西村あさひ法律事務所
NISHIMURA & ASAHI
個人情報保護・データ保護規制ニューズレター

Ⅰ. タイの個人情報保護法制と実務対応
Ⅱ. 個人情報保護・データ保護規制 各国法アップデート

2019年
11月29日号

Ⅰ. タイの個人情報保護法制と実務対応

執筆者:石川 智也

2020 年 5 月 27 日より、タイの個人情報保護法が本格的に適用開始となる。

タイの個人情報保護法は、一言で言うと GDPR の内容を多くの点で取り込んでおり、また、違反の態様によっては現地の責任者が身体拘束される刑事罰まであるため、タイに進出している日本企業の関心は非常に高く、既に多くの相談を頂いている。本稿では、タイの個人情報保護法制の概要と、日本企業が如何に取り組むべきかについて概説する。詳細については、当事務所において各種セミナーを開催しているので、そちらもご参照いただきたい。

1. タイの個人情報保護法の概要

(1) 地理的適用範囲

管理者または処理者がタイに所在する場合には、タイで処理が行われるか否かを問わず、個人情報の収集、利用または開示にタイの個人情報保護法が適用される。また、管理者または処理者がタイ国外に所在する場合であっても、①タイに所在するデータ主体に対する商品またははサービスの提供(支払いの有無を問わない)と、②タイ国内で行動するデータ主体の行動の監視を行う場合には、タイに所在するデータ主体の個人情報の収集、利用または開示にタイの個人情報保護法が域外適用される(域外適用の条文は、GDPR3 条 2 項と同じである。ただし、GDPR では前文で域外適用の解釈が示されていたのとは異なり、タイの個人情報保護法では特に解釈は示されていない)。そして、域外適用を受ける場合には、原則としてタイに「代理人」を設置しなければならないのも、GDPR と同様である。

簡単にいうと、タイの現地拠点においては規模の大小にかかわらずタイの個人情報保護法が適用される。また、日本企業についてもタイの個人に向けて商品・サービスを提供したり、何らか分析する目的でタイの個人の行動を監視したりする場合には、そのデータ処理についてタイの個人情報保護法が域外適用される。文言上は、GDPRと同じ域外適用のスコープを有するため、ウェブサイトで Cookie を利用してタイの個人の行動を追跡してしまう場合(ウェブサイトの訪問者を分析する場合や、ターゲティング広告を行う場合)にも適用され得る。しかし、域外適用については、GDPR 対応を行っている場合には、追加で対応が必要になる事項は多くないだろう。

(2) 適法性の根拠・同意・センシティブデータ

管理者は、個人情報の収集、利用または開示を行う場合には、原則として事前にまたはそれらの処理を行う際にデータ主体の同意を取得しなければならない。同意を取得していない場合には、所定の事由を除いて個人情報の収集、利用または開示を行うことができない。この所定の事由には GDPR の適法性の根拠（GDPR6 条 1 項）の内容が多く取り込まれており、契約の履行のために必要な場合、管理者または第三者の正当な利益のために必要な場合、管理者が服する法的義務を遵守するために必要な場合等には、同意を取得していなくても個人情報の収集、利用または開示を行うことができる。

同意の要件は 19 条で規定されており、文言上は GDPR と同様に厳格である。

また、センシティブデータの収集、利用または開示については要件が厳格化されており、原則として明示の同意（explicit consent）がなければ収集、利用または開示を行うことができない。また、同意なくして処理できることとなる例外事由も極めて限定的に規定されている。

(3) データ主体への情報提供

管理者は、データ主体が既に知っている場合を除き、個人情報の収集の前または収集の際に、データ主体に対して以下の事項の詳細を知らせる必要がある。

① 利用または開示される個人情報の収集の目的（同意によらない場合の収集の適法性の根拠を含む）
② 法律もしくは契約により、または契約締結のために個人情報を提供しなければならない場合であることの通知（データ主体が個人情報を提供しない場合に生じ得る影響の通知を含む）
③ 収集される個人情報とその保有期間（保有期間を特定できない場合には、具体的な保有基準に従った保有期間の見通し）
④ 個人情報が開示され得る個人または団体の類型
⑤ 管理者（代理人やデータ保護責任者がいる場合はそれらも含む）の情報、住所および連絡方法の詳細
⑥ 個人情報保護法上の、所定のデータ主体の権利

GDPR と比べると提供するべき情報の項目は少ないが、同意によらない場合の収集の適法性の根拠や保有期間の記載が求められるため、データマッピングを通じた個人情報の取扱状況の確認は必須である。

(4) データ主体の権利

GDPR と同様に、データ主体にアクセス権、データポータビリティ権、個人情報の取扱いに異議を唱える権利、削除権、個人情報の利用を差し控えるよう要求する権利、正確性等の維持を求める権利が認められており、対応期限などもある。そのため、GDPR 対応の際と同様に、データ主体の権利行使に耐え得るマニュアルを作成することが望ましい。

(5) 管理者の義務

管理者には、本ニューズレターにおいて別途掲げているもののほか、①情報セキュリティのための措置の実施、②第三者に個人情報を開示する場合における第三者の不当利用・開示を防止する措置、③個人情報を削除・破棄すべきときに削除・破棄する仕組みの構築、④データ漏えい等が生じた際の当局・本人への通知・連絡（後記(6)参照）、⑤域外適用を受ける場合の代理人の指名（前記(1)参照）が義務として課されている。

(6) データ漏えいが生じた際の当局・本人への通知・連絡

管理者は、GDPR と同様に、自然人の権利・自由にリスクを及ぼすおそれがないといえない場合には、個人情報保護委員会事務局に、不当な遅滞なく、可能な場合には気づいてから 72 時間以内に通知しなければならない。また、自然人の権利・自由に高いリスクを及ぼすおそれがある場合には、データ主体に、遅滞なくデータ侵害の事実と救済手段を連絡しなければならない。これらの通知や例外事由については個人情報保護委員会が公表する基準および手続に従う必要があるとされている。

対応としては、上記の基準および手続の制定動向を踏まえながら、GDPR 対応と同様に、データ漏えいが生じた際の当局・本人への通知・連絡を行うためのマニュアルを作成することになる。

(7) 記録義務

管理者は、GDPR と同様に、以下の事項を書面または電子的方法により記録しなければならない。

① 収集した個人情報
② 種類毎の個人情報の収集の目的
③ 管理者の詳細
④ 個人情報の保管期間
⑤ 個人情報にアクセスする権利および手段（個人情報へのアクセス権を有する個人に関する条件や、個人情報にアクセスする条件を含む）
⑥ 同意のない個人情報の利用または開示
⑦ データ主体からの要求や異議の拒否
⑧ 個人情報の適切なセキュリティ措置の説明

対応に当たっては、少なくとも、データ主体に提供すべき情報（前記(3)参照）と、これらの項目を網羅する形でのデータマッピングが必要になる。

(8) 処理者の義務

処理者には、本ニューズレターにおいて別途掲げているもののほか、以下の義務が課されている。

① 管理者の指示に従って個人情報を収集、利用または開示する
② 適切なセキュリティ措置を講じ、データ漏えい等を管理者に通知する
③ 個人情報保護委員会が規定する基準および方法に従って、個人情報の処理活動を記録する

また、管理者は、処理者との間で契約を締結し、個人情報保護法を遵守するための処理者の義務に従って処理者が活動を行うのを管理しなければならない。GDPR28 条 3 項と異なり、契約に規定するべき条項については、特に規定されていない。

(9) データ保護責任者

管理者または処理者は、以下の場合にデータ保護責任者を選任しなければならない。

① 管理者等の個人情報の収集、利用または開示における活動が、大規模であるため、個人情報の定期的な監視またはシステムを必要とする場合
② 管理者等の中心的活動がいわゆるセンシティブデータの収集、利用または開示である場合

データ保護責任者の選任が必要となる要件は、GDPR と類似しているものの、若干異なっている。特に、①については「中心的活動」の限定がかかっていない点、②については「大規模」の限定がかかっていない点で、GDPR よりもデータ保護責任者の選任が必要な場合は広くなる可能性があるのではないかと考えられる。

データ保護責任者の職務は、①管理者等とその従業員等への個人情報保護法の遵守に関する助言、②管理者等とその従業員等の法の遵守に関する調査、③個人情報保護委員会事務局との協力、④職務の過程で得た個人情報の秘密保持であり、GDPR と類似している。もっとも、タイの個人情報保護法においてはデータ保護影響評価が義務づけられていない（なお、Privacy by Design や Privacy by Default の規定もない）ため、データ保護影響評価への協力はデータ保護責任者の職務とされていない。

GDPR と同様に、データ保護責任者は従業員でも外部委託でも良いとされている。また、独立性が確保されており、職務を理由に契約を解消することはできず、職務実施時の問題は CEO に直接報告できる仕組みにする必要がある。

(10) 国外移転規制

管理者が外国に個人情報を移転する場合には、原則として当該移転先の外国が個人情報保護委員会が定める個人情報保護の基準に従った十分な個人情報保護の水準を備えている必要がある。もっとも、①グループで個人情報保護に関するポリシーを定め、それが個人情報保護委員会により認証された場合と、②個人情報保護委員会の定める基準と方法に従い、実効的な法的救済手段を含め、データ主体が自身の権利を行使することができる適切な保護措置を備えた場合には、この限りではない。①はGDPR にいう Binding Corporate Rules(BCR)類似の枠組みであり、また、②は Standard Contractual Clauses(SCC)類似の契約を想定しているのではないかと思われるものの、具体的な内容は明らかになっていない。

また、個人情報を受領する第三国における不十分な個人情報保護の水準について説明を受けた上でデータ主体が明示的に同意する場合や、データ主体が契約当事者である契約の履行のために必要な場合等にも、外国に個人情報を移転することができる。これらは GDPR の derogation(GDPR49 条 1 項)の枠組みを導入したものであるが、GDPR ではガイドラインによって derogation に依拠できる場合は限定的に解されている。タイの個人情報保護法においてどのように解されるのかは、今後の実務の動向を注視する必要がある。

(11) エンフォースメント

まず、民事責任については、裁判所は実損害の補償に加えて、その 2 倍までの懲罰的損害賠償を課すことができる。

また、刑事責任については、違反の態様によっては 1 年以下の禁固または 100 万バーツ(約 350 万円)以下の罰金が課され、これらは併科され得る。日本企業にとって脅威なのは、法人が違反者の場合で、取締役や個人情報の処理に責任を負う者の指示や行為の結果として違反が発生したときや、当該人物が義務を負う指示や行為を怠っていたときには、当該人物も処罰される旨が明記されている点である。

さらに、違反の性質に応じて 300 万バーツ(約 1050 万円)以下の課徴金が課され得る。センシティブデータに関する違反については、500 万バーツ(約 1750 万円)以下の課徴金が課され得る。

2. 日本企業が如何に取り組むべきか

タイの個人情報保護法には未だ不明確な点や、当局による基準または手続の制定に委ねられている点が少なくないが、それは対応を開始しなくて良いということを意味するものではない。

タイの個人情報保護法に対応するためには、GDPR と同様に、現地でどのような個人情報を取り扱っているか情報を収集する(いわゆるデータマッピングを行う)必要がある。この情報がそろっていなければ、今後当局が基準等を公表したとしても、施行日までに対応を間に合わせることができない。現地拠点の対応に際して、本社がどの程度サポートするのか、サポートするとしてどのような態勢で臨むのか早期に決定する必要がある。また、域外適用との関係では、少なくともタイの個人に向けて商品・サービスを提供している日本企業も対応は必須である。対応を行うか否かの検討のところで、施行までの残り時間を消費してしまうことのないようにしたい。

その上で、プライバシーノーティス、法定の要件を備えた同意書、法定の記録簿、処理者との間のデータ処理契約、越境移転規制に対応するためのドキュメント等の法定のドキュメントを整備するとともに、社内規則の整備、データ漏えい・データ主体からの権利行使に対応するための体制構築、データ保護責任者の選任、社内でのセミナー等による役職員への周知等のコンプライアンス態勢の整備を行っていくことになる。これらは、既に対応を開始することができるものもあれば、今後当局による基準の制定を待って対応することにならざるを得ないものもあるが、法律の施行日は決まっており、それに向けて取り組んでいく必要がある。

遅くとも年内には対応プロジェクトの方針について固めておくことが望ましいだろう。

Ⅱ. 個人情報保護・データ保護規制　各国法アップデート

執筆者：岩瀬　ひとみ、松本　絢子、石川　智也、河合　優子、松村　英寿、村田　知信

1.　日本

2019 年 10 月 8 日、総務省と経済産業省は、「情報信託機能の認定スキームの在り方に関する検討会　とりまとめ」および「情報信託機能の認定に係る指針　ver2.0」を公表した。情報銀行は、パーソナルデータの円滑な流通・利活用を実現するための仕組みとして注目される。詳細は、当事務所ロボット/AI ニューズレター2019 年 10 月 18 日号をご参照いただきたい。

2.　欧州

GDPR6 条 1 項(b)号に基づく個人データの処理に関するガイドライン

・　2019 年 10 月 8 日に行われた欧州データ保護会議（European Data Protection Board）の本会議において、「オンラインサービスの提供の文脈における GDPR6 条 1 項(b)号に基づく個人データの処理に関するガイドライン（Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects – version adopted after public consultation）」の意見募集後のバージョンが承認された。同ガイドラインは、どのようなデータ処理が「契約の履行のために必要」といえるかという点を具体例を交えて説明するとともに、「契約の履行のために必要」といえない場合に、どのような適法性の根拠に依拠してデータ処理を行うべきかといった点を説明している。

Equinix 社の Binding Corporate Rules（BCR）の承認

・　上記の欧州データ保護会議の本会議において、英国のデータ保護監督機関である ICO が提出した、Equinix 社の Binding Corporate Rules（BCR）の承認決定の草稿に関するオピニオンが採択され、同社の BCR が承認された。
BCR の申請手続は以下のような流れで行われるところ、本件は、GDPR の施行後、③の欧州データ保護会議による承認が行われた初の事例となる。

①　申請企業が主たる監督機関を指定し、GDPR 上の要件を満たす BCR をドラフトする
②　①の BCR ドラフトを指定した監督機関がレビューし、承認決定の草稿を作成する
③　②の承認決定の草稿を欧州データ保護会議がレビューし、承認する

これまで、欧州データ保護会議による承認が進まず、BCR の承認には数年を要すると言われていたが、欧州データ保護会議による承認プロセスが始まったことで、今後、GDPR の下で BCR の承認事例が増加する見通しであり、日本および EEA 以外の地域を含めグローバルに事業を展開する企業においては、域外移転の枠組みとして BCR の申請を検討することも考えられる。

3.　中国

2019 年 10 月 26 日に中華人民共和国暗号法が公布され、2020 年 1 月 1 日より施行される。同法は、暗号産業の発展を目的に、暗号の定義や事業者のルール、違反行為に対する罰則などを定めたもので、2019 年 7 月 5 日に公表された法案から大きな変更はない。施行日が迫っていることから、中国において暗号製品・サービスの提供・使用をしている企業は法令遵守に向けて早急に対応を進める必要がある。

4.　シンガポール

2019 年 10 月 9 日、Personal Data Protection Commission (PDPC)は、“Advisory Guidelines on Key Concepts in the PDPA”

のうち、第 6 章の “Organisations” および第 15 章の “Access and Correction Obligations” の内容を改訂した。第 6 章の改訂は、個人データをシンガポール国外に移転する際の、組織およびデータ仲介者の義務を明確化するものであり、第 15 章の改訂は情報開示請求を拒否できる場合を明確化するものである。また、同日、 “Advisory Guidelines On The Personal Data Protection Act For Selected Topics” も改訂され、新たに個人データをクラウドサービスを介してやり取りする場合の、事業者およびクラウドサービスプロバイダーの責任を明確化する章が追加された。

5. インドネシア

電子システムおよび取引の実施に関する 2019 年政令第 71 号が 2019 年 10 月 10 日に施行され、2012 年政令第 82 号が失効した。従前は、公共サービスを提供する場合には、インドネシア国内にデータセンターおよびリカバリーセンターを設置することが義務づけられていたが、公共サービスの具体的な意義が明らかでなく、通信情報省によって広く解される傾向にあった。本改正により、公的電子システム事業者のみが電子システムおよびデータをインドネシア国内に置くことが要請され、民間の電子システム事業者はインドネシア国外にも電子システムおよびデータを置くことができることが明確にされた。

6. スリランカ

スリランカの The Ministry of Digital Infrastructure and Information Technology は、2019 年 9 月 24 日に個人データ保護法の最終草案を公表した。この法案は議長による認証日から 3 年以内に施行される。OECD Privacy Guidelines や APEC Privacy Framework、欧州評議会条約、GDPR、CCPA、その他の国の法令など、国際的なベストプラクティスを考慮して策定された。最終草案ではデータ管理者の登録義務は削除されたが、代わりに「データ保護管理プログラム」と呼ばれる内部統制・手続の実施に関する透明性・説明責任が導入されている。GDPR と同様の域外適用規定が設けられており、適用を受ける企業は法令遵守に向けた対応の準備を始めることが望ましい。

7. ケニア

ケニア政府は、個人データ保護法の最終草案を 2019 年 11 月 8 日に承認した。現時点では施行日は不明であるが、GDPR を基に策定されており、ケニアでビジネスを行う企業のほか、域外適用を受ける企業については法令遵守に向けた対応の準備を始めることが望ましい。

岩瀬（いわせ） ひとみ
西村あさひ法律事務所　パートナー弁護士
h_iwase@jurists.co.jp

1997 年弁護士登録、2004 年ニューヨーク州弁護士登録。1994 年早稲田大学法学部卒業、2003 年スタンフォード大学ロースクール卒業(LL.M.)。知財/IT 関連の各種取引や争訟(特許関連訴訟、商標関連訴訟、システム関連紛争等)を主に扱う。IT 分野では、国内お外国が絡む、様々な局面における個人情報・データ関連の規制その他の問題や、クラウド、AI、IoT 等新しい技術を用いたビジネスに絡む各種法律問題についてアドバイスを行う。

松本（まつもと） 絢子（あやこ）
西村あさひ法律事務所　パートナー弁護士
a_matsumoto@jurists.co.jp

2005 年弁護士登録、2013 年ニューヨーク州弁護士登録。2012 年ノースウェスタン大学ロースクール卒業(LL.M.)後、2012-2013 年ニューヨークの米国三菱商事会社および北米三菱商事会社に出向。国内外の M&A や企業組織再編のほか、コーポレートガバナンス、コンプライアンス、情報管理、ブランド戦略、保険等に関連する企業法務一般を幅広く扱う。情報管理関連では、個人情報や営業秘密、知財、インサイダー取引規制等に関する法律問題や、AI・クラウドに絡む法律問題等についてアドバイスを提供している。情報法制学会会員。

石川（いしかわ） 智也（のりや）
西村あさひ法律事務所　パートナー弁護士
n_ishikawa@jurists.co.jp

2006 年弁護士登録。2005 年東京大学法学部卒業、2015 年バージニア大学ロースクール卒業(LL.M.)、2016 年ミュンヘン知的財産法センター卒業(LL.M.)、Noerr 法律事務所ミュンヘンオフィスに出向、2017 年ニューヨーク州弁護士登録。グローバルでの個人情報保護法制・データ規制へのコンプライアンス対応について多くの日本企業にアドバイスを提供。特に、GDPR 対応については 150 社を超える日系企業へのアドバイス経験を有し、関連する講演・執筆記事も多数。情報法制学会会員、Certified Information Privacy Professional/Europe(CIPP/E)。

河合（かわい） 優子（ゆうこ）
西村あさひ法律事務所　パートナー弁護士
y_kawai@jurists.co.jp

2006年弁護士登録。2013年コロンビア大学ロースクール卒業(LL.M.)、2014年ニューヨーク州弁護士登録。
M&A、ジョイントベンチャー、データ関連法制、ライセンス・電子商取引その他企業法務全般について、クロスボーダー案件を中心に数多く担当。日本の個人情報保護法制については、多国籍企業を含む国内外の企業・組織をクライアントとし、データの域外移転や医療・遺伝子関連データの取得等を含む多岐に渡る問題点について、多くのアドバイスを継続的に提供。情報法制学会会員。一般社団法人遺伝情報取扱協会監事。

松村（まつむら） 英寿（ひでとし）
西村あさひ法律事務所　弁護士
h_matsumura@jurists.co.jp

2002 年弁護士登録。M&A、アライアンスをはじめとするコーポレート分野全般、AI・データの利活用や自動運転・MaaS 等の新たなモビリティサービスに関する案件、スタートアップ支援等、幅広い業務に従事。著書は、『データ取引の契約実務』(商事法務・2019)、『データの法律と契約』(商事法務・2019)、『AI の法律と論点』(商事法務・2018)等多数。

村田（むらた） 知信（ともぶ）
西村あさひ法律事務所 ホーチミン事務所　弁護士
to_murata@jurists.co.jp

2010 年弁護士登録、2018 年カリフォルニア大学ロサンゼルス校ロースクール卒業(LL.M.)後、ロンドンの知財ファームである Bristows LLP に出向。2019 年からベトナム外国弁護士に登録してホーチミンオフィスで勤務し、ベトナム、タイ、シンガポール等を含む東南アジアのサイバーセキュリティー、データ保護等の IT 関連規制や IT・知的財産に係る取引・紛争を中心にアドバイスを提供している。基本/応用情報技術者試験合格、情報処理安全確保支援士登録(2019 年)。

（当事務所の連絡先）　東京都千代田区大手町 1-1-2 大手門タワー 〒100-8124
Tel: 03-6250-6200 (代) Fax: 03-6250-7200
E-mail: info@jurists.co.jp　URL: https://www.jurists.co.jp