デジタル個人情報保護規則の公表

2025 年 12 月 15 日
One Asia Lawyers 南アジアプラクティスチーム
吉田　重規 (弁護士・日本法)
山田 薫

2023 年 8 月に成立した、インド初の包括的な個人情報保護法令となる「2023 年デジタル個人情報保護法（DPDP 法）」[1]に関し、その運用の詳細を定めた「2025 年デジタル個人情報保護規則（DPDP 規則）」[2]が 2025 年 11 月 14 日に公表されました。これに合わせて DPDP 法の段階的な施行タイムラインも公表されました。

DPDP 法および DPDP 規則は 3 段階で施行されることとなり、個人情報の取り扱いに係る企業の義務に関連する規定は、企業の遵守のため 18 か月の準備期間が設けられ、**2027 年 5 月 13 日より施行開始**となります[3]。

しかしながら、今回の公表内容ですべてがクリアになったわけではなく、「具体的な対策が見えた領域」と、「依然として今後の通知待ちとなる領域」が混在しています。

本ニュースレターでは、DPDP 法における企業義務の全体像」を整理した上で、規則により明確化された具体的実務と、今後の注視が必要な事項について解説いたします。

1．DPDP 法における企業の主な義務（全体像）

DPDP 法において、個人情報を取り扱う企業（Data Fiduciary[4]）には、主に以下の義務が課されています。今回の規則は、これらの義務の「具体的な履行方法」を定めたものです。

- **適法な根拠に基づく処理:** 本人の同意、または正当な目的（Employment purposes 等）に基づく処理
- **通知（Notice）と同意（Consent）：** 使用目的等の通知と、明確な同意の取得
- **正確性と完全性:** 本人に影響を与える決定を行う場合等の正確性確保
- **合理的なセキュリティ保護措置:** データ侵害を防ぐための技術的・組織的対策の実施
- **侵害時の報告:** 漏洩時の規制当局（Data Protection Board、「DPB」）および本人への報告
- **保存制限（消去義務）：** 利用目的達成後のデータ消去
- **データ主体の権利対応:** 本人からのアクセス請求、訂正、消去、苦情申立への対応
- **苦情処理体制（Grievance Redressal）：** 苦情対応責任者の設置、対応
- **重要データ管理者（Significant Data Fiduciary、「SDF」）の追加義務**：指定された事業者への追加義務。ただし SDF の指定基準は現時点で未定
- **越境移転：**現状は原則転送可。ただし、越境移転の具体的要件や制限国リスト等は今後追加可能あり。
- **罰則**：罰金は**最高 25 億ルピー**（約 45 億円）と高額

---

[1] Digital Personal Data Protection Act, 2023：
https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
[2] Digital Personal Data Protection Rules, 2025：
https://www.meity.gov.in/static/uploads/2025/11/53450e6e5dc0bfa85ebd78686cadad39.pdf
[3] DPDP 法の施行タイムライン：
https://www.meity.gov.in/static/uploads/2025/11/c56ceae6c383460ca69577428d36828b.pdf
[4] GDPR 等の管理者「Controller」に相当

２．【明確化した事項】直ちに対応検討が必要なポイント

今回の規則公表により、上記の義務のうち、特に「セキュリティ対策」と「有事の対応」について具体的な基準が示されました。これらはIT システムや運用フローに直結するため、以下の点について、現行運用とのギャップ分析が急務となります。

① 合理的なセキュリティ保護措置

規則第 6 条（Reasonable security safeguards）において、企業が講ずべき「最低限（at the minimum）」のセキュリティ対策が具体的に例示されました。なお、自社（Data Fiduciary）だけでなく、委託先（Data Processor）における処理も管理対象となります。

(a) データの秘匿化技術の導入：適切なデータセキュリティ措置（appropriate data security measures）を講じること（**例（such as）**：、**暗号化**（encryption）、**難読化**（obfuscation）、**マスキング、バーチャルトークン**の使用）
▶ 実務対応：条文上は「暗号化、難読化、マスキング等」が例示されています。これら（または同等以上の技術）を採用せずにデータ侵害が発生した場合、「合理的・適切な保護措置」を講じていなかったと判断されるリスクがあるため、実務上は、保管・通信データの暗号化や、開発・テスト環境におけるマスキング処理などの措置が強く求められます。

(b) アクセス制御の徹底：コンピュータ・リソースへの適切な**アクセス制御**措置
▶ 実務対応：ID 管理、多要素認証導入、最小権限の原則に基づくアクセス権限の棚卸しが求められます。

(c) ログ監視と検知体制：不正アクセスの検知・調査・再発防止を可能にするための、適切なログ取得、モニタリング、およびレビューによる「可視化（Visibility）」
▶ 実務対応：ログを取るだけでなく、定期的なレビューや異常検知時のアラート体制が求められることとなります。

(d) 侵害時の事業継続・回復措置（バックアップ等）：データ破壊やアクセス喪失により、機密性・完全性・可用性が侵害された場合でも、処理を継続するための措置（**データバックアップ**等）
▶ 実務対応：ランサムウェア対策等を想定したバックアップ体制とリストア手順の整備が含まれます。

(e) ログおよび関連データの「1 年間」保存義務：不正アクセスの検知・調査・再発防止を可能にするため、当該ログおよび関連する個人データを、原則として**「1 年間」保持**すること
▶ 実務対応：多くの企業でログ保存期間は「3 ヶ月～6 ヶ月」の設定が見られますが、インドにおいては「1 年」への設定変更と、それに伴うストレージ容量の確保が必要となり、**コストに直結**する可能性があります。

(f) 委託先との契約義務：委託先となるデータ処理者との**契約**において、合理的なセキュリティ保護措置を講じる旨の規定を設けること
▶ 実務対応：既存のベンダー契約（Data Processing Agreement 等）を見直し、必要に応じて本規則に準拠したセキュリティ条項を追加する必要があります。

(g) 実効性を確保するための技術的・組織的対策：上記の保護措置が実効的に遵守されるための、技術的および組織的対策
▶ 実務対応：定期的なセキュリティ監査や従業員トレーニング等が該当します。

② データ漏洩時の報告期限（72 時間ルール）
データ侵害（Data Breach）を認知してから「72 時間以内」に、DPB および影響を受ける本人への報告が義務付けられました（規則第 7 条(2)(b)）。
▶ 実務対応：金曜夜間にインシデントが発覚した場合などを想定し、誰が判断し報告を行うか、緊急時連絡体制（エスカレーションフロー）の策定が必要です。

３．今後の見通しと未確定事項

セキュリティ要件等が明確となった一方で、日本企業にとって重要な関心事である以下の点については、今回の規則本体には詳細が含まれておらず、今後の追加通知やガイドラインによって補完される見込みです。

- **越境移転（Cross-border transfer）の具体的規制**
  現時点では、特定の国への移転を禁止する「ブラックリスト方式」等の詳細基準は明示されていません。今後の通知により、制限国リスト、要件付き転送、認証や契約条件など、具体的な制限が示される可能性があります。
- **重要データ管理者（Significant Data Fiduciary）の指定基準**
  どのような規模・種類のデータを扱う企業が、より重い義務（外部監査、インパクト評価実施と DPO への報告、インド居住データ保護責任者（DPO）設置等）を負う「重要データ管理者」に指定されるか、その閾値は未定です。
- **過去のデータの取り扱い（遡及適用）**
  DPDP 法上、同法施行前に本人同意を取得している場合でも、**施行後は速やかに同法に準拠した通知を行う義務**が生じます（第 5 条(2)(a)）。企業は、過去に同意に基づき取得した個人情報を遡って確認し、そのデータ主体を特定した上で、DPDP 法第 5 条 2 項が施行される 2027 年 5 月 13 日以降、実務上できる限り速やかに通知を行う実務負担が発生することとなります。ただし、過去のどの時点まで遡及すべきか、改めて通知を行うべき範囲・手順については明確化されていません。

なお、今後の追加通知は、インド電子情報技術省の公式サイト上に順次公開されていく方式が採られる模様です[5]。本ニュースレター発行時点では、DPDP 法および規則の条項ごとの施行タイミング（タイムフレーム）と、DPB の委員数が「4 名」に決定されたことのみが通知されており、具体的な運用体制の大部分が通知ベースで追加されていくことが見込まれます。

４．日本企業における実務上の留意点と、今からやっておくべき準備

規則第 6 条の要件は非常に具体的であり、IT・セキュリティ面および法務・コンプライアンス面の両面での対応が求められます。
まずは IT 部門との連携の上、上記の要件について、特に「ログ保存期間 1 年」や暗号化等の秘匿化技術に関し、現行システムが準拠しているかの確認が強く推奨されます。
同時に、「どのデータが・どこに・何のために」あるかを可視化するデータマッピングを完了させておき、越境規制や消去義務の詳細が決まった際に即座に対応できる体制整備も必須と

[5] https://www.meity.gov.in/documents/act-and-policies/digital-personal-data-protection-rules-2025-gDOxUjMtQWa?pageTitle=Digital-Personal-Data-Protection-Rules-2025

なります。また、委託先との契約レビュー、プライバシーポリシーや同意書の改訂準備を進めつつ、今後の追加通知を注視する必要があります。
One Asia Lawyers では、引き続きインド当局の通知をモニタリングし、実務への影響を随時発信してまいります。

以上

ONE ASIA LAWYERS

◆ One Asia Lawyers ◆

「One Asia Lawyers Group は、アジア全域に展開する日本のクライアントにシームレスで包括的なリーガルアドバイスを提供するために設立された、独立した法律事務所のネットワークです。One Asia Lawyers Group は、日本・ASEAN・南アジア・オセアニア各国にメンバーファームを有し、各国の法律のスペシャリストで構成され、これら各地域に根差したプラクティカルで、シームレスなリーガルサービスを提供しております。

この記事に関するお問い合わせは、ホームページ https://oneasia.legal または info@oneasia.legal までお願いします。

なお、本ニュースレターは、一般的な情報を提供することを目的としたものであり、当グループ・メンバーファームの法的アドバイスを構成するものではなく、また見解に亘る部分は執筆者の個人的見解であり当グループ・メンバーファームの見解ではございません。一般的情報としての性質上、法令の条文や出典の引用を意図的に省略している場合があります。個別具体的事案に係る問題については、必ず各メンバーファーム・弁護士にご相談ください。

＜著者紹介＞

<table>
<tr>
<td>  </td>
<td>吉田 重規
One Asia Lawyers 南アジアプラクティスチーム
インド提携事務所パートナー弁護士（日本法）
2018 年 One Asia Lawyers 加入、2025 年より南アジアオフィス所属。クロスボーダーM&A などの日系企業進出支援業務のほか、インド企業法務全般に関するサポートを行っている。
One Asia Lawyers 加入前は約 6 年間企業内弁護士として企業法務全般に従事し、同所加入後はカンボジアを中心に東南アジアにおける日系企業への幅広い分野の法務案件を扱ってきた。
shigeki.yoshida@oneasia.legal</td>
</tr>
<tr>
<td>  </td>
<td>山田 薫
One Asia Lawyers 南アジアプラクティスチーム
パラリーガル

2021 年 One Asia Lawyers 南アジアオフィス加入。国際協力機関や在インド日系企業での勤務経験を活かし、南アジア各国の現地弁護士と協働して進出日系企業に対する法的なサポート、各種法律調査等を行う。
kaoru.yamada@oneasia.legal</td>
</tr>
</table>