダイレクトマーケティング目的での個人情報の使用の停止及び再使用の禁止を要求することが可能である。当該要求に従わない場合、企業は刑事責任を負う。
タイ	ダイレクトマーケティングは PDPA によって直接規定されているわけではないが、コンピュータ犯罪関連法（CCA: Computer Crime-related Act）等の他の法令が適用される。例えば、受信者が容易にオプトアウト若しくは配信停止できるような機会を与えないまま、不快な方法によりコンピュータデータ若しくは電子メールを他人に送信した者は処罰される。
フィリピン	DPA IRR は、DPA に基づくデータ処理に適用されるものと同様のデータプライバシー原則を、データプロファイリングにも拡張している。 DPA IRR のセクション 3（p）で定義されているように、データプロファイリングとは、業務パフォーマン

	ス、経済状況、健康状況などの個人に関する事柄を評価又は予測するための個人データの自動処理の形式を意味する。データ主体に対しては、プロファイリングのための個人情報データの処理の目的と範囲に関する特定の情報を提供する必要がある。データ主体は、自動化された意思決定とプロファイリングをもたらすデータ処理について通知を受ける権利を有し、当該データ処理に対して異議を述べる権利を有する。 さらに、(4)で述べた通り、データの共有が商業目的（ダイレクトマーケティングなど）である場合は、当該データを対象とするデータ共有契約を締結する必要がある。データ共有契約は、NPC の独自のイニシアチブによる調査や、データ主体から提出される苦情の対象となる。
インドネシア	特に存在しない。
シンガポール	当該規定は存在する。用いられるマーケティング手段にもよるが、原則として、事前のオプトイン若しくはオプトアウト、又は既存の取引関係に基づく黙示の承認をもって承諾の取得とすることができる。 電話勧誘販売との関係では、個人が電話勧誘販売業者からの電話を回避するために登録することができる勧誘電話拒否登録システムが、PDPC に基づいて設置されている。事業者等は、当該個人からの明確な同意がない限り、当該勧誘電話拒否登録システムに登録されている電話番号に対し、電話をすることができない。