Deloitte.

Centre for
Regulatory Strategy
Asia Pacific

AIにかかわるデータプライバシー：
リスク・倫理的課題とイノベーションとのバランス

2025年10月
デロイト トーマツ サイバー合同会社

***このレポートはAIを使って英語から日本語に翻訳されています。**

本レポートの構成

アイコンをクリックすると、各セクションに移動できます。

はじめに

人工知能(AI)の利活用におけるデータプライバシー　は、イノベーションと倫理の間のバランスをどのように図っていくかについての試金石の一つと言えます。

AIにかかわる技術は前例のないペースで進歩していて、それが効果的に機能するために膨大な量の個人データに依存しており、個人データがどのように収集され、利用され、保護されるかについて大きな懸念が生じています。

AIにかかわる技術は、インターネットの普及とデジタルデータの収集・保存の時代を通じて長年見られてきたプライバシーの懸念をさらに深めます。AIが他と一線を画しているのは、データに対する莫大なニーズとそのプロセスの不透明さであり、収集される個人データやその利用方法、また修正や削除に関するユーザーのコントロールはさらに弱まっています。今日のデジタル環境では、個人はオンライン上で追跡されるのを避けることは難しくなっており、AIの台頭はこれらの課題をさらに深刻化させる可能性があります。

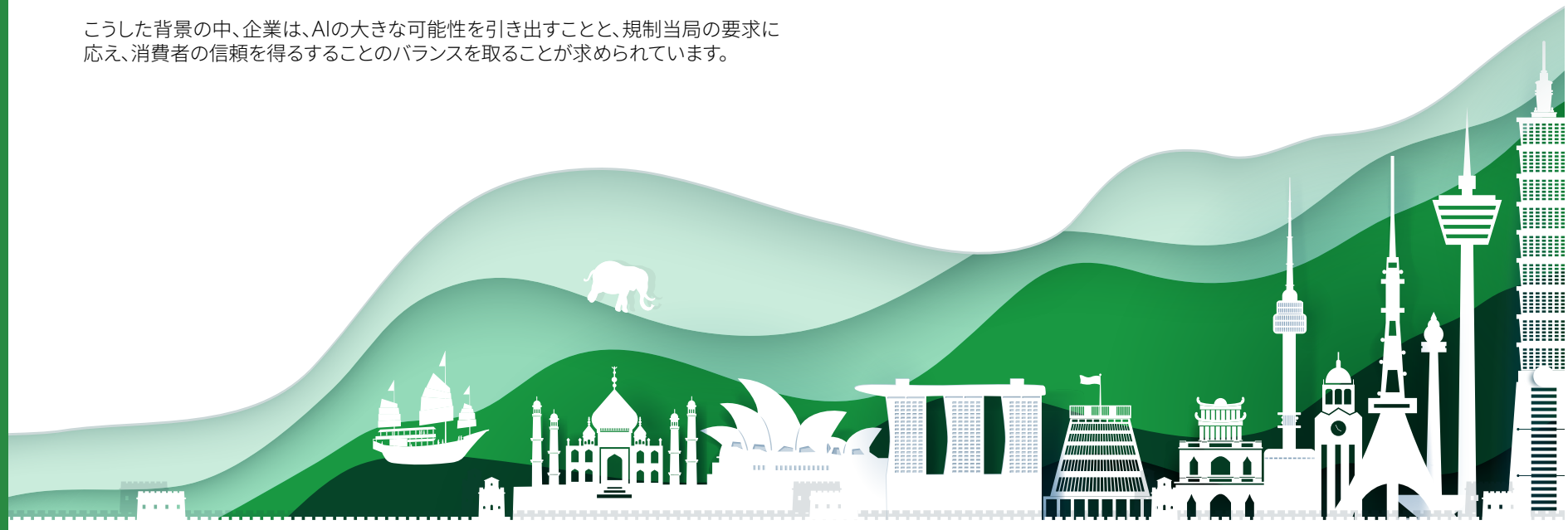
ChatGPTやスマートホームデバイスなどの会話型ツールから、ヘルスケア診断や顔認識に使用される高度なアプリケーションまで、AIシステムはユーザーやその他多くの人々の両方からのデータをもとにモデルを改良し、出力結果を生成します。しかしながら、プライバシーにかかわる保護がなければ、こうしたデータは不適切に利用される可能性があり、企業を重大なレピュテーションのリスクやレギュレーションのリスクにさらす可能性があります。そのため、AIデータのプライバシーの問題は、世界中の政策立案者、開発者、その他のステークホルダーにとって重要な焦点となっています。

こうした背景の中、企業は、AIの大きな可能性を引き出すことと、規制当局の要求に応え、消費者の信頼を得るすることのバランスを取ることが求められています。

このレポートでは、AIにかかわる規制上の問題としてデータプライバシーに焦点を当て、上記の2つの期待を同時に満たそうとするときの課題を明らかにしようとしています。[1]私たちは、アジアパシフィック (AP) 地域における現在のデータプライバシーの状況と、特定のデータにかかわるAIの要件を分析し、ステークホルダーが責任を持って効果的にエコシステム創り出すのに役立てていただくための洞察や実用的な方策を示すことを目的としています。

消費者の懸念

データ保護に対する消費者の懸念は、AIの利活用において重要な指標になります。[2] オンラインおよびデジタルサービスのメリットがデータ保護のリスクを上回ると考えている消費者は、わずか半数だったという調査結果もあります。[3]Deloitteの”State of Ethics and Trust in Technology Annual Report”(第3版) によると、米国の技術専門家と企業の回答者の72%が、データプライバシーをトップ3の懸念事項の1つに挙げており、回答者の約40%が最大の懸念事項とされています。[4]さらに、消費者の約62%は、AIの使用が倫理的であると考える企業をより信頼しており、そのような製品には追加料金を支払ってもよいと考えていると示されています。[5]一方で、オーストラリアの消費者の間では、悪意を持ったアクターによる個人データの利用と個人データのプライバシーに関する懸念が、生成AI (GenAI) に関連する2つの最も重要な問題として浮上しており、回答者の約65%がこれらの問題を主な懸念事項として挙げています。[6]AIの利用においてデータプライバシーに適切に対処することは、消費者の信頼を高める上でますます重要になっています。



データプライバシーにかかわる規制の概況

データプライバシーにかかわる規制においては、EUにおける一般データ保護規則(GDPR)の導入が、その進展の大きな契機になりました。[7]

GDPRは、場所に関係なく、特定の状況があればEUに所在する人のデータを取り扱うすべての企業に適用され、データの収集、利用、保護に関する厳格な制約を課します。主な特徴には、拡充されたデータ主体の権利や、徹底した説明責任、違反に対する厳しい罰則などがあり、主要なグローバル標準となっています。また、GDPRでは、データ処理活動の記録の保持、規制当局へのデータ侵害の迅速な報告、特定のケースにおけるデータ保護責任者の指名など、その他の厳格な要件も導入しており、これらの義務により、企業企業はコンプライアンス・プロセスを確立、レビューし、実証する必要があります。

GDPRは、データプライバシーの文脈において先駆的な規制であり、他の地域や国の規制当局がそれを踏まえて新しい規制を導入したり、既存のフレームワークを更新したりしています。さらに、GDPRは「ブリュッセル効果」の顕著な例であり、域外においても、データを利活用する事業者に影響を与えていて、大規模なグローバル企業では、効率性と相互運用性を高めるために、業務全体にわたってこれらのルールを採用するケースも増えています。GDPRはAIに特化した規制ではありませんが、AI技術を利用する企業に特に関連するいくつかの重要な要求事項を定めています。

データプライバシーとAIの規制は世界的に急速に進化しており、個人データ保護を強化するためにアジア太平洋地域全体で重要な措置が取られています。例えば、オーストラリアでは、増加するデータ侵害に対処し、子どものオンラインプライバシーを強化するために、2024年プライバシーおよびその他の法律改正法案が導入されました。中国本土（以降「中国」）の個人情報保護法（PIPL）とデータセキュリティ法（DSL）は、データ保護と国家の安全保障のための包括的な基準を定めています。シンガポールと香港はAIに関する詳細なガイドラインを発表し、透明性と倫理的配慮を強調しています。日本、韓国、台湾（中国）（以降「台湾」）は、強化されたセキュリティ対策と柔軟なデータ処理ルールを含むようデータ保護法を更新しました。インドのデジタル個人データ保護法（DPDP）とDPDP規則は、データ保護とコンプライアンスのための堅牢なフレームワークの確立を求めています。インドネシア、マレーシア、フィリピン、ベトナムも、国際的な整合性を確保しながら、現代の課題に対処するために、データ保護法を強化しています。これらの取り組みは、イノベーションとデータ保護のバランスをとり、国際協力を促進するというコミットメントの高まりを反映しています。さらに、ほとんどの制度では、個人データに関する権利を個人に付与し、データ管理者や処理者に個人データの適切な保護及び管理を要求する要求事項を含んでいます。

しかし、AI特有の考慮事項をデータプライバシー規制の枠組みに組み込むアプローチは大きく異なります。香港、シンガポール、韓国など、AI開発の促進に重点を置いている一部の法域では、データプライバシーの規制との関連で、AIに特化したガイダンスを積極的に公開しています。対照的に、アジア太平洋地域の他の国では、一般的なデータプライバシー規制の確立と強化に重点を置いています。これらのフレームワークはAIの利用に特化したものではなく、AI技術を導入する企業は包括的な規制要件に準拠する必要があります。

さらに、規制における要求事項が項目レベルで一致していても、特定の同意要件や、侵害報告の期限、データの保存と移転にかかわるルールにおいて重要な相違が残る可能性があります。中国、韓国、インドネシアなどの一部の地域では、データローカライゼーションが、クラウドサービスの利用とコンフリクトを起こす可能性があります。複数のソースから日常的にデータを取り込んで処理するAIモデルは、小さなコンプライアンス上のギャップを重大なレギュレーションリスクにすぐに変えてしまう可能性があります。例えば、企業地域の規制によって明示的に禁止されている場所に、意図せず個人データを保存することが挙げられます。つまり、データを保存する目的でサードパーティのサービスを使用することにより、企業がデータの保存場所を正確に把握することが難しくなるという問題です。

近年のAI開発の急速なペースを踏まえ、AIを利用する企業は、堅牢なデータプライバシーフレームワークを整備・運用し、規制違反を防止して、個人データを倫理的かつ合法的に扱うための適切なガバナンスと監視を確保する必要があります。

アジア太平洋地域における**データプライバシーの要求事項**

	執行・罰則	AIにかかわる特定のガイドラインや要求事項	域外適用	越境移転にかかわるルール	データ保護責任者(DPO)にかかわる要求事項	データローカライゼーションにかかわるルール*	機微な個人情報の分類**	子供のデータ保護にかかわるルール	本人の権利
オーストラリア	✔	✔	✔	✔	✖	✖	✔	✔	✔
中国	✔	✔	✔	✔	✔	✔	✔	✔	✔
香港特別行政区	✔	✔	✖	✔	✖	✖	✔	✔	✔
インド	✔	✖	✔	✔	✔	✖	✖	✔	✔
インドネシア	✔	✖	✔	✔	✔	✔	✔	✔	✔
日本	✔	✖	✔	✔	✖	✖	✔	✖	✔
マレーシア	✔	✖	✔	✔	✔	✖	✔	✔	✔
ニュージーランド	✔	✔	✔	✔	✔	✖	✔	✔	✔
フィリピン	✔	✔	✔	✔	✔	✖	✔	✔	✔
シンガポール	✔	✔	✔	✔	✔	✖	✔	✔	✔
韓国	✔	✔	✔	✔	✔	✔	✔	✔	✔
台湾	✔	✖	✔	✔	✖	✖	✔	✔	✔
タイ	✔	✖	✔	✔	✔	✔	✔	✔	✔
ベトナム	✔	✖	✔	✔	✔	✔	✔	✔	✔

*オーストラリアなど、いくつかの国・地域では、包括的なデータローカライゼーションのルールが見られませんが、ヘルスケアなどのセクターによっては、データ主権にかかわる特定の規制があります。
**機微な個人情報とは、例えば健康や雇用、教育、刑事司法、個人の財務状況などの情報を指します。

域外適用
データプライバシー規制における重要な特徴の1つは、もとの管轄区域の境界を越えて規制が適用される域外適用の原則です。GDPR第3条では、EU域内に設立された企業企業だけでなく、EU域内の個人に商品やサービスを提供したり、個人の行動を監視したりするEU域外の企業にも規制が適用されます。これは、日本を含め世界の他の場所にある企業が、EUに所在する人の個人データを処理する場合、データ処理が物理的に行われる場所に関係なく、GDPRに準拠しなくてはならないケースがあることを意味しています。この域外適用の範囲は、データフローのボーダレスな性質を踏まえ、EUの人のデータがどこに移動しても保護されるように設計されています。

域外適用の原則はヨーロッパに特有のものではなく、アジア太平洋地域の規制当局においても採用が増えています。例えば、シンガポール国内の個人に商品やサービスを提供する過程で個人データを収集または処理する場合、シンガポールの個人データ保護法 (PDPA) は、シンガポール国外の企業にも適用される可能性があります。同様に、韓国の個人情報保護法 (PIPA) と日本の個人情報保護法 (APPI) には、自国内のデータを取り扱う外国の企業にも適用範囲を拡大する条項が見られます。こうした傾向は、データプライバシーが国境を越えて維持されなければならないことについて、世界的な認識が広がっていることを示しています。これは、多国籍企業にとって、コンプライアンスへの取り組みが各地域・国に限定されなくなったことを意味してます。データプライバシーにかかわるガバナンスに対して包括的で国境を越えたアプローチは、世界中の規制当局の期待に応えるために不可欠な要素になっています。

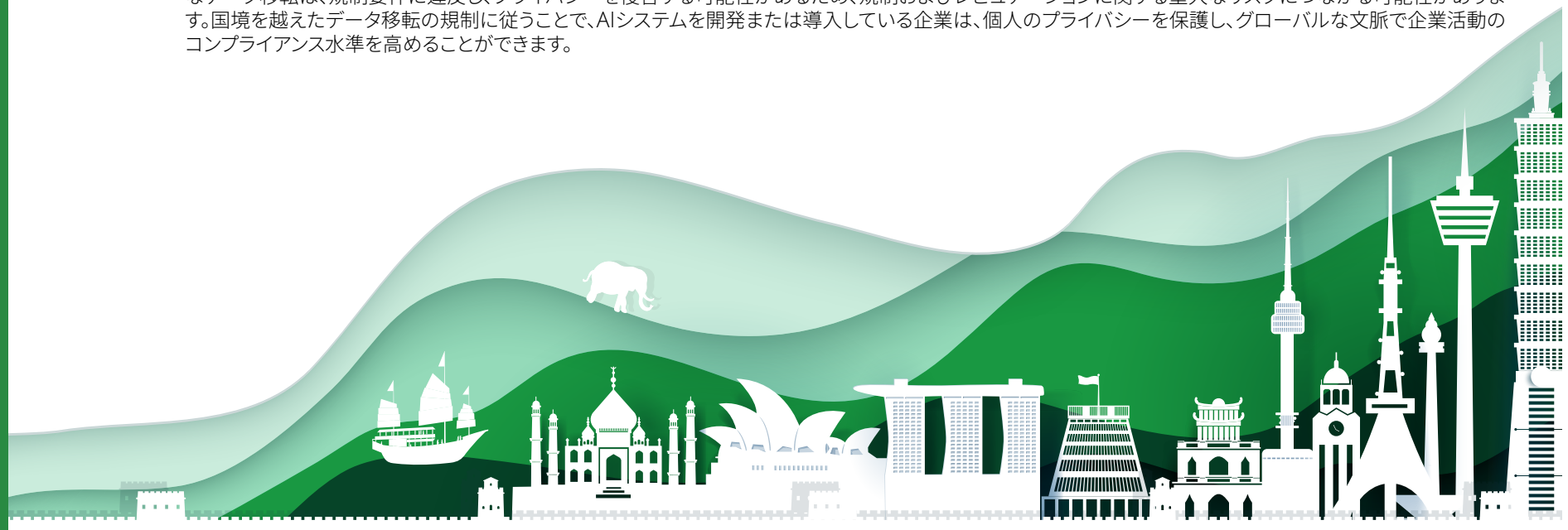
データプライバシーに関する主な課題

同意

個人データの合法的、公正かつ透明な処理を求める規制は、同意の概念を有することが多く、AIの利用との関連性が高いと言えます。AIを導入する企業は、個人から明示的な同意を得るなど、規制で示された根拠をもとに個人データを処理する必要があります。これは、センシティブな情報を推測したり、個人に影響を与える自動決定を行ったりする可能性のあるAIシステムにとって特に重要になります。コンプライアンスを維持するために、企業は顧客のデータがどのように管理されるかを明確かつオープンに伝え、個人がその情報を得たうえで、データを削除する権利を行使できるようにする必要があります。さらに、同意を得る際には、企業はデータがどのように利用されるかを明確にする必要があり、特にセンシティブな情報を取り扱う場合や、リスクが高いと考えられるAIのユースケースを扱う場合には、広範で曖昧な、または一括した同意を要求することは避けるべきと考えられます。また、情報が誤用されたり、当初の意図を超えてAIのトレーニングに転用されたりすることを防ぐために、堅牢な保護措置を講じる必要もあります。新たな目的のためにデータを利用するにあたって、あるいはAIシステムの目的やアウトプットの変更において、企業はそのようなデータの利用が最初に提示した目的と一致しているかどうかを評価することも重要です。また、ユーザーに対する透明性を維持し、必要に応じてユーザーの同意を再評価し、更新する必要もあります。企業はまた、サードパーティのAIサービスの提供者が、データプライバシーの義務と利害関係者の期待に沿って、データ主体の同意を取得して管理するための堅牢なメカニズムを備えていることを目にすることもあるでしょう。これらの原則をAIシステムの導入時に合わせて組み込むことで、企業は不適切なデータ利用のリスクを軽減し、個人のプライバシーと自主性の尊重を示すことができます。

国境を越えたデータ移転

多くのAIシステムがグローバルなデータフローに依存しており、複数の地域にまたがるデータを処理することが多いため、国境を越えたデータ移転の規制は、AIの利活用と密接に関連しています。これらの規制では、企業は、管轄区域外、もとの法域と特に同等のプライバシー規制がない場所に移転された個人データが適切に保護されることを確実にする必要があります。AIアプリケーションの場合、企業はデータがどこに保存され、処理され、アクセスされるかを評価し、データをエクスポートする際の保護プロセスを確立することが求められます。さらに、ほとんどの地域では、センシティブデータ(健康状態や生体認証、金融にかかわるデータなど)とそうでない個人データを区別したり、未成年者に対してより厳しいプライバシー要件を設けたりしています。そのため、これらの種類のデータセットの国境を越えた移動には、追加的な制限が課されることもあります。同様に、特定の地域では、健康状態にかかわるデータなど、特定の種類のデータに対してデータローカライゼーション要件が適用されます。これらの規制は、AIモデルの初期設計時に十分に理解し、導入後に定期的に確認する必要があります。不適切なデータ移転は、規制要件に違反し、プライバシーを侵害する可能性があるため、規制およびレピュテーションに関する重大なリスクにつながる可能性があります。国境を越えたデータ移転の規制に従うことで、AIシステムを開発または導入している企業は、個人のプライバシーを保護し、グローバルな文脈で企業活動のコンプライアンス水準を高めることができます。



データの最小化

データの最小化は、データプライバシー規制の中核的な要素であり、GDPRでは、個人データの収集が「適切であり、関連性があり、かつ、処理の目的に関連して必要なものに限定されていること」と定義されています（第5条（1）(c)）。[8]さらに、保管制限の原則に従って、企業は目的を達成するために必要な期間のみ個人データを保持し、その後は速やかに削除しなければなりません。また、データ最小化の規制により、企業は、特定の目的を達成するために必要な個人データのみを収集し、処理することも求められます。企業がAIを利用する場合、こうした原則は特に重要になります。AIシステムはトレーニングや運用に大規模なデータセットを必要とすることが多く、不必要または過剰なデータ収集のリスクを高める可能性があるからです。データ最小化を実現するために、AIを利用する企業は、収集するデータの種類と量を慎重に評価して正当化し、不適切な情報や過剰な情報を収集しないようにしなければなりません。データ最小化の原則に従うことで、企業はプライバシーを強化し、個人の権利を侵害する可能性の低いAIソリューションを構築できるようになります。この点で、AIモデルは最初から明確で具体的な目標を念頭に置いて設計されるべきであり、すべてのデータ入力がその目標に直接関連することを確実にする必要があると考えられます。ただし、このアプローチは、広範な機能を実現するために膨大で多様なデータセットでトレーニングされる汎用AI（GPAI）モデルには課題をもたらします。GPAIモデルの有効性は、多くの場合、トレーニング中に大規模で詳細なデータにアクセスできることに依存しているため、厳密なデータの最小化はGPAIモデルの有用性を制限することにもつながります。そのため、データの最小化は、焦点を絞ったAIシステムには適していますが、GPAIのオープンエンドの性質とは本質的には相容れないことも考えられます。

求められる対応の例

これまで述べてきた点も踏まえ、企業におけるAIの利活用において重要な点を挙げます：

現在の規制の要求事項をもとに設計段階でコンプライアンスを確保すること。AIシステムはまた、新しい要求事項に適応するために柔軟であること

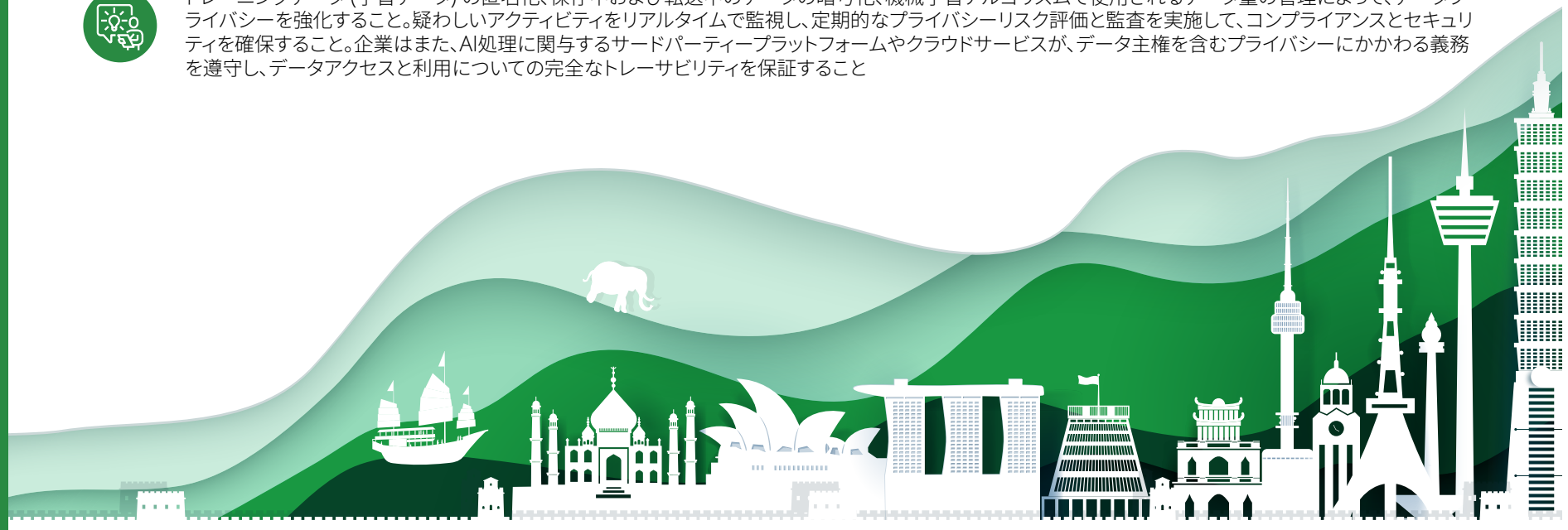
データプライバシーの規制と業界のベストプラクティスに沿ったAIツールと機能を開発するために、企業内の専門知識と能力に投資すること

データを必要以上に長く保存せず、不要になった時点で適切に廃棄することを確実にするために、AIデータのアーカイブと破棄に関するポリシー、プロセス、管理を確立すること

AIにかかわるリスク管理の文化を醸成するために、AIの利活用に関連するデータプライバシーの重要性について社内の意識を高めること

データ収集からモデルの展開までのAIライフサイクルにプライバシーバイデザインを組み込むこと。各AIモデルまたはユースケースの目的と成果を明確に定義すること

トレーニングデータ (学習データ) の匿名化、保存中および転送中のデータの暗号化、機械学習アルゴリズムで使用されるデータ量の管理によって、データプライバシーを強化すること。疑わしいアクティビティをリアルタイムで監視し、定期的なプライバシーリスク評価と監査を実施して、コンプライアンスとセキュリティを確保すること。企業はまた、AI処理に関与するサードパーティープラットフォームやクラウドサービスが、データ主権を含むプライバシーにかかわる義務を遵守し、データアクセスと利用についての完全なトレーサビリティを保証すること



個人データがどのように使用されているかに関する個人の懸念に積極的に対処し、消費者および主要なステークホルダーとの信頼を構築すること。AIシステムで使用するためにデータがどのように収集され、アクセスされ、保存されているかを記載したレポートを公開すること

AIシステムが将来のデータプライバシー規制に準拠していることを確認するために、継続的な監視を行うこと。監査可能性と説明責任をサポートするために、データアクセスとAIモデルの利活用に関する詳細なログを保持し、プライバシー規制への準拠を示すことができるようにすること

包括的なAIガバナンスのフレームワークを企業内に導入すること。DeloitteのTrustworthy AI Frameworkは、高度な技術力と最先端のガバナンスプラクティスを組み合わせた一連のサービススイートであり、AIを効果的に導くのに役立ちます

サードパーティのサービスを利用すること、またはオンサイトデータストレージソリューションに投資することのメリットを評価すること。複数リージョンのデータに依存するAIトレーニング用のデータセットまたは推論パイプラインを利用する場合、移転影響評価 (TIA) も含めた越境移転にかかわる対応を行うこと

結論として、企業は、データプライバシーを事後のコンプライアンスとして扱うのではなく、中核的な設計の原則として組み込んだAI戦略を採用すべきと考えられます。このアプローチは、安全なイノベーションを可能にし、ステークホルダーの信頼を維持し、レピュテーションリスクとレギュレーションリスクの両方を軽減することになります。

最終的には、データプライバシーをAIにかかわる議論の中心に据え、倫理とコンプライアンスの文化を醸成することで、企業の経営層は、責任があり信頼できるリーダーシップを示しながら、AIによる価値創造を目指すことができるようになります。

地域・国ごとの詳細

AIにかかわるデータプライバシー規制のアプローチと成熟度は、地域・国によって違いが際立っています。ただし、アジア太平洋の各法域において導入されているデータプライバシー規制は、EUのGDPRなどの他の規制が持つ主要な規範を含んでいます。これには、データ主体の権利の確立、データの最小化や目的の制限などの原則、国境を越えたデータ移転の管理などが含まれます。

このセクションでは、アジア太平洋地域におけるデータプライバシー規制の現状と、それらがAIとどのように関連しているかについて整理します。

オーストラリア

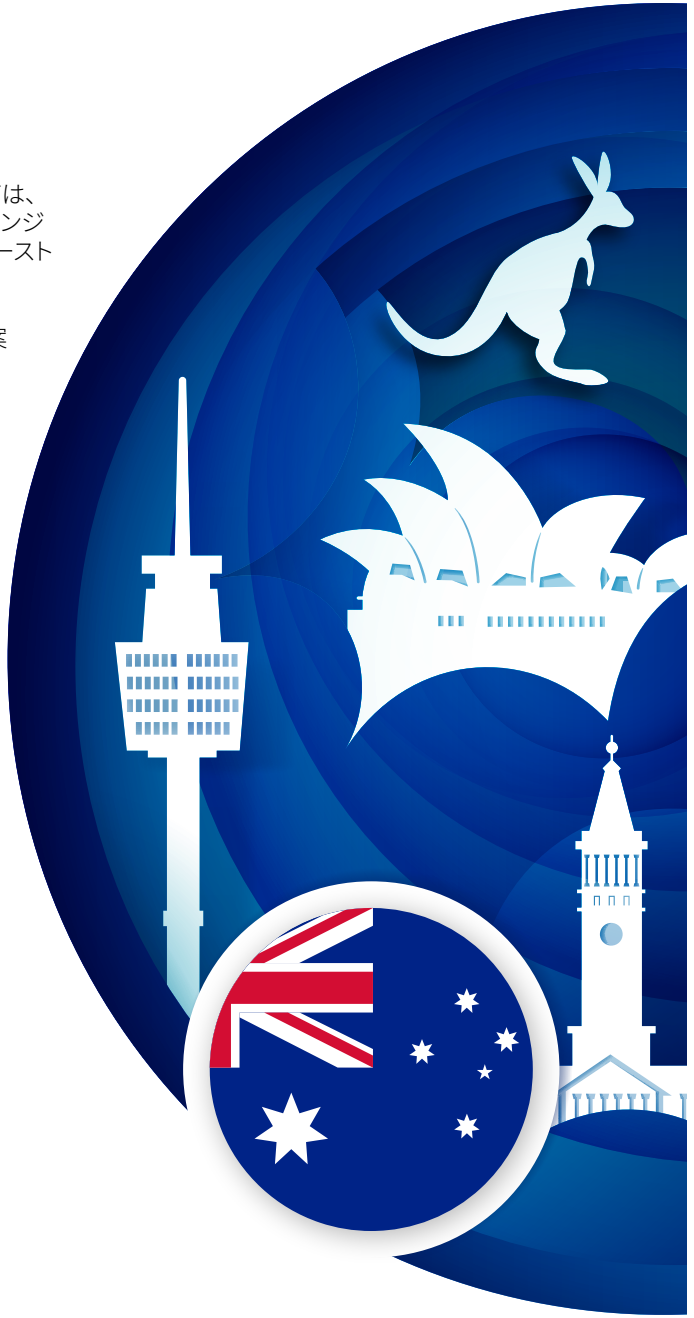
データプライバシーは、オーストラリア国内でますます重要なトピックになっています。

2025年5月、オーストラリアの当局 (Australian Office of the Australian Privacy Commissioner: OAIC)*は、企業と政府機関が1,100件以上のデータ侵害を報告したと発表しました。その中でフィッシングとソーシャルエンジニアリング/なりすましが、データが盗まれた主な方法として挙げられています。また、医療サービス提供者とオーストラリア政府は最も頻繁にデータ侵害を通知した、とされています。

オーストラリア政府は、2024年12月10日に国王の裁可を受けたプライバシーおよびその他の法律の改正法案2024 (以下「法案」) の導入を通じて、データプライバシー規制の強化を優先事項としています。この法案は、現代の要求に沿ったデータプライバシー規則とオーストラリアプライバシー原則 (APPs) を更新した1988年プライバシー法の導入に続く、より広範なデータプライバシーフレームワークの更新の一部を形成することになります。

法案の主な特徴は次のとおりです:

- ドキシング (個人の身元を特定できる情報を、本人の許可なくインターネット上などで暴露・公開する行為) を犯罪として明示
- 重大なプライバシー侵害の禁止
- 自動意思決定 (ADM) システムに関するポリシーの強化
- OAICによる若年者のオンラインプライバシー規範の制定
- 海外における個人データの開示に対する保護を提供

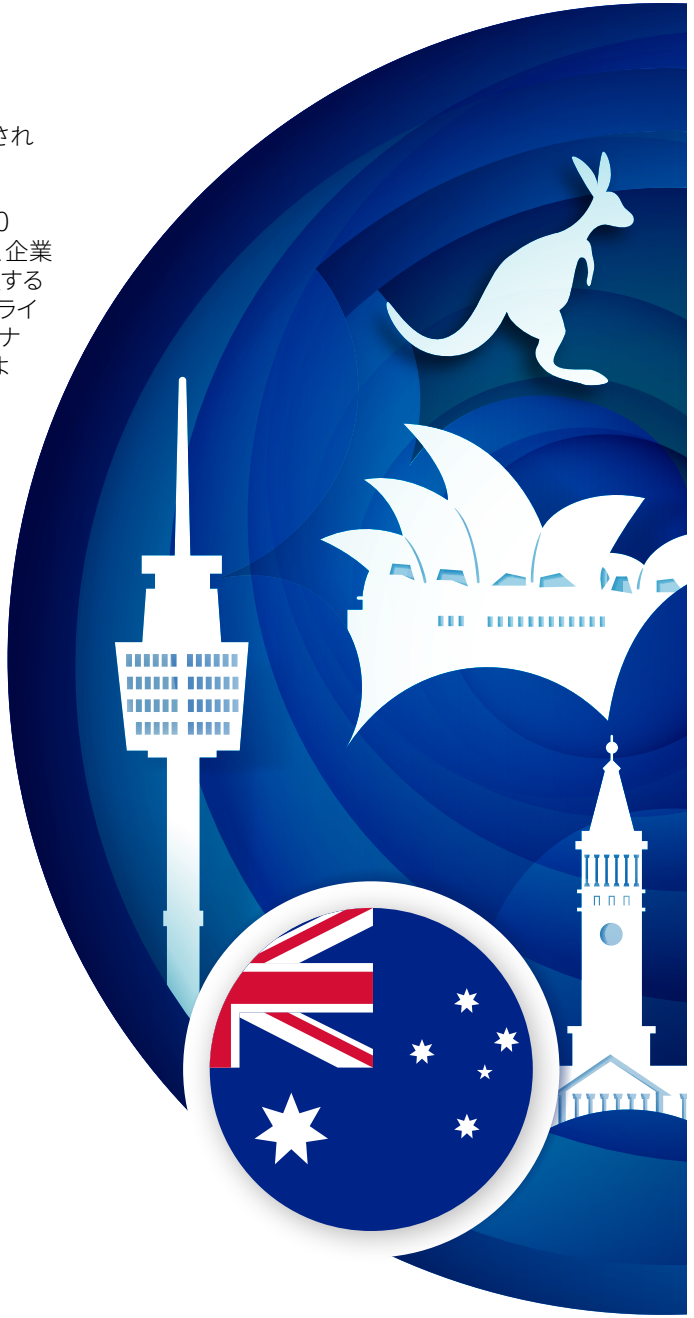


*OAICとは、オーストラリアにおけるデータプライバシーの規制当局です。

その後、オーストラリア政府はデータプライバシー規制をさらに強化するための一連の改革を可決すると予想されていますが、本稿執筆時点では、これらの改革のリリースに関する正式なスケジュールは見られていません。

AIに関して、OAICは、データのプライバシーと保護に関連してAIがもたらすリスクを公表しています。2024年10月、OAICは、法案がAIにどのように適用されるかを詳述した二つのガイドをリリースしました。最初のガイドは、企業が市場に流通しているAI製品を利用する際にプライバシー義務を遵守することを容易にし、適切な製品を選択するのに役立つとされています。2つ目は、個人データを使って生成AIモデルをトレーニングする開発者に対して、プライバシーに関するガイダンスを提供しています。これらのガイドにより、オーストラリアの企業は適切なデータガバナンスプロセスを確立し、AIイノベーションがデータプライバシー規制に準拠して行われることをより確実できるようになります。

さらに、2025年2月、パリで開催されたAIアクションサミットにおいて、オーストラリアのプライバシーコミッショナーは、韓国、フランス、英国、アイルランドのデータ保護当局と共同宣言に署名し、「プライバシー保護AI」を可能にするデータガバナンスを確立することを約束しました。これにより、オーストラリアは、イノベーションを促進し続けながらAIのデータプライバシー保護を強化するための効果的なガバナンスフレームワークを確立するためのグローバルな協力へのコミットメントを示しました。



中国

中国は近年、データプライバシーとデータセキュリティの枠組みを確立しています。

2021年11月に制定された個人情報保護法 (PIPL) は、中国初の個人データの保護に特化した法律です。PIPLでは個人データの処理を管理し、個人の権利を保護して、合法性、透明性、必要性などの原則を導入しています。

PIPLの主な特徴は次のとおりです:

個人の権利
ユーザーは自分のデータにアクセスし、修正し、削除を要求できます。また、他の企業へのデータ転送を要求することもできます

未成年者のデータ
14歳未満の未成年者のデータを処理するには、保護者の同意と特定の処理規則が必要です

自動化された意思決定
取引慣行における不合理な差別的取扱いを禁止し、ターゲットマーケティングのオプトアウトの選択肢を義務付けています

データ移転
個人データは、明示的な同意があり、セキュリティ評価または契約に準拠している場合にのみ、国外に転送できます

域外適用
中国国内で個人データを処理する外国の企業は、PIPLに準拠し、中国において代表者を指定しなければならない

罰則
違反した場合、最高5,000万元または年間売上高の5%の罰金、および業務停止の可能性がある

2021年9月1日に制定されたデータセキュリティ法 (DSL) は、中国におけるデータ管理と保護のための包括的な枠組みを確立しています。

DSLの主な特徴は次のとおりです：

安全保障へのフォーカス
国家安全保障と公共の利益のためのデータセキュリティの重要性を強調し、リスクを低減するためのデータ取扱者の責任を規定しています

説明責任と罰則
違反した企業は、罰金や業務停止などの厳しい罰則に直面する可能性があります

当局間の調整
データセキュリティを監督し、セクター間のコンプライアンスを確保するために、さまざまな政府機関間の協力を義務付けています

データの取扱いにおける義務
データを取り扱う事業者は、データを侵害や誤用から保護するためのセキュリティ対策を講じる必要があります。これには、リスク評価とインシデント対応メカニズムが含まれます

国境を越えたデータ移転
セキュリティ評価や国内法の遵守など、中国本土外へのデータ移転の条件を設定します。政府のセキュリティ評価を通じた認可やデータ主体から明示的に得た同意等が移転にあたって必要になります

データ分類
安全保障や、公共の利益に対する重要性をもとにデータをさまざまなレベルに分類し、各カテゴリに合わせたセキュリティ対策を要求しています。「中核データ」には、安全保障上機密性の高いデータが含まれ、「重要データ」は、「中核データ」よりも機密性が低いが、国家および経済の安全保障上重要であるとみなされます。また、「一般データ」は、漏洩しても重大な損害を引き起こさないデータとされています

中国サイバースペース管理局 (CAC) が、PIPLとDSLにかかわるコンプライアンスを監督する主要な機関になります。

AIに関連して、自動意思決定に関するPIPLの規制は、AIアプリケーションにも適用されます。PIPLは透明性、公平性、自動意思決定を使用するアプリケーションからオプトアウトする権利を要求しており、AIアプリケーションを使用する企業はこれらの要件に準拠する必要があります。DSLにはAIに特化した規制は見られませんが、大規模で機密性の高いデータセットの取り扱いに関するガイダンスは、AIアプリケーションを使用する企業が遵守する必要があります。

特に金融サービスに関しては、2024年12月に国家金融規制庁 (NFRA) が銀行および保険機関のデータセキュリティに関する行政措置 (NFRAデータ規則) を導入しています。

NFRAデータ・ルールの主な特徴は次のとおりです:

- 商業銀行、信託会社、保険会社、その他の金融機関を含む指定機関に適用されます
- データは、顧客データ、ビジネスデータ、運用・管理データ、システム運用・セキュリティデータの4つのカテゴリに分類され、中核データ、重要データ、機密データ、一般データのレベルがあります
- 国家の安全や公共の安全を脅かす「重要データ」は、より厳しい規制を受けます
- 主な要件には、ガバナンス構造の確立、データセキュリティのリスク管理への統合、データ資産の登録、アウトソーシングの制約などがあります
- データセキュリティ保護のベースラインは、データ管理の最低基準を規定します
- 「機密データ」については、セキュリティ評価を実施し、脅威を監視し、インシデントのタイムリーな報告を含むインシデント対応メカニズムを確立する必要があります
- 包括的なデータセキュリティ監査を、少なくとも3年ごとに行う必要があります

中国は、生成AI産業に対する最初の施策である生成人工知能サービス管理のための暫定措置(「措置」) を8月15日付けで導入しました。CACが策定したこの施策は、業界の標準化とイノベーションの促進を目的としているとされています。

主な特徴は次のとおりです:

規制の枠組み
データコンプライアンスおよび知的財産に関するサービス提供者の法的責任を確立します

管理
AIサービスの評価と記録の保持を含む、コンプライアンスと監視のガイドラインを規定しています

国際的な規制
海外事業者にも中国の法律を遵守させることを念頭に置いています

データ品質
サービス提供者は、トレーニングデータが高品質で、正確、多様であり、合法的なソースであることを確認すること、利用される個人データについてはユーザーの同意が必要であることを規定しています

中国はこの措置を通じて、AIアプリケーションとサービス提供者が既存のデータ保護法を遵守し、データの品質と同意に関する追加のガイダンスを提供することを義務付けています。

香港特別行政区

香港におけるデータプライバシーは、個人データ保護委員会 (PCPD) の管轄下にあります。

香港のデータプライバシー法である個人情報保護 条例 (PDPO) は、AP地域で最も長く制定されているデータプライバシー法の1つです。PDPOの最新の改正は2021年に行われ、データ侵害時の通知、データ保持ポリシー、ダイレクト・マーケティング規制、PCPDの執行権限の強化に焦点が当てられています。

2024年6月、PCPDはAIの利用に関連するデータプライバシーに関する具体的なガイダンスである人工知能:モデル個人データ保護フレームワーク (モデル) フレームワークをリリースしました。これは、2021年に発行された「人工知能の倫理的な開発と利用に関するガイダンス」にもとにして書かれています。

主な特徴は次のとおりです:

対象者
個人データを扱うAIシステムを利用するすべての企業を対象として設計されており、当初のAI開発者に焦点を当てていたものを拡大しています

リスクベースのアプローチ
個人データ (プライバシー) 条例 (PDPO) を遵守するための実践的なガイダンスを提供しています

中核的な価値と原則
このフレームワークでは、データスチュワードシップの3つの価値(尊敬、有益、公正)と7つの倫理原則(説明責任、人間による監視、透明性と解釈可能性、データプライバシー、有益なAI、信頼性/堅牢性/セキュリティ、公平性)が強調されています

フレームワーク構造 (4部構成)
AI戦略とガバナンス、リスクアセスメントと人的監視、AIモデルのカスタマイズとAIシステムの実装と管理、ステークホルダーとのコミュニケーションとエンゲージメントから構成されています

全体として、モデルフレームワークは、データ保護と倫理的な配慮を確保しながら、企業がAIの複雑さに対処できるよう支援することを目的としています。

インド

2023年デジタル個人データ保護法 (DPDP法) は、インドにおけるデータ保護のための包括的な枠組みを定めています。

DPDP法の主な特徴は次のとおりです

インドのデータ保護委員会 (DPB) の設立
データプライバシーの侵害に関連する紛争に対処する独立機関が設立されます

同意
データ処理には明示的な同意が必要であり、同意を撤回する権利もあります

個人の権利
個人データにアクセスし、訂正し、指名し、消去する権利が本人に与えられます

データ侵害時の通知
データ侵害が発生した場合は、本人とDPBに通知・報告する必要があります

罰則
違反には重大な罰則があります

適用除外
政府機関については、一定の要件の下に適用除外が存在します

処理の原則
データは、特定の目的のために収集され、最小限に抑えられ、必要な場合にのみ保持される必要があります

国境を越えたデータ移転
インド国外へのデータ移転は、安全策(例えば、同レベルのデータ保護規制を有する国にデータを移転し、明示的な同意を得ること)を講じた上で可能になります。国境を越えたデータ移転については、さらなる規制ガイダンスが期待されます

2025年11月、インド電子情報技術省は、DPDP法の運用を目的としたデジタル個人データ保護規則(DPDP規則)を公布しました。

DPDP規則の主な特徴は次のとおりです:

- 個人は、同意を撤回し、苦情を効果的に処理する仕組みを使うことができます。また、データにアクセスし、修正、消去することができます
- データ受託者は、定義された保存期間での取扱い、コンプライアンス監査の実施、透明性の高いプロセスを通じて、プライバシーとセキュリティを確保します
- 暗号化、72時間以内の侵害報告、本人確認、および子どもと障がい者に対する特別な保護が義務付けられています

DPDP法にもDPDP規則にも、AIに関するデータプライバシーに特化した具体的な規定は見られていません。しかし、DPDP法とDPDP規則は、倫理的なデータの取り扱いを促進するフレームワークを確立しており、これはAIガバナンスアプローチを確立する企業にとって重要な規律になります。

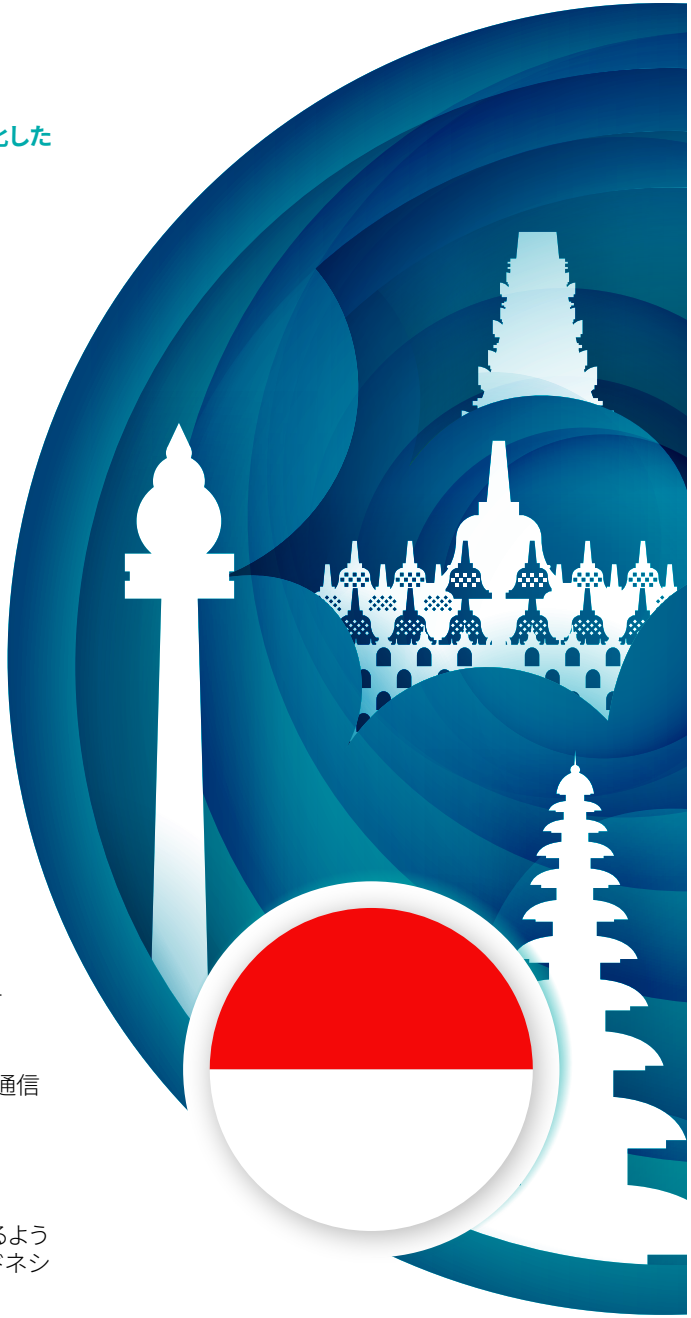
インドネシア

一般に個人データ保護法 (PDP法) と呼ばれる2022年のインドネシア法第27号は、個人データの保護に特化したインドネシア初の包括的な法律です。

2022年10月に施行されました。

PDP法の主な特徴は以下のとおりです:

- 違反は罰金または刑事罰につながるとされています
- インドネシアの内外を問わず、インドネシア人の個人データを取り扱うすべての事業体を対象としています
- アクセス、修正、削除、同意の撤回、異議申し立て、制限、苦情の権利を個人に与えています
- 管理者/処理者に対して、適法性のあるデータ処理、データ保護、侵害発生時の通知、また必要に応じてデータ保護オフィサーの任命を要求しています
- 同意を主要な根拠としているほか、契約上の必要性、法的義務、重大な利益、公共の利益及び正当な利益といった他の根拠も認めています
- 越境移転は、移転先がインドネシアと同等以上のデータ保護レベルを有する法域である場合、特定の移転について十分なレベルの拘束力のあるデータ保護が適用できる場合とされています
- 個人データ保護機関の設置が義務付けられています 。なお、設置までの暫定期間においては、通信デジタル部がコンプライアンスを監督することになっています



2024年10月に2年間の移行期間が終了し、すべての対象事業者がPDP法に完全に準拠することが求められるようになりました。対象事業者には、インドネシア国内で活動しているか海外で活動しているかにかかわらず、インドネシア国民または居住者の個人データを取り扱うあらゆる関係者が含まれます。

日本

日本におけるデータプライバシー規制の中核は、個人情報保護委員会 (PPC) が監督する個人情報の保護に関する法律 (APPI) です。

APPIは、日本におけるデータの取り扱い、国境を越えたデータ移転、および個人情報の保護を規定しています。APPIは3年ごとに見直すことが求められており、2024年6月、PPCは個人情報保護法の3年ごとの見直しに向けた検討に関する中間報告 (以下、「中間報告」という。) を公表しました。改正されたAPPIは2026年に制定される見通しです。

現在のAPIの主な機能は次のとおりです:

個人情報の定義
氏名、生年月日、その他の記述等(文書、図画、若しくは電磁的記録に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項をいう)により特定の個人を識別することができるもの(他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む)

データ主体の権利
本人は、自身のデータ(事業者の保有個人データ)について、、開示、訂正・削除、利用停止・消去の請求を行うことができます

安全管理措置
事業者は、個人データの漏えい、滅失又はき損を防止するために必要な措置を講じなければならない

データ侵害の報告・通知
報告対象事態が見られた場合にはPPCへの報告と影響を受ける本人への通知が義務付けられています

外部委託
データ処理を外部委託する場合は、委託先の適切な監督が求められます

データ処理の原則
明確で特定された目的のためにのみ個人情報を収集し、利用することを要求しています

同意の要件
要配慮個人情報情報の収集、第三者への個人データの提供、国境を越えたデータ移転 には、事前の同意が必要になっています(越境移転については次の事項を参照)

越境移転
データを国外に移転するには、次のいずれかの条件が必要になっています:
- いわゆる同等性認定等、移転先のある国が同等の水準国であること
- 移転先が、基準に適合する体制を整備した事業者であること
- 本人の同意があること

PPCはまた、2023年6月に「生成AIサービスの利用に関する注意喚起等」を発表しました。この文書では、AIを利用する事業者における個人データの取扱いについて、次の重要な要件を挙げています。

事業者は、生成AIサービスへの個人データの入力が、特定された利用目的を達成するために必要な範囲内で行われていることを十分に確認すること

生成 AI サービスを提供する事業者が、個人データを機械学習に利用しないこと等を十分に確認すること

さらに、文書には、ChatGPTサービスの提供者であるOpenAIに対する注意喚起も含まれています。

マレーシア

マレーシアでは2010年6月に個人データ保護法 (PDPA) が可決され、2013年11月に発効しました。

PDPAにより、PDPAを監督する政府機関として2011年5月に個人データ保護局 (JPDP) が設立されました。

適用範囲
マレーシア国内の個人データにかかわる商取引に適用されます。

7つの主要な原則:

- 同意を伴う合法的な取扱い
- データ収集について通知を受けた個人は、取扱いを拒否することも可能
- 法律で許可されていない限り、同意された目的のためにのみ開示されるデータ
- 適切なセキュリティ対策
- 必要に応じたデータ保存期限
- データの正確性、完全性、最新性の確保
- 自身のデータについての個人によるアクセス・修正の権利

2024年10月、マレーシア政府は、PDPAに含まれている条項を更新し、国際データ保護基準への整合性を強化する2024年個人データ保護 (改正) 法 (PDPAA) を発表しました。

主な更新内容は次のとおりです:

- 「データユーザ」を「データ管理者」に変更
- 生体認証データを機密性の高い個人データに分類
- データ侵害時におけるPDPDおよび影響を受けるデータ主体への報告・通知の義務化
- 違反時には100万リンギット以下の罰金・3年以下の懲役
- データ主体による、ポータブルフォーマットでのデータ開示要求
- 国境を越えたデータ移転のためのホワイトリスト制度の廃止
- データ管理者及び処理者による、データ保護オフィサー (DPO) の任命

ニュージーランド

ニュージーランドでの主要なデータプライバシー関連法は、2020年プライバシー法です。

この法律は、Office of the Privacy Commissioner (OPC) によって施行され、13の情報プライバシー原則 (IPP) を定めています。

これらの原則は次のとおりです：

収集の目的
個人データは、企業の役割に直接関連する合法的な目的のために収集される必要があります

個人データの情報源
個人データは、一定の例外を除き、本人から直接収集される必要があります

同意
個人は自分の個人データの収集について知らされたうえで、同意を求められる必要があります

収集の方法
個人データは、公正かつ合法的な方法で収集されるべきであり、不公正または誤解を招くような慣行は避けるべきとされています

ストレージとセキュリティ
企業は、個人データを安全に保管し、紛失、誤用、または不正アクセスから保護する必要があります

アクセスと訂正
個人は、自分の個人データにアクセスし、それが不正確な場合には訂正を要求する権利を有します

保存
個人データは、収集した目的のために必要な期間を超えて保存できません

開示
本人の同意がある場合または法律で要求されている場合を除き、個人データは第三者に開示できません

個人データの利用
個人データは、他の利用について同意を得ない限り、収集された目的のためにのみ使用される必要があります

正確性
企業は、個人データが正確、最新、完全であることを保証するために合理的な措置を講じる必要があります

透明性
個人は、個人データの利用および関連する権利について知らされる必要があります

国境を越えた開示
十分な保護がなされていない限り、個人データを海外に開示できません

固有の識別子
企業は、職務上必要でない限り、個人に固有の識別子を割り当てることを避ける必要があります

AIに特化したデータプライバシーにかかわるガイダンスについては、NPCは、ニュージーランド企業がAIを使用する際にIPPを考慮する方法に関するガイダンスを公開しています。ガイダンスでは、AI固有の質問をIPPに沿ってプライバシー影響評価に統合できることを示唆しています。

フィリピン

フィリピンでは2012年8月、2012年データプライバシー法 (DPA) が制定されました。

DPAの主な要素は次のとおりです:

個人データの保護
個人データおよびセンシティブデータを処理する公的機関と民間企業の両方に適用されます

合法的な処理
データを特定の目的で合法的、公正、透明に処理することが要求されます

データ主体の権利
通知を受ける権利、異議を申し立てる権利、アクセスする権利、修正する権利、消去する権利、苦情を申し立てる権利、データポータビリティの権利、損害賠償を求める権利が含まれます

セキュリティ対策の義務付け
不正アクセスや侵害からデータを保護するための適切なセキュリティを必要とします

コンプライアンスにかかわる執行
National Privacy Commission (NPC) は、違反に対して執行を行います

国境を越えたデータ移転
十分なデータ保護法が適用される国へのデータ転送が認められています

適用除外
公共の利益や法、規制をもとにした報道、芸術、文学または研究にかかわる情報の最小限の範囲での収集、アクセス、使用、開示、またはその他の処理に限り、取扱い義務が免除されます

NPCは定期的にDPAの追加ガイダンスを発表するほか、AIシステムへのDPAの適用に関する具体的なガイダンスも発表しています。

AIシステムへのDPAの適用に関するガイダンスの主な特徴は以下のとおりである：

透明性とコミュニケーション
AIにおけるデータ処理の性質と目的について、データ主体に情報を提供すること

ガバナンスと倫理的なデータ処理
偏見の監視、自動化された意思決定への人間の介入など、倫理的なデータ処理のための効果的なガバナンスメカニズムを実装すること

データの正確性と最小化
個人データを正確かつ最新の状態に保ち、AI開発に不要なデータを排除すること

権利の解釈
データ主体の権利と利益になるように規制を解釈すること

個人データ管理者 (PIC) および個人データ処理者 (PIP) の義務
プライバシー原則を遵守し、セキュリティ対策を実施して、個人データのAI処理に対する説明責任を確保すること

法的根拠とデータ主体の権利
個人データを処理するための適切な法的根拠を特定し、データ主体の権利の行使を促進するメカニズムを実装して、AIシステムのライフサイクル全体を通じてアクセスを確保すること

シンガポール

データプライバシーに関する基本的な法律は、2012年個人データ保護法 (PDPA) です。

2020年、シンガポール政府は、同意、データ利用の例外、および新しい定義に関連するデータプライバシー対策を強化した2020年個人データ保護 (改正) 法を発表しました。

個人データ保護委員会 (PDPC) は、PDPAをもとに、企業間で責任あるデータ管理が行われるよう監督する当局になります。PDPCは、2024年3月にAIの推奨・決定システムにおけるパーソナルデータの利用に関するアドバイザリーガイドライン (以下ガイドラインという。) を公表しました。

ガイドラインは、PDPAの下での機械学習のための個人データの使用について明確にしています。

主な詳細は次のとおりです:

AIシステムをトレーニングする際に、**業務改善や研究の例外を利用することで、同意を得ることを回避できる**とされています。

- 業務改善の例外では、個人の行動を把握し、製品やサービスの向上や開発にデータを利用することができます。一方、個人に影響を及ぼす意思決定を行うためにデータを利用することが禁止されており、データの利用は個人に悪影響を及ぼしてはならない、とされています
- 研究目的の例外では、データは研究のためにのみ利用されなければならず、また研究は公共の利益にかなうか、明らかな社会的利益を有するものである必要があります

プライバシーを保護し、トレーニングに使用される個人データの量を制限するために、企業は個人データを匿名化することが推奨されています

AIシステムで**個人データをどのように利用するかについて、透明性を持つ必要**があります

同意、通知、説明責任などのPDPAの義務を遵守することが必須になります

PDPAおよび関連する改正に基づくその他の一般的な規則には、以下のものが含まれます

同意の要件
企業は、個人データを収集、使用、または開示する前に、個人から同意を得る必要があります

目的の制限
個人に通知された特定の正当な目的のためにのみデータを収集できます

アクセス権と訂正権
個人は、企業が保有する自身の個人データにアクセスし、必要に応じて訂正を要求する権利を持ちます

データ保護の義務
企業は、個人データを保護し、その正確性を確保するために、合理的なセキュリティ対策を実施する必要があります

データ侵害時の通知
企業は、データ侵害が発生した場合、影響を受ける個人とPDPCに通知する必要があります

Infocomm Media Development Authority (IMDA) は、データ保護のリスクを軽減しながら生成AIアプリケーションのためのデータへのアクセスを促進する方法を調査するために、プライバシー強化技術(PETs)のサンドボックスを導入しました。PDPCは主にデータプライバシーを取り扱っている一方、IMDAはデータガバナンスとデジタルトラストに関する議論と開発にも関与しています。

PDPCは、合成データ (SD) 生成を採用するビジネスのための包括的なフレームワークを確立するために、Proposed Guide to Synthetic Data (SD) Generationをリリースしました。このガイドでは、AIモデルをトレーニングするための合成データの生成について説明しています。合成データは通常は架空のデータであり、個人データとはみなされませんが、再識別リスクをもたらすことがあります。このガイドでは、一般的なユースケースに合わせて企業がこれらのリスクを最小限に抑えるためのベストプラクティスを推奨し、ガバナンス管理、契約プロセス、および残存リスクに対処するための技術的手段について概説しています。

韓国

2011年、韓国は個人情報保護法 (PIPA) を導入し、個人情報保護の枠組みを確立しました。[42]

個人情報保護委員会 (PIPC) は、データプライバシーに関するポリシーを策定し、PIPAの適用を監督する独立したデータ保護機関です。

主な内容は次のとおりです:

同意
データの収集と処理には明示的な同意が必要です

データの最小化
企業は必要なデータのみを収集する必要があります

個人の権利
個人は自分のデータにアクセスし、修正し、削除することができます

データセキュリティ
個人データを保護するためのセキュリティ対策が義務付けられています

データ侵害時の通知
企業は、個人およびPIPCにデータ侵害を通知する必要があります

罰則
コンプライアンス違反に対して罰金と制裁措置を課します

越境転送
韓国国外へのデータ転送に制限が課されています

監督
PIPCを設置し、コンプライアンスを統括します

2023年、PIPCはPIPAの見直しを行い、2025年9月15日に改正法が導入されました。[43]

主な改正の内容は次のとおりです:

- 緊急事態における至急のデータ処理にかかわる**柔軟性の向上**
- 公的機関と民間機関の**紛争解決プロセスの改善**
- 大規模なデータセットを扱う公的機関向けに**強化されたセキュリティ対策**
- 行政上の罰金に直面している中小企業のための**延長された支払いオプション**
- 事前の同意なしにドローンのようなデバイスを介して**合法的なデータ処理を行うためのガイドライン**
- データ侵害と子どもの同意に関する、オンラインおよびオフラインの企業に対する一貫した規範
- 国際的なデータ移転のための多様な条件とペナルティ計算の変更

改正PIPAはAIを念頭に置いて導入されました。消費者データの権利の強化と国際データ移転の条件は、個人のデータプライバシー権を確保しつつ、韓国におけるAIの安全な開発を確保するためのPIPCのイニシアティブとされています。

さらに、PIPCは、データプライバシーに関連する生成AIのためのいくつかの詳細なガイドラインを導入しています。これらのガイドラインは、商用および社内で開発されたAIシステムの開発、トレーニング、展開、ガバナンスに関する法的な安全基準を定めています。

その最新かつ包括的なものは、2025年8月の「生成AIの開発と利用における個人データ処理のためのガイドライン」です。

このガイドラインは、AIの開発と導入のあらゆる段階における企業の最低基準を定めています。これらは、商用の大規模言語モデル、カスタマイズされたオープンソースモデル、完全に自己開発されたソリューションなど、あらゆる種類のAIシステムに包括的に適用されます。各カテゴリについて、ガイドラインは、サービス提供者の検証、堅牢なデータガバナンス、徹底的な文書化、プライバシー影響評価などの明確なコンプライアンス義務を規定しています。特に、ガイドラインでは、商用APIベースの大規模言語モデルにかかわるデータ共有とサービスレベル契約のプライバシー条項に対する期待も示されています。

AIライフサイクル全体にわたるコンプライアンス要件には、次のものが含まれます：

目的の設定と戦略的プランニング
目的の設定と戦略的プランニング、リスクの評価、データ利用における根拠の文書化

開発とアーキテクチャ設計
プライバシー・バイ・デザインの導入、データ資料の最小化、国境を越えたデータ移転におけるコンプライアンスの確保

AIトレーニングと開発
トレーニングデータの検証、公平性の確保、安全対策の文書化

導入と管理
継続的な監視、ユーザーの同意の管理、インシデント対応、定期的なコンプライアンスレビュー

このガイドラインでは、最高プライバシー責任者の任命を義務付けるなど、AIのプライバシーを順守するための強力なガバナンス構造を確立することも求めています。

主な要素は次のとおりです：

- 経営幹部のアカウンタビリティ
- 部門横断的な協力
- 監査のための包括的な文書化
- プライバシーにかかわるプラクティスについてのスタッフ研修

ガバナンスフレームワークは、アルゴリズムのバイアス、透明性、人間による監視の必要性など、AI固有のリスクにも対処します。さらに、ガイドラインはAI技術の新たなトレンドを取り入れており、新しいテクノロジーや規制要件の変化に応じて定期的に更新されるように設計されています。

PIPCは他にも以下のようなガイドラインを発表しています：

安全なAIデータ活用のためのAIプライバシーリスクマネジメントモデル
(2024年12月)[45]

合成データの生成と利用のための参照方法と手順を示した**合成データ生成と利用ガイド**
(2024年12月)[46]

AI開発およびサービスのための公的に利用可能な個人情報の処理に関するガイドライン (2024年7月) には、AIのトレーニングとサービスのために公的に利用可能な個人情報を収集・利用するための基準が含まれています[47]

AIシステムの開発・運用のための**AI個人情報保護自己評価チェックリスト (開発者・運用者向け)** (2021年7月)[48]

台湾

台湾の個人データ保護法 (PDPA)(「台湾」) は、個人データの収集、処理、利用を管理する主要な法律になります。[49]

PDPAは当初2012年10月に発効し、最新の改正は2023年5月に行われました。PDPAには、2016年3月に改正された個人データ保護法施行規則が添付されています。[50]

PDPAの主な内容は次のとおりです:

適用範囲
個人データを取り扱う公的機関と民間の組織の両方に適用されます

データの最小化
特定の目的のために必要なデータのみの収集が奨励されています

定義
個人データと機微な個人データを明確に定義し、保護のためのカテゴリーを確立します

同意
個人データを収集または処理する前に、個人からの明示的な同意が必要になります

個人の権利
個人データにアクセス、訂正、および削除する権利と、同意を取り消す権利が個人に付与されています

データセキュリティ
技術的および組織的な保護措置を含む、個人データを侵害から保護するための対策が義務付けられてます

同意の要件
機微な個人データの収集、第三者への個人データの提供、データの越境移転には、原則個人による事前の同意が必要になっています。また、個人には利用目的を通知しなければなりません

データの越境移転
台湾外への個人データの移転において、移転先国での適切な保護レベルの確保が求められています。PDPAでは国境を越えたデータ移転を直接禁止していませんが、医療記録などの特定のデータにはローカライズの要件があります

罰則
違反に対する罰則 (罰金や行政処分など) を定めています

台湾では、2023年5月の改正を受けて個人データ保護委員会 (PDPC) 準備室が、2023年12月に設置されました。PDPCは、AIシステムが遵守し、個人データの保護を求めるデータプライバシーフレームワークを作成する責任があるとされています。外務省は2025年8月、データの革新と活用の発展の促進に関する法律案を公表しました。この法案は、AI利用のためのデータガバナンス規則を規定するものであり、台湾がAIに関するデータの懸念に対処しようとしていることを示しています。

タイ

タイにおけるデータプライバシー規制の中核となるのは、2019年に可決され、2022年6月から施行された個人データ保護法 (PDPA) です。[52]

2024年4月、タイは、個人データ保護委員会 (PDPC) と国家デジタル経済社会委員会が監督する国家個人データ保護促進マスタープランを策定しました。[53]このマスタープランでは、タイにおける個人データ保護を調査・分析し、2024年から2027年までの現在の政策、戦略、目標を概説しています。

PDPAの主な原則は次のとおりです:

データ越境移転
国外に移転されるデータは適切に保護される必要があります

目的の制限
個人データは、特定された、明示的な、正当な目的のためにのみ収集することができます

データ主体の権利
個人は、自分のデータにアクセスし、訂正、削除する権利、およびデータの使用に異議を唱える権利を持ちます

データセキュリティ
企業は、不正または違法な処理、損失、または損害から個人データを保護するための対策を実施する必要があります

同意
データ管理者は、特定の適用除外(例えば、契約上の必要性や法的義務)を除き、個人データを収集、使用、または開示する前に明示的な同意を得る必要があります

マスタープランの主な目的は次のとおりです:

- 法的・政策的枠組みの強化
- データ保護に関するスキルと意識の向上
- デジタルサービスに対する国民の信頼の向上
- 効果的なガバナンスとコンプライアンスのサポート

マスタープランの目標を実現するための主な戦略には、以下のものが含まれます:

- 法規制の見直し
- データ保護にかかわる要員のトレーニング
- 啓発キャンペーンの実施
- セキュアなテクノロジーの推進
- PDPCによる監督の強化

タイでは、AIにおけるデータプライバシーの懸念に関する法律やガイドラインはまだ見られていませんが、PDPCはマスタープランを通じて、AIへの移行に備え、変化するデータ環境に合わせてデータプライバシー規制を策定する意向を示しています。

2025年6月、タイ中央銀行は、リスク管理、透明性、顧客保護に焦点を当てた金融サービスにおけるAI利用に関するパブリックコンサルテーションのガイドライン案を発表しました。[54]これらのガイドラインは、タイの法律の下で金融機関と決済システム運営者に適用され、説明責任、ライフサイクルリスク管理、顧客保護を求めていますまた、法的基準、リスク評価戦略、人間による監視、データとモデルの制御、サイバーセキュリティ対策に沿ったAI利用ポリシーを提案しています。

ベトナム

ベトナムにおける主なデータプライバシー規制は、2023年4月に公布された個人データ保護に関する法令であり、デジタル経済における個人データの保護とプライバシーの確保を目的としています。[55]

主な内容は次のとおりです:

- **個人データを保護し**、デジタル経済におけるプライバシーを確保することを目的とします
- 適切なデータ保護法を持つ国への国境を越えたデータ移転が認められています
- **国家安全保障、防衛、公衆衛生など、特定のデータ処理活動は除外されます**
- 目的を特定し、データ収集を最小限に抑えて、**データ処理が合法的、公正、透明であることが求められています**
- 情報の通知や、アクセス、訂正、消去、異議申し立て、データポータビリティに関する**データ主体の権利が認められています**
- **データ侵害が発生した場合、企業は当局と影響を受けるデータ主体に通知する必要があります**
- **ベトナム国内で個人データを処理するすべての企業と個人に適用されます。**外国企業も含まれます
- **当局を通じて法令を執行し、行政上の罰金、業務停止、刑事告発を含む違反に対する罰則を適用します**
- **個人データの定義は、個人を識別できる情報**であり、機微な個人データは、人種、民族、政治的見解、宗教的信念、健康、および生体情報に関連する情報とされています

2025年6月26日、ベトナム国会は2025年個人データ保護法 (LPDP) を公布し、同法は2026年1月1日から施行されます。[56]同法は、個人データとその保護、関連機関、企業、および個人の権利・義務および責任に関する規則を定めています。

LPDP 2025の主な特徴:

データ取引の禁止
この法律は個人データの売買を明確に禁止しており、違反した場合には重大な罰則が科されます。これは、違法なデータの商業化を抑制することを目的としています

データ主体の権利の強化
個人には、自分のデータがどのように処理されるかについて通知を受ける権利、自分のデータにアクセスして修正する権利、自分のデータに対して異議を唱えたり、データの消去を要求したりする権利など、拡張された権利が与えられます。同意は、特定の目的のために明示的かつ自発的に示されなければなりません

厳しい罰則
この法律では、違反した場合に厳しい行政および刑事罰が科されます。ベトナムでは、重大な違反があった場合、企業の年間総売上高の最大5%の罰金が科される可能性があります。違法なデータ取引に対する罰則は、違法な利益の最大10倍になる可能性があります

企業における厳格な義務
データ管理者と処理者は、個人データを保護するための堅牢なセキュリティ対策を実装する必要があります。主要な義務には、個人に対する明確なデータ取扱い通知の提供、及びデータ侵害の所轄官庁及び影響を受けるデータ主体双方への報告が含まれます。注目すべき新しい要件は、採用されなかった求職者のデータを強制的に削除することが挙げられます

デロイトの専門家

Authors

Nicola Sergeant
Managing Director
ACRS Operations Lead
Japan
nicola.sergeant@tohmatsu.co.jp

Rhys Belcher
Senior Consultant
ACRS
Hong Kong SAR
jobelcher@deloitte.com.hk

Asia Pacific Centre for Regulatory Strategy (ACRS)

神谷 精志
Executive Sponsor
Asia Pacific Regulatory & Financial Risk Lead
seiji.kamiya@tohmatsu.co.jp

首藤 佑樹
ACRS Steering Committee
Partner
AP Consulting Growth Leader
yshuto@tohmatsu.co.jp

Tony Wood
ACRS Steering Committee
Partner
AP Banking & Capital Markets Leader
tonywood@deloitte.com.hk

Ye Fang
ACRS Steering Committee
Partner
China SR&T FS Industry Lead
yefang@deloitte.com.cn

Sean Moore
Australia Co-lead
Partner
AU SR&T FS Industry Lead
semoore@deloitte.com.au

Nai Seng Wong
SEA Co-lead
Partner
SEA Regulatory Strategy Lead
nawong@deloitte.com

小林 晋也
Japan Co-lead
Managing Director
JP SR&T Insurance Sector Lead
shinya.kobayashi@tohmatsu.co.jp

Asia Pacific Trustworthy AI Leaders

Dr Elea Wurth
Partner
Asia Pacific & Australia
ewurth@deloitte.com.au

Amy Dove
Partner
New Zealand
amydove@deloitte.co.nz

染谷 豊浩
Partner
Japan
toyohiro.sometani@tohmatsu.co.jp

Chris A. Chen
Partner
Taiwan
chrisachen@deloitte.com.tw

Jessica Kim
Partner
South Korea
jessikim@deloitte.com

Silas Hao Zhu
Partner
China
silzhu@deloitte.com.cn

Dishell Gokaldas
Partner
Singapore
dgokaldas@deloitte.com

Jayant Saran
Partner
India
jsaran@deloitte.com

Pence Cong Peng
Partner
China
pepeng@deloitte.com.cn

Brad Puye Lin
Partner
Hong Kong SAR
bradlin@deloitte.com.hk

Contributors

Harm Ellens
AI Governance &
Risk Management Specialist
Director
Australia
hellens@deloitte.com.au

Mayuran Palanisamy
Digital Privacy &
Trust Offering Leader
Partner
India
mayuranp@deloitte.com

Lucy Mannering
Privacy
Leader
Partner
Australia
lmannering@deloitte.com.au

Han H. Lin
Privacy &
Data Protection Specialist
Managing Director
Taiwan
hanhlin@deloitte.com.tw

大場 敏行
Privacy, Security &
IT Governance Specialist
Managing Director
Japan
toshiyuki.oba@tohmatsu.co.jp

Mariette Van Niekerk
Data Science
Lead
Managing Director
New Zealand
mvanniekerk@deloitte.co.nz

Acknowledgements

Tommy Hartanto
Director
Indonesia
thartanto@deloitte.com

Joey Xu
Senior Manager
China
joexu@deloittecn.com.cn

Herbert Rollom
Director
Philippines
hrollom@deloitte.com

Andy T. Tsou
Manager
Taiwan
atsou@deloitte.com.tw

Dae Woo Lee
Manager
Korea
dlee37@deloitte.com

Anh Quoc Luu
Senior Manager
Vietnam
anhqluu@deloitte.com

Kerrie Hie
Director
Australia
khie@deloitte.com.au

Shoya Kusoda
Senior Consultant
Japan
shoya.kusuda@tohmatsu.co.jp

Eric Kanikevich
Consultant
Australia
ekanikevich@deloitte.com.au

Fransisca Fransisca
Manager
Hong Kong
fransisca@deloitte.com.hk

Jane Zhang
Associate Director
China
janezhang@deloittecn.com.cn

Christina Fialova
Consultant
Singapore
cfialova@deloitte.com

Steven S. Fang
Manager
Taiwan
stefang@deloitte.com.tw

Prakash Arikrishnan
Director
Malaysia
parikrishnan@deloitte.com

Monai Supanit
Senior Manager
Thailand
msupanit@deloitte.com

Tony Zhi-Wei Tang
Associate Director
Australia
totang@deloitte.com.au

Samuel Yue Xuan Ang
Consultant
Singapore
saang@deloitte.com

参考文献

1. Deloitte Center for Government Insights, *The AI regulations that aren't being talked about*, November 2023, AI regulation | Deloitte Insights
2. Deloitte Asia Pacific AI Institute, AI at a crossroads – Building trust as the path to scale, January 2025, AI at a crossroads | Deloitte China
3. Deloitte Centre for Technology, Media and Telecommunications, *Data privacy and security worries are on the rise, while trust is down*, September 2023, Consumer data privacy and security | Deloitte Insights
4. Deloitte US, *Third Edition: State of Ethics and Trust in Technology*, September 2024, Deloitte's 2024 ethical technology report | Deloitte US
5. Capgemini Research Institute, *"AI and the ethical conundrum" Report*, October 2020, AI and the ethical conundrum: How organisations can build ethically robust AI systems and gain trust - Capgemini
6. Lonergan Research, *DPSI Consumer Survey Research Report*, February 2025, dpsi-consumer-survey-research-report-lonergan-research-feb2025.pdf
7. European Parliament, *General Data Protection Regulation (GDPR)*, April 2016, Regulation - 2016/679 - EN - gdpr - EUR-Lex
8. European Parliament, *General Data Protection Regulation (GDPR)*, April 2016, Regulation - 2016/679 - EN - gdpr - EUR-Lex
9. Office of the Australian Privacy Commissioner, *OAIC stats show record year for data breaches*, May 2025, OAIC stats show record year for data breaches | OAIC
10. Australian Government, *Privacy and Other Legislation Amendment Bill 2024*, December 2024, Privacy and Other Legislation Amendment Bill 2024 – Parliament of Australia
11. Australian Government, *Privacy Act 1988*, December 1988, Privacy Act 1988 - Federal Register of Legislation
12. Australian Government, *Australian Privacy Principles*, Australian Privacy Principles | OAIC
13. Office of the Australian Privacy Commissioner, *Guidance on privacy and the use of commercially available AI products*, October 2024, Guidance on privacy and the use of commercially available AI products | OAIC
14. Office of the Australian Privacy Commissioner, *Guidance on privacy and developing and training generative AI models*, October 2024, Guidance on privacy and developing and training generative AI models | OAIC
15. Office of the Australian Privacy Commissioner, *Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI*, February 2025, Joint statement on building trustworthy data governance frameworks to encourage development of innovative and privacy-protective AI | OAIC
16. National People's Congress, *Personal Information Protection Law*, November 2021, http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm
17. National People's Congress, *Data Security Law of the People's Republic of China*, June 2021, Data Security Law of the People's Republic of China
18. National Financial Regulatory Administration, *Rules on Data Security of Banking and Insurance Institutions*, December 2024, NFRA
19. Cyberspace Administration of China, *Interim Measures for the Management of Generative Artificial Intelligence Services*, July 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm
20. Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal Data (Privacy) Ordinance*, August 1995, 《個人資料(私隱)條例》 Personal Data (Privacy) Ordinance
21. Office of the Privacy Commissioner for Personal Data Hong Kong, *Personal Data (Privacy) (Amendment) Ordinance 2021*, October 2021, s12021254032
22. Office of the Privacy Commissioner for Personal Data Hong Kong, *Artificial Intelligence: Model Personal Data Protection Framework*, June 2024, ai_protection_framework.pdf
23. Office of the Privacy Commissioner for Personal Data Hong Kong, *Guidance on the Ethical Development and Use of Artificial Intelligence*, August 2021, pcpd.org.hk/english/resources_centre/publications/files/guidance_ethical_e.pdf
24. Parliament of India, *The Digital Personal Data Protection Act, 2023*, August 2023, 2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
25. Government of India, *Digital Personal Data Protection Rules, 2025*, January 2025, Draft Digital Personal Data Protection Rules, 2025 – Innovate India
26. Government of Indonesia, *Law of the Republic of Indonesia Number 27 of 2022 Concerning Personal Data Protection*, October 2022, Salinan UU Nomor 27 Tahun 2022.pdf
27. Japanese Government, *Act on the Protection of Personal Information*, May 2003, Act on the Protection of Personal Information - English - Japanese Law Translation
28. Personal Information Protection Commission, *Interim Report on Considerations for the Triennial Review of the Act on Protection of Personal Information*, June 2024, 個人情報保護法　いわゆる３年ごと見直しに係る検討の中間整理 -個人情報保護委員会-
29. Personal Information Protection Commission, *Precautionary Notice on Use of Generative AI Services*, June 2023, 生成AIサービスの利用に関する注意喚起等について（令和５年６月２日）｜個人情報保護委員会
30. Parliament of Malaysia, *Personal Data Protection Act 2010 (Act 709)*, June 2010, PDP Act 2010 • Protection of Personal Data

31. Parliament of Malaysia, *Personal Data Protection (Amendment) Act 2024*, October 2024, PDP (Amendment) Act 2024 • Protection of Personal Data

32. New Zealand Government, *Privacy Act 2020*, June 2020, Privacy Act 2020 No 31 (as at 30 March 2025), Public Act Contents – New Zealand Legislation

33. New Zealand Privacy Commissioner, *Artificial Intelligence and the Information Privacy Principles*, September 2023, AI-and-the-Information-Privacy-Principles.pdf

34. National Privacy Commission, *Data Privacy Act, 2012*, August 2012, Republic Act 10173 - Data Privacy Act of 2012 - National Privacy CommissionNational Privacy Commission

35. National Privacy Commission, *Joint Advisory - Considerations on the Use Of Privacy Enhancing Technologies (PETs) In The Insurance Industry*, March 2025, NPC-IC-Joint-Advisory-2025.03.11-Considerations-on-the-Use-of-PETs-in-the-Insurance-Industry-w-SGD.pdf

36. National Privacy Commission, *Guidelines on The Application of Republic Act No. 10173 or the Data Privacy Act Of 2012 (DPA), Its Implementing Rules and Regulations, and the Issuances of the Commission to Artificial Intelligence Systems Processing Personal Data*, December 2024, Advisory-2024.12.19-Guidelines-on-Artificial-Intelligence-w-SGD.pdf

37. Singapore Government, *Personal Data Protection Act 2012*, October 2012, Personal Data Protection Act 2012 - Singapore Statutes Online

38. Singapore Government, *Personal Data Protection (Amendment) Act 2020*, December 2020, Personal Data Protection (Amendment) Act 2020 - Singapore Statutes Online

39. Personal Data Protection Commission, *Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems*, March 2024, advisory-guidelines-on-the-use-of-personal-data-in-ai-recommendation-and-decision-systems.pdf

40. Infocomm Media Development Authority (IMDA), Privacy Enhancing Technology Sandbox, Privacy Enhancing Technology Sandboxes | IMDA

41. Personal Data Protection Commission (PDPC), *Proposed Guide to Synthetic Data Generation*, July 2024, proposed-guide-on-synthetic-data-generation.pdf

42. Personal Information Protection Commission, Korea, *Personal Information Protection Act*, September 2023, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly

43. Personal Information Protection Commission, Korea, *Amended Personal Information Protection Act (PIPA) and its Enforcement Decree Become Effective*, September 2023, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly

44. Personal Information Protection Commission, Korea, *The PIPC Sets Out Personal Data Processing Criteria for Generative AI*, August 2025, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA □□, Global Privacy Assembly

45. Personal Information Protection Commission, Korea, *AI Privacy Risk Management Model for Safe Utilization of AI and Data*, December 2024, Press Release Details | Personal Information Protection Commission

46. Personal Information Protection Commission, Korea, *PIPC Unveils Guidelines on Generating and Utilizing Synthetic Data*, December 2024, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly

47. Personal Information Protection Commission, Korea, *Guideline on Processing Publicly Available Data for AI Development and Services*, July 2024, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly

48. Personal Information Protection Commission, Korea, *AI Personal Information Protection Self-checklist*, July 2021, PIPC, Korea, GPA, 2025 GPA, GPA Seoul, 2025 GPA Seoul, AI, Data, Privacy, GPA 서울, Global Privacy Assembly

49. Government of the Republic of China (Taiwan), *Personal Data Protection Act*, May 2023, Personal Data Protection Act - Article Content - Laws & Regulations Database of The Republic of China (Taiwan)

50. Government of the Republic of China (Taiwan), *Enforcement Rules of the Personal Data Protection Act*, March 2016, Enforcement Rules of the Personal Data Protection Act - Article Content - Laws & Regulations Database of The Republic of China (Taiwan)

51. Ministry of Digital Affairs, *Draft Act on Promoting the Development of Data Innovation and Utilization Released for Public Consultation*, August 2025, Draft Act on Promoting the Development of Data Innovation and Utilization Released for Public Consultation — the Ministry of Digital Affairs Drives Data Sharing and AI Development | Press Releases - News and Releases | Ministry of Digital Affairs

52. Personal Data Protection Committee, *Personal Data Protection Act*, May 2019, Personal Data Protection Act B.E. 2562 (2019) - PDPC

53. Personal Data Protection Committee, *Master Plan for the National Promotion and Protection of Personal Data*, April 2024, แผนแม่บททการส่งเสริมและการคุ้มครองข้อมูลส่วนบุคคลของประเทศ พ.ศ. 2567 - 2570 - PDPC

54. Bank of Thailand, *Hearing on the Draft Bank of Thailand Policy Guidelines Risk Management of Artificial Intelligence System*, June 2025, (Draft) Bank of Thailand Policy Guidelines Risk Management of Artificial Intelligence System

55. Government of Vietnam, *Decree 13/2023/ND-CP on Personal Data Protection*, April 2023, 13/2023/ND-CP in Vietnam, Decree No. 13/2023/ND-CP dated April 17, 2023 on protection of personal data in Vietnam

56. National Assembly of Vietnam, *Law of Personal Data Protection 2025*, June 2025, https://thuvienphapluat.vn/van-ban/Bo-may-hanh-chinh/Luat-Bao-ve-du-lieu-ca-nhan-2025-so-91-2025-QH15-625628.aspx?dll=true

Deloitte.

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイトネットワークのメンバーである合同会社デロイト トーマツ グループならびにそのグループ法人（有限責任監査法人トーマツ、合同会社デロイト トーマツ、デロイト トーマツ税理士法人およびDT弁護士法人を含む）の総称です。デロイト トーマツ グループは、日本で最大級のプロフェッショナルグループのひとつであり、各法人がそれぞれの適用法令に従いプロフェッショナルサービスを提供しています。また、国内30都市以上に2万人超の専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループWebサイト、www.deloitte.com/jpをご覧ください。

Deloitte（デロイト）とは、Deloitte Touche Tohmatsu Limited（“Deloitte Global”）、そのグローバルネットワーク組織を構成するメンバーファームおよびそれらの関係法人（総称して“デロイトネットワーク”）のひとつまたは複数を指します。Deloitte Globalならびに各メンバーファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。Deloitte Globalおよびその各メンバーファームならびに関係法人は、自らの作為および不作為についてのみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。Deloitte Global はクライアントへのサービス提供を行いません。詳細はwww.deloitte.com/jp/aboutをご覧ください。

デロイト アジア パシフィック リミテッドは保証有限責任会社であり、Deloitte Globalのメンバーファームです。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィックにおける100を超える都市（オークランド、バンコク、北京、ベンガルール、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、ムンバイ、ニューデリー、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、最先端のプロフェッショナルサービスを、Fortune Global 500®の約9割の企業や多数のプライベート（非公開）企業を含むクライアントに提供しています。デロイトは、資本市場に対する社会的な信頼を高め、クライアントの変革と繁栄を促進することで、計測可能で継続性のある成果をもたらすプロフェッショナルの集団です。デロイトは、創設以来180年の歴史を有し、150を超える国・地域にわたって活動を展開しています。“Making an impact that matters”をパーパス（存在理由）として標榜するデロイトの約46万人の人材の活動の詳細については、www.deloitte.comをご覧ください。

Member of
Deloitte Touche Tohmatsu Limited

Designed by CoRe Creative Services. RITM2335313

IS 669126 / ISO 27001

BCMS 764479 / ISO 22301

IS/BCMSそれぞれの認証範囲はこちらをご覧ください
http://www.bsigroup.com/clientDirectory