Miura & Partners

インド最新法令 UPDATE Vol.10

インドのデジタル個人データ保護法制－規制の全体像と実務対応のポイント－

2026 年 4 月 14 日

弁護士 白井 美和子

インドでは、デジタル経済の拡大とプライバシーに対する権利意識の高まり[1]を受け、2023 年 8 月 11 日に、初の包括的なプライバシー・データ保護法である 2023 年デジタル個人データ保護法（Digital Personal Data Protection Act, 2023。以下「DPDP 法」といいます。）[2]が成立・公布されていましたが、同法は規定の詳細の多くを下位規則に委任していたため、中央政府による規則の公布が待たれている状況でした。このような背景の下、インド電子情報技術省（Ministry of Electronics & Information Technology）は、2025 年 11 月 13 日、①2025 年デジタル個人データ保護規則（Digital Personal Data Protection Rules, 2025。以下「DPDP 規則」といい、DPDP 法と合わせて「DPDP 法令」といいます。）を公布するとともに、②DPDP 法の各規定の施行日を指定しました。これにより、コンプライアンス体制の具体的な構築に必要な運用詳細の多くが明らかとなり、各規定の施行日も確定したことから、各企業は、データ受託者（Data Fiduciary）[3]の義務等主要な規定が施行される 2027 年 5 月 13 日に向けて、DPDP 法令に沿ったコンプライアンス体制の整備を進めています。

本稿では、1. 各規定の施行スケジュール、および、2. 新たに公布された DPDP 規則を踏まえたインドのデジタル個人情報保護体制の全体像を概説した上で、3. インドで事業を展開する日系企業が DPDP 法令の完全施行に向けて対応すべき事項を解説します。

1. 各規定の施行スケジュール

DPDP 法の各規定は、以下のとおりの段階的なスケジュールで施行されます。データ受託者に対する義務等の主要な規定は、DPDP 規則の公布から 18 か月後の 2027 年 5 月 13 日に施行されます。

[1] インドの最高裁判所は、2017 年に、インド政府が導入した生体認証を含む個人識別制度（Aadhaar 制度）の合憲性が争われた事案において、2017 年にプライバシー権をインド憲法上の基本的権利として明確に認める判決を下しました（Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.）。この判決がインドにおけるデジタル個人情報保護法の制定に大きな影響を与えています。

[2] これまでは、一部のセンシティブな個人データおよび情報の保護について、Information Technology Act, 2000 およびその下位規則である Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 等に個別に規定されている状況でした。

[3] DPDP 法では、「データ受託者（Data Fiduciary）」は、個人データの処理の目的および手段を決定する者とされており（法 2 条(i)）、これは欧州連合の一般データ保護規則（General Data Protection Regulation、以下「GDPR」）における「Controller」と同義です。なお、「データ処理者（Data Processor）」は、データ受託者に代わりデータを処理する者を指します（法 2 条(k)）。また、DPDP 法では、データ主体は「Data Principal」と規定されています（法 2 条(j)）。

施行時期	対象規定
即日施行（2025 年 11 月 13 日）	定義、データ保護委員会（Data Protection Board of India）の組織に関する規定等
12 か月後（2026 年 11 月 13 日）	同意管理者（Consent Manager）[4]の登録およびデータ保護委員会の同意管理者に対する権限に関する規定
18 か月後（2027 年 5 月 13 日）	適用範囲、データ受託者の義務、重要データ受託者の追加的義務、データ主体の権利義務、データ保護委員会の権限等、適用除外、罰則等に関する規定

2. DPDP 法令の規制概要

DPDP 法令の主要な規制内容（2025 年 11 月に公布された DPDP 規則において規定された点を含む）は、以下のとおりです。なお、DPDP 法は、GDPR をベースとしているものの、それとは異なる規定も多数存在しており、相違点を意識することが肝要となります。

(1) 適用範囲

DPDP 法は、デジタル形式の個人データの処理に適用されます（法 3 条(a)）。DPDP 法上、「個人データ（Personal Data）」とは、当該データにより、または、当該データに関連して識別可能な個人に対するデータと定義されており（法 2 条(t)）、センシティブな個人データのカテゴリーは設けられていないため、全ての個人データに対して原則として同一の規律が適用されます。また、DPDP 法は物理的な形式で収集されたのちにデジタル化されたデータには適用されますが、物理的な形式のまま保管されているものには適用されません。なお、データ主体が自ら公開した個人データには同法の適用が排除されています（法 3 条(c)(ii)）。これらの点は GDPR や日本の個人情報保護法とは相違があるため留意が必要です。

DPDP 法は、インド国内のデータ主体に対する商品またはサービスの提供に関連してインド国外で処理される個人データにも適用されます（法 3 条(b)）。したがって、インドの消費者に対して商品やサービスを提供している外国企業は、インドに拠点がなかったとしても、DPDP 法の適用対象となる可能性があるため留意が必要です。

(2) 個人データ処理の適法性根拠

個人データの処理は、①データ主体からの同意、または、②特定の正当な利用（legitimate use）のためである場合に許容されます（法 4 条(1)）。

[4] Consent Manager 制度：「同意管理者（Consent Manager）」と呼ばれるデータ保護委員会に登録したプラットフォーム事業者を通じて、データ主体が自らの同意の付与、管理、確認、撤回を一元的に行うことができる仕組みであり、インド特有の制度として導入が予定されています。

① **データ主体からの同意**

データ主体によって与えられる同意は、自由に与えられ、特定され、十分な情報に基づき、無条件であり、かつ積極的行為によって示される明確なものである必要があります。また、当該同意は、特定された目的のためにその個人データが処理されることへの同意を意味し、かつ当該目的のために必要な個人データに限られます（法 6 条(1)）。なお、データ主体はいつでも同意を撤回できます（法 6 条(5)）。

DPDP 規則では、データ受託者がデータ主体から同意を取得する際の通知（Notice）は、以下の要件を満たさなければならないと規定しています（規則 3 条）。また、通知は、英語またはインド憲法第 8 附則に定める 22 の言語のうち、データ主体が選択した言語で閲覧できるようにする必要があります（法 6 条(3)）。

(a) データ受託者から提供されるいかなる情報からも独立して、提示され、かつ、理解可能であること

(b) データ主体による十分な情報に基づく特定された同意の付与に必要な事項について、明確かつ平易な形で公正な説明を提供するものでなければならず、少なくとも、以下の内容を含むこと

  (i) 収集する個人データの項目ごとの記述（an itemised description）、および、

  (ii) 具体的な処理の目的および当該処理により提供される商品・サービス等

(c) データ受託者のウェブサイトやアプリのリンク、ならびに、データ主体が、同意の撤回（なお付与と同程度に容易である必要あり）、DPDP 法上の権利行使およびデータ保護委員会への苦情申立てを行うことができるその他手段の説明を提供すること

DPDP 法におけるこの通知は、十分な情報提供および理解に基づく同意取得の一部として位置づけられており、処理の透明性を主眼とする GDPR の通知と比較して、同意に必要な情報に特化し、データ主体に対するより具体的かつ実務的な方法での情報提供を求めていると考えられます。

② **正当な利用**

同意がなくとも個人データの処理が許容される「正当な利用」となる事由は、DPDP 法 7 条に具体的に列挙されています。政府による公的な目的による処理のほか、特に雇用主による一定の従業員個人データの処理が正当な利用として明示的に認められている点に特色があります。一方、GDPR における「正当な利益（Legitimate Interest）」に相当する包括的な規定は定められていない点に留意が必要です。

(3) データ受託者の一般的な義務

上記(2)の同意等に関する義務のほかに、データ受託者に課される主要な義務は以下のとおりです。なお、データ受託者は、自己に代わってデータを処理する「データ処理者」による処理についても責任を負う点に留意が必要です。

① 合理的なセキュリティ対策

DPDP 規則 6 条は、データ受託者は、最低限のセキュリティ対策として、(a) 暗号化等による適切なデータ保護、(b) アクセス制御、(c) 不正アクセスの検知・調査・再発防止のためのログ管理・監視、(d) データバックアップ、(e) ログおよび個人データの処理日から 1 年間の保存、(f)データ処理者との契約における規定整備、ならびに、(g) 技術的・組織的対策を実施しなければならないと規定しています。これらのセキュリティ対策は、データ受託者が保有または管理する全ての個人データに適用され、データ処理者が処理する個人データにも講ずる必要があることに留意が必要です。

② 個人データ侵害が発生した場合の通知・報告義務

データ受託者は、個人データ侵害の発生を認識した場合、①当該侵害により影響を受けるデータ主体および②データ保護委員会に対し、指定された方法により、「直ちに（immediately）」通知を行う義務があります（法 8 条(6)）。現状、GDPR のようなリスクの閾値は設定されていない点に留意が必要です。

DPDP 規則では、個人データ侵害の場合の通知内容等が具体的に規定されており、①データ主体に対しては、侵害の性質・程度・時期、データ主体への影響、リスク軽減のために講じられた措置、安全対策等を遅滞なく通知しなければならず（規則 7 条(1)）、②データ保護委員会に対しては、遅滞なく侵害の概要を通知するとともに、侵害を認識してから原則として 72 時間以内に詳細な情報を報告しなければならないとされています（規則 7 条(2)）。

③ 個人データの消去義務

データ受託者は、データ主体が同意を撤回した時点、または、同意を取得した目的が果たされなくなったと合理的に考えられる時点のいずれか早い時点で、当該個人データを消去し、データ処理者に当該個人データを消去させる義務を負います（法 8 条(7)）。

DPDP 規則は、一定のデータ受託者について、同意を取得した目的が果たされなくなったとみなされる場合を規定しており、具体的には、インドにおいて 2,000 万人超の登録ユーザーを有する e コマース事業者およびソーシャルメディア事業者ならびに 500 万人超の登録ユーザーを有するオンラインゲーム事業者は、データ主体との最後の接触から 3 年が経過した場合、法令遵守に必要な場合を除き、当該個人データを消去する必要があります（規則 8 条(1)および附則 3）。なお、この場合、消去の 48 時間前までにデータ主体への通知が必要となります。

④ 問い合わせ窓口の公表義務

データ受託者は、データ保護責任者（Data Protection Officer）または問い合わせ対応担当者の連絡先を、ウェブサイトまたはアプリにおいて目立つ形で公表するとともに、データ主体からの権利行使に関する連絡に対する返答において記載する必要があります（規則 9 条）。

(4) 児童の個人データ処理についての追加的義務

データ受託者は、児童（18 歳未満の者）または後見人が指定されている者の個人データを処理する前に、親権者または後見人から、指定された方法により、「検証可能な同意（verifiable consent）」を取得することが義務付けられます（法 9 条(1)）。DPDP 規則では、データ受託者は、親権者からの検証可能な同意を確保するために適切な技術的、組織的な措置を講じ、親権者が識別可能な成人であることを同人から提供された情報等を参照して確認しなければならず（規則 10 条）、また、法定後見人を有する障害者についても同様に、後見人が裁判所等により適法に任命されていることの確認が求められています（規則 11 条）。GDPR では 16 歳未満（加盟国により 13 歳まで引下げ可能）が対象であるのに対し、DPDP 法では 18 歳未満と対象年齢が高く設定されている点に留意が必要です。

また、データ受託者は、児童の福祉に有害な影響を与える恐れのある個人データ処理、ならびに、児童に対する追跡もしくは行動モニタリングおよび児童に向けたターゲット広告を行うことを禁じられています（法 9 条(2)および(3)）。

なお、DPDP 規則は、医療機関が児童の健康保護のために医療サービスを提供する場合等、児童の個人データの処理に関し法 9 条(1)および(3)の適用が免除される場合を具体的に明らかにしています（規則 12 条および附則 4）。

(5) 重要データ受託者（Significant Data Fiduciary）の追加的義務

DPDP 法は、中央政府が、処理する個人データの量・機微性、データ主体の権利に対するリスク等の諸要素を検討した上で「重要データ受託者」となるデータ受託者を指定することができると規定しています（法 10 条(1)）。なお、現状、具体的な重要データ管理者の指定基準は明らかにされていません。

重要データ受託者に指定された者は、①データ保護責任者の選任、②独立したデータ監査人の選任、③12 か月に 1 回のデータ保護影響評価（Data Protection Impact Assessment）および監査の実施ならびに当該評価および監査における重要な所見を記載した報告書の提出、④その他指定された措置の実施が義務付けられます（法 10 条(2)）。DPDP 規則により、④として、アルゴリズムソフトウェアがデータ主体の権利にリスクをもたらさないことの検証や、中央政府が指定する個人データおよびトラフィック・データのインド国外移転禁止措置の実施が義務付けられています（規則 13 条）。

(6) 越境移転

DPDP 法は、かつての草案にあった厳格なデータローカライゼーション（国内保存義務）を撤廃し、ブラックリスト方式を採用しており、中央政府が指定する制限国（ブラックリスト）以外への移転は原則自由とされています（法 16 条(1)）。ただし、セクター別の厳格な規制が優先する場合があるため留意が必要です。なお、現時点では越境移転の制限対象国は明らかにされていません。

上述のとおり、重要データ受託者については、中央政府が指定する個人データについて域外移転が制限されますが（規則 13 条(4)）、対象となる個人データ等は現状明らかにされていません。また、中央政府は、全てのデータ受託者に対し、外国政府、外国政府の機関、または、その管理下にある者への特定の個人データの開示についての要件を定めることができます（規則 15 条）。

(7) 制裁金

DPDP 法への違反に対する刑事罰はありませんが、最大 25 億インド・ルピー（約 42.5 億円 [5]）という極めて高額な制裁金（Penalty）が規定されています。主要な違反行為とその制裁金の上限額は以下のとおりです。

違反行為	制裁金上限
合理的なセキュリティ措置の不履行（法 8 条(5)）	25 億ルピー
個人データ侵害の通知義務違反（法 8 条(6)）	20 億ルピー
児童の個人データに関する義務違反（法 9 条）	20 億ルピー
重要データ受託者の義務違反（法 10 条）	15 億ルピー
その他のデータ受託者による義務違反	5 億ルピー

3. 日系企業に求められる今後の対応

2027 年 5 月の完全施行を見据え、日系企業は以下の対応を進める必要があります。

(1) 施行までのロードマップ策定

日系企業は、データ受託者に関する主要な規定が施行されるまでの期間を活用し、①データマッピング（現状把握）、②ギャップ分析、③システム改修までのロードマップを策定する必要があります。上述のとおり、インド国内のグループ法人だけでなく、商品またはサービス提供のためにインド国内のデータ主体の個人データを処理している日本本社やインド国外の関連法人も域外適用の対象となる可能性があるため留意が必要です。

[5] 1 インド・ルピー＝1.7 円（2026 年 4 月 1 日時点の為替レート）で算定。

(2) コンプライアンス体制の構築

① 同意取得時の通知およびプロセスの刷新

DPDP 法令が求める、通知の多言語対応や個人データの項目別の記述等は既存のシステムでは対応できない可能性があり、DPDP 法令が求める通知要件に応じた同意取得のフローやユーザーインターフェイスの見直しが必要となります。なお、既存の顧客・従業員の個人データに対しても施行後速やかに法令に準拠した通知を行う必要があります（法 5 条(2)）。

また、上述のとおり、インドでは 18 歳未満が児童として厳格な規制の対象となります。インドの顧客に向けて e コマースやオンラインサービスを提供する日系企業は、親権者からの検証可能な同意を取得するための技術的・組織的措置を検討する必要があるとともに、自社の製品および処理活動をレビューし、児童を対象としたトラッキング、行動モニタリング、ターゲティング広告を排除する対応が求められます。

② セキュリティ対策の点検・強化およびデータ侵害対応体制の整備

セキュリティ対策について、DPDP 規則 6 条で最低限講ずべき対策が具体化されたことを踏まえ、現行の IT 環境および運用がこれらの要件を満たしているかを確認し、必要に応じた強化を行うことが急務となります。

また、個人データ侵害が発生した場合、リスク閾値なしの即時通知および 72 時間以内のデータ保護委員会への詳細報告が必要となり、これは実務上極めて重い負担となります。現地法人におけるインシデント検知から本社への報告、当局対応までのフローを確立し、演習を行うことが推奨されます。

③ 委託先管理および契約の見直し

データ受託者は、データ処理者の活動を監督する責任を有しており、データ処理者との契約における規定整備は最低限の合理的セキュリティ対策の一つとして義務付けられています。データ受託者は、データ処理者（委託先）との契約において、DPDP 法令に準拠したセキュリティ対策整備義務、侵害時の管理者への報告義務、監査権限等が含まれているかを確認し、必要に応じて既存の契約を改訂する必要があります。

また、日本本社とインド現地法人、または現地代理店等との間で、共同で個人データの処理を行う場合、DPDP 法には共同管理者に関する明示的な規定がないため、同意取得の主体、データ主体・データ保護委員会との窓口担当、責任分担等について、文書により明確に合意しておくことが重要となります。

(3) 未確定事項等のモニタリング

今回の DPDP 規則でも、越境移転の制限国リスト、重要データ受託者の指定基準、同意管理者のプラットフォーム仕様、重要データ受託者において越境移転が禁止される個人データ等は明らかになっておらず、今後政府により指定される予定である未確定事項が残されています。また、データ保護委員会が本格的に稼働した後に解釈指針やガイドラインが発行されることが予

想されます。したがって、各企業は、中央政府およびデータ保護委員会の今後の動きを継続的にモニタリングし、必要な対応を適時に行う体制を整えることが求められます。

本ニュースレターは、法務等に関するアドバイスの提供を目的とするものではありません。
具体的な案件に関するご相談は、弁護士等の専門家へ必ずご相談いただきますよう、お願いいたします。
また、本ニュースレターの見解は執筆者個人の見解であり、当事務所の見解ではありません。