「2025年インドデジタル個人データ保護規則―日本企業への影響と次のステップ（日本のデータ保護実務家の視点から）」

（「日本DPO協会　第47回個人情報保護セミナー」
「2025年インドデジタル個人データ保護規則―日本企業への影響と次のステップをインド及び日本のデータ保護実務家が解説」（2025年12月18日））

一般社団法人日本DPO協会 事務局長
Ikigai法律事務所ニューデリー・バンガロールオフィス・客員外国弁護士
S&K Brussels法律事務所　事務所代表・パートナー
弁護士（日本・ニューヨーク州・ブリュッセル（B-List）　杉本 武重
takesehige.sugimoto@sandkbrussels.com
https://www.sandkbrussels.com/

S&K Brussels

© S&K Brussels LPC 2023-2025 All Rights Reserved.

杉本 武重
Takeshige Sugimoto

takeshige.sugimoto@sandkbrussels.com
https://en.sandkbrussels.com/
T+81-3-6410-8315; +32 494 67 33 51; +1 212 653 0640
S&K Brussels法律事務所
東京：〒143-0016　東京都大田区大森北1-17-13 ACN大森駅前ビル6階
ブリュッセル：Bastion Tower Level 12, Place du Champ de Mars 5, box 14, Brussels 1050 Belgium
ニューヨーク：1330 Avenue of the Americas, Suite 23, New York, NY 10019 USA

＜弁護士会登録＞

2006年　弁護士登録（59期）
　　第一東京弁護士会所属
2013年　ニューヨーク州弁護士会所属
　　ブリュッセル弁護士会（B-List）所属

一般社団法人日本DPO協会事務局長／Ikigai法律事務所ニューデリー・バンガロールオフィス・客員外国弁護士／S&K Brussels法律事務所東京・ブリュッセルオフィス　パートナー弁護士（日本（第一東京弁護士会）・ニューヨーク州・ブリュッセル（B-List））　杉本 武重

経歴

2000年　駒場東邦高等学校卒業
2004年　慶應義塾大学法学部法律学科卒業
2006-2013年　長島・大野・常松法律事務所アソシエイト
2012年　シカゴ大学ロースクール法学修士課程卒業(LL.M)
2013年　オックスフォード大学法学部法学修士課程卒業(MJur)
2013-2014年　WilmerHale法律事務所ブリュッセルオフィスアソシエイト、2015-2017年同オフィスシニアアソシエイト
2015年-2021年、2023年-2024年　デュッセルドルフ日本商工会議所法務専門委員
2016-2017年　公正取引委員会競争政策研究センター客員研究員
2017-2018年　Gibson Dunn & Crutcher法律事務所ブリュッセルオフィスオブカウンセル
2018-2019年　Bird & Bird法律事務所ブリュッセルオフィス・パートナー
2022-2024年　Future of Privacy Forum (FPF)（ワシントンDC）シニアフェロー
2019年-現在　当事務所開設・代表パートナー（-2024年）、パートナー（2024年-）
2019年-現在　（一社）日本DPO協会設立発起人理事（-2024年）、事務局長（2024年-）
2024年-現在　Ikigai法律事務所ニューデリー・バンガロールオフィス・客員外国弁護士

最近の主要講演

- 講演「インドデジタル個人データ保護法および規則への企業実務対応」（Ikigai Law & S&K Brussels共催「インド個人データ保護法セミナー」（2025年12月17日）インド・ニューデリー@インド日本商工会会議室）
- Roundtable Discussion「米国におけるデータプライバシー規制・AI規制の動向と今後の展望＆司法省による懸念国へのデータ越境移転の規制と日本企業の実務対応～故意の違反の場合、禁錮刑などの刑事罰も～」（2025年9月4日）（日本経済団体連合会米国事務所会合）
- 講演「「米国プライバシー権法」草案と企業の対応」（JCAW ハイブリッドセミナー6月研修会（2024年6月6日）（JCAW ワシントン日本商工会主催））

主要な取扱分野

- EU: ①デジタル関連法：一般データ保護規則（GDPR）、データ法、AI法、サイバーレジリエンス法、デジタルサービス法、データガバナンス法、その他EU立法機関（欧州委員会、EU理事会、欧州議会）で検討中の法案、②競争関連法：競争法、デジタル市場法、③EU宇宙法案
- 米国：①州レベルのデータ保護・プライバシー法・AI規制法、カリフォルニア州消費者プライバシー法（CCPA）その他の州法、②連邦レベルのデータ保護・プライバシー法・AI規制法（㋐個人情報の取扱いに対する規制：児童オンラインプライバシー保護法（COPPA）、その他の連邦法、連邦取引委員会法（FTC法）第5条、その他連邦議会において検討中の法案、㋑機微個人データの越境移転に対する規制：外国の敵対勢力から米国人のデータを保護する法律、懸念国又は対象人による米国人の機微個人データ及び政府関連データへのアクセスに関する司法省規則、㋒AI規制法：連邦議会において検討中の法案）
- インド：デジタル個人データ保護法・規則、AI関連規制、競争法、労働法・雇用関連法
- 日本：データ規制関連法：個人情報保護法・マイナンバー法、経済安全保障推進法等の機微技術情報等に関する規制、不正競争防止法等の営業秘密保護に関する規制、電気通信事業法、AI規制関連法、独占禁止法、宇宙開発法
- グローバル：英国、シンガポール、中国、ブラジル、ベトナム、インドネシア等のデータ保護・プライバシー保護法・AI規制法・宇宙法

© S&K Brussels LPC 2023-2025 All Rights Reserved.

アジェンダ（講演「インドデジタル個人データ保護法および規則への企業実務対応」）

I. インドのデジタル個人データ保護法の概要 4
II. インドのデジタル個人データ保護法のコンプライアンス対応プロジェクトの概要 11
III. インド2025年デジタル個人データ保護規則（DPDP規則） 63

© S&K Brussels LPC 2023-2025 All Rights Reserved.

I. インドのデジタル個人データ保護法の概要

© S&K Brussels LPC 2023-2025 All Rights Reserved.

インド2025年デジタル個人データ保護規則（DPDP規則）

- 2025年11月13日、インド電子・情報技術省（MeitY）は、インド2025年デジタル個人データ保護規則（**DPDP規則**）を告示し、インド初の包括的データ保護法の実施に向けた大きな節目となった。
- DPDP規則は、2023年デジタル個人データ保護法（**DPDPA**）について、DPDPAの主要領域に関する実施規定を具体化することにより、同法の運用面の明確性を与える。
- これらの領域には、通知および同意、子どものデータの処理、最低限のセキュリティ保護措置、個人データ侵害の通知、データの越境移転、ならびに重要データ受託者の追加責任に関する事項が含まれる。
- 最終化されたDPDP規則は、2025年1月3日にパブリック・コンサルテーションのために公表された2025年デジタル個人データ保護規則（草案規則）を踏まえて策定された。
- 概して、最終化されたDPDP規則は草案規則と大部分で整合しており、変更は軽微な精緻化および明確化にとどまる。
- 本スライドでは最終化されたDPDP規則の内容をふまえて日本企業によるインドDPDPA・DPDP規則のコンプライアンス対応の実務について詳細に解説する。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAの基本概念

■ 適用範囲（DPDPA3条）
- DPDPAは、インド領域内におけるデジタル個人データの処理に適用されるが、その前提として、当該個人データが（i）デジタル形態で収集されたもの、又は（ii）非デジタルで収集された後にデジタル化されたものであることが要求される（3条(a)）。
- また、DPDPAには域外適用があり、インド領域内のデータ主体に対して商品又はサービスを提供することに関連する活動に関して、インド領域外で処理されるデジタル個人データにも適用される（3条(b)）。
- 一方で、DPDPAは、（i）個人による個人的又は家庭内目的の処理、及び（ii）データ主体又は（インド法上の義務により）他者によって一般に入手可能にされた個人データには適用されない（3条(c)）。

■ 「個人データ」「デジタル個人データ」
- 個人データとは、個人に関するデータであって、当該データにより、又は当該データに関連して、当該個人が識別されるものをいう。
  - 個人データには、氏名、電話番号、電子メールアドレス、住所等の識別情報に限られず、オンライン上の識別子、利用履歴、嗜好等のプロファイリングに用い得る情報も含み得る（もっとも、具体的に「個人を識別し得るか」は文脈依存である）。
- デジタル個人データとは、デジタル形態の個人データをいう。
- Aadhaar番号
  - Aadhaar番号は、インド固有識別番号庁（UIDAI）が所管する識別制度に基づく識別子であり、DPDPA上も「個人を識別し得るデータ」として個人データに該当し得る（ただし、Aadhaar固有の取扱いは別法制（Aadhaar法等）の影響も受け得るため、実務では個別確認が必要となる）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAの基本概念

■ 「デジタル」の限定と非個人データ
- DPDPAの対象はデジタル個人データであり、紙媒体等の非デジタル記録は、それがデジタル化されない限り直接の対象にならない。
- また、匿名化により個人が識別されない情報（非個人データ）は、定義上、DPDPAの対象外となる（ただし、匿名化が不十分で再識別可能な場合には個人データと評価され得る点に留意する）。

■ 「一般に入手可能」例外と留意点
- DPDPAは、データ主体が自ら一般に入手可能にした個人データ、又はインド法上の義務により他者が一般に入手可能にした個人データには適用されない。
  【例】個人Xがブログ等で自身の見解を発信する際、ソーシャルメディア上で自ら個人データを一般に入手可能にした場合、当該個人データについてDPDPAは適用されない。
- ただし、DPDPAの適用除外であることと、他法令・契約・不法行為・プラットフォーム規約上の適法性が確保されることは別問題であるため、実務上は切り分けて評価するのが安全である。

■ 「処理」の概念
- DPDPAにおける「処理」は、データの収集、記録、組織化、保存、共有等を含む広い概念であり、デジタル／自動化に限定されない（ただし、法の対象が「デジタル個人データ」である点が入口要件となる）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAの基本概念

- 自社がデータ受託者とデータ処理者のいずれに該当するのかを、事業内容及び実際のデータ処理の態様に基づいて確認する必要がある。

  - データ受託者（Data Fiduciary）
    - 単独で、又は他の者と共同して、個人データの処理の目的及び手段を決定する者をいう（2条（i））。データ受託者は、自己が行う処理のみならず、自己のためにデータ処理者が行う処理についても、本法及びこれに基づく規則が遵守されることを確保する責任を負う。

  - データ処理者（Data Processor）
    - データ受託者に代わって個人データを処理する者をいう（2条（k））。データ処理者は、DPDPA上、原則として直接の義務を負わないが、データ受託者との間で締結される有効な契約に基づき、個人データを処理する立場にある。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAの基本概念

データ受託者の一般的義務（DPDPA8(1)-(11)）
8条（1）データ受託者は、データ主体が本法に規定された義務と反対の合意をした場合又は当該義務を履行しなかった場合であっても、データ処理者が自己のために又は自己に代わって行う処理を含め、本法の規定及び本法に基づく規則を遵守する責任を負う。 8条（2）データ受託者は、有効な契約に基づいてのみ、データ主体への商品又はサービスの提供に関連する活動のために、データ処理者を雇用し、選任し、使用し、又はその他の方法で関与させ、自己に代わって個人データを処理させることができる。 8条（3）データ受託者が処理する個人データが、(a) データ主体に影響を与える決定を行うために使用され、又は (b) 他のデータ受託者に開示される場合には、当該個人データを処理するデータ受託者は、当該個人データの完全性、正確性及び一貫性を確保しなければならない。 8条（4）データ受託者は、本法及び本法に基づく規則の規定の効果的な遵守を確保するため、適切な技術的及び組織的措置を講じなければならない。 8条（5）データ受託者は、個人データの侵害を防止するため、合理的なセキュリティ保護措置を講じることにより、自己が保有し、又は自己の管理下にある個人データを保護しなければならない。 8条（6）データ受託者は、個人データの侵害を認識した場合、DPBI及び影響を受ける各データ主体に対して、所定の書式及び方法により、その旨を通知しなければならない。 8条（7）データ受託者は、施行中の法律に従うために当該個人データの保管が必要な場合を除き、次のことを行わなければならない。 (a) データ主体が同意を撤回した場合又は特定された目的がもはや果たされていないとみなすことが合理的である場合のいずれか早い時点で、個人データを消去すること。 (b) データ受託者がデータ処理者に処理のために提供した個人データを、データ処理者に消去させること。 8条（8）8条（7）（a）にいう目的は、規則において定められた期間にわたり、データ主体が、特定された目的の遂行のためにデータ受託者に接触することも、当該処理に関連して自己の権利を行使することも行わない場合には、もはや果たされていないものとみなされる。 8条（9）データ受託者は、データ保護オフィサー（該当する場合）又はデータ受託者に代わって、データ主体の個人データの処理に関してデータ主体からの質問に回答することのできる者の業務連絡先を、所定の方法により公表しなければならない。 8条（10）データ受託者は、データ主体からの苦情を解決するための効果的なメカニズムを確立しなければならない。 8条（11）本条において、データ主体が、特定された目的の遂行のために、データ受託者に対して直接又は電子的若しくは物理的な通信手段により接触していない期間については、データ主体はデータ受託者に接触していないものとみなされることを明確にする。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAの制裁金制度

- DPDPAにおいては、義務違反の内容に応じて異なる制裁金額が定められている（33条（1）、別表）。
  - データ受託者は、具体的な制裁金が規定されていないDPDPA又は規則の規定に違反した場合、5億インドルピー（約9億円）以下の制裁金を課される可能性がある。
  - 個人データ侵害を防止するための合理的な安全保護措置を講じる義務を履行しなかった場合、25億インドルピー（約43億円）以下の制裁金を課せられる可能性がある。
  - 侵害の性質、重大性、期間、影響を受けた個人データの種類や性質、侵害の反復性など、適切な制裁金を決定するために考慮される一般的なパラメータを定めている。
  - 中央政府は、2倍以内の範囲内で別表に記載する制裁金の額を改正する権限を有する（42条（1））

違反	制裁金
個人データの侵害を防止するための合理的な安全管理措置を講じるデータ受託者の義務の違反（8条(5)）	25億インドルピー（約43億円）以下
DPBI又は影響を受けるデータ主体への個人データ侵害通知義務の違反（8条(6)）	20億インドルピー（約34億円）以下
子供に関する追加的な義務の違反（9条）	20億インドルピー（約34億円）以下
重要なデータ受託者の追加的な義務の違反（10条）	15億インドルピー（約26億円）以下
データ主体の義務違反（15条）	1万インドルピー（約17,000円）以下
自発的な確約であってDPBIが受け入れたものの条件に違反した場合（32条）	28条に基づく手続きが開始される違反に適用される範囲
DPDPA又はその規則のその他の規定違反	5億インドルピー（約9億円）以下

© S&K Brussels LPC 2023-2025 All Rights Reserved.

II. インドのデジタル個人データ保護法のコンプライアンス対応プロジェクトの概要

© S&K Brussels LPC 2023-2025 All Rights Reserved.

DPDPAコンプライアンス対応プロジェクトの全体像

Step 1：DPDPAコンプライアンス対応プロジェクトの立ち上げ

- DPDPA対応関係者によるDPDPAの内容の把握、及び経営陣への説明
- DPDPAコンプライアンス対応プロジェクトの立ち上げ、DPDPA対応の外部専門家の選定、DPDPA対応計画の策定と開始

Step 2：コンプライアンス対応のための事実調査、法的評価及び社内体制・規程の整備

Step 2-1-1：データマッピング（事実調査）の実施

- DPDPAの適用対象となる個人データにつき、データフロー、すなわち、取得する個人データの情報源・種類、処理目的、保持期間、個人データの移転状況を網羅的にリストアップし処理業務のリスト（処理記録）を作成
- ✓ データマッピング質問票への回答やインタビューを併用して事実を把握する

Step 2-1-2：データマッピングの結果得られた事実に基づく法的評価

- 個人データの取得、利用、移転の関係での自社のDPDPA上の位置づけの整理とそれに基づく対応事項の検討

Step 2-1-3：データマッピングの結果に基づくコンプライアンス文書の作成

- プライバシーポリシー・通知、同意書、処理契約等の作成

Step 2-2：社内体制・規程の整備

- 個人データの処理に係る社内体制・規程（データ保護マネジメントシステム規程等）の作成・見直し
- 個人データのセキュリティ手続き・実務に係る社内規程の作成・見直し
- データ主体からの請求に係る社内体制の整備・見直し
- 権利行使対応マニュアルの作成・見直し
- データ侵害発生時の対応マニュアルの作成・見直し
- 必要な研修プログラムの検討

Step 3：コンプライアンス措置の実施

- Step 2-1-3で作成・更新したプライバシーポリシーの掲載・データ主体への通知、データ主体からの同意の取得、処理者等との契約締結
- 社内関係者に対する周知徹底、研修等

Step 4：継続的なコンプライアンス対応

- データ主体からの請求への対応
- 従業員の研修の実施

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 1：DPDPAコンプライアンス対応プロジェクトの立ち上げ

- DPDPA対応関係者において、DPDPA及びDPDP規則の内容を把握する。
  - 欧州連合（EU）の一般データ保護規則（GDPR）等への対応のために、既にデータ保護部門が設置されている場合は、当該データ保護部門がDPDPA対応を主導することが考えられる。
  - 専門化・特化したデータ保護部門が設置されていない場合は、法務部、総務部、情報セキュリティ部門、インド担当部門等の代表者により横断的な対応体制を構築することが考えられる。
  - インド拠点において日本本社から独立してDPDPA・DPDP規則へのコンプライアンス対応を行わなければならないケースが相当多いものと考えられる。この場合の日本本社の既存の個人情報保護体制との整合は求められるものと考えられるため、日本本社との連携は必要となると考えられる。

- 制裁金制度、データ主体からDPBIへの苦情申立て、データ侵害発生時の通知対応等の可能性を踏まえ、DPDPA対応の重要性、想定されるリスク及び必要なリソース（人員、予算、システム対応等）を経営陣に説明する必要がある。

- 経営陣の承認を得て、DPDPA対応チームを設置し、DPDPA対応に係る助言を求めるべき外部専門家（インド法及び実務に通じた弁護士、コンサルタント等）を選定する。

- 体制を整えた上で、DPDPAコンプライアンス対応プロジェクトを立ち上げる。

- DPDPA対応計画（スコープ、優先順位、成果物、スケジュール、責任分担、外部委託範囲等）を策定し、その実施を開始する。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 1：DPDPAコンプライアンス対応プロジェクトの立ち上げ
基礎知識（適用範囲）

- DPDPAは、次のいずれかの要件を満たすデジタル個人データの処理に適用される（3条（a）及び（b））。
  - ① インド領域内において行われるデジタル個人データの処理（3条（a））であって、次のいずれかに該当する場合
    - 個人データがデジタル形式で収集されたものである場合（3条（a））
    - 個人データが非デジタル形式で収集された後にデジタル化されたものである場合（3条（a））
  - ② インド領域外において行われるデジタル個人データの処理（3条（b））であって、当該処理が、インド領域内のデータ主体に対する商品又はサービスの提供に関係する活動に関連して行われる場合（3条（b））

- 一方、DPDPAは、次のいずれかの要件を満たす個人データについては適用されない（3条（c））（このほか、個別の適用除外規定が置かれている）。
  - ① 個人的又は家庭内の目的のために、個人によって処理される個人データ（3条（c））
  - ② 次の者によって一般に入手可能なものとされた個人データ（3条（c））
    - 当該個人データに係るデータ主体（3条（c））
      例えば、個人Xがブログで自身の意見を発信するに際し、ソーシャルメディア上で自己の個人データを公開した場合、当該個人データについてDPDPAの規定は適用されない（3条（c））。
    - インドにおいて施行中の法律に基づき、当該個人データを一般に利用可能なものとする義務を負う者（3条（c））

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 1：DPDPAコンプライアンス対応プロジェクトの立ち上げ
基礎知識（関連主体）

- インドに拠点を有しない場合であっても、インド市場に商品又はサービスを提供する日本企業にとっては、DPDPAに基づきデータ受託者としての義務を履行する必要が生じ得る。

  - 特に、子供の個人データを処理する場合、又は、インド政府により「重要なデータ受託者」に指定された場合には、通常のデータ受託者に課される義務に加えて、追加的な義務が課せられる（9条、10条）。

  - DPDPAにはデータ処理者の定義規定は置かれているものの、データ処理者に対して直接義務を課す規定は設けられていない。そのため、データ処理者を利用する場合であっても、DPDPA及びDPDP規則の遵守については、原則としてデータ受託者が責任を負う構造となっている。

  - DPDPAは、データ主体に対しても一定の義務を課しており、例えば、虚偽又は軽率な苦情の申立ての禁止、虚偽の情報提供の禁止等が定められている（15条）。

  - また、DPDPAには、他の個人情報保護法制には必ずしも見られない特殊な関係主体として、「同意管理者」に関する規定が置かれている。同意管理者は、データ主体に代わって同意の付与、管理、見直し又は撤回を行う主体として位置付けられており、これに関する規定は、6条（7）、6条（8）及び6条（9）等に定められている。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 1：DPDPAコンプライアンス対応プロジェクトの立ち上げ
基礎知識（関連主体）

データ受託者	単独で、又は、他者と共同で、個人データの処理の目的及び手段を決定する者（2条（i））
重要な データ受託者	データ受託者またはデータ受託者の類型であって、DPDPA10条に基づき中央政府が指定し、その旨を告示したもの（2条(z)）。 中央政府は、(a) 処理する個人データの量および機微性、(b) データ主体の権利に対するリスク、(c) インドの主権および統一性に対する潜在的影響、(d) 選挙民主主義に対するリスク、(e) 国家安全保障、(f) 治安その他の関連要素を考慮して、重要データ受託者を指定し、告示する（10条）。
データ処理者	データ受託者のために個人データを処理する者（2条（k））
データ主体	個人データがその個人に関するものである当該個人（2条（j）） ✓ 当該個人が子供であるときは、当該子供の親又は適法な後見人が含まれる ✓ 当該個人が障がい者であるときは、当該者のために行為する適法な後見人が含まれる
同意管理者	データ主体が、アクセス可能で透明性があり相互運用可能なプラットフォームを通じて、自己の同意を付与し、管理し、見直し、撤回できるようにするための単一の窓口として機能する者であって、データ保護委員会に登録されたもの（2条(g)）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2：コンプライアンス対応のための事実調査、法的評価及び社内体制・規程の整備

- Step2（コンプライアンス対応のための事実調査、法的評価及び社内体制・規程の整備）は、DPDPAコンプライアンス対応プロジェクトの中核に当たり、次の内訳から成る
  - Step2-1：事実調査及び法的評価
    - Step2-1-1：データマッピング（事実調査）の実施
    - Step2-1-2：データマッピングの結果得られた事実に基づく法的評価
    - Step2-1-3：データマッピングの結果に基づくコンプライアンス文書の作成
  - Step2-2：社内体制・規程の整備
- Step2-1及び2-2は並行して実施する

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-1：データマッピング（事実調査）の実施

- データマッピングとは、DPDPAの適用対象となるデジタル個人データについて、データフロー、すなわち、当該データの取得から利用、保存、移転及び削除に至るまでの処理及び移転の詳細を網羅的にリストアップするプロセスをいう。

- 具体的には、少なくとも次の事項を把握・整理する。
  - 取得する（又は既に取得している）デジタル個人データの情報源及び種類
    - 個人データが非デジタル形式で収集された後にデジタル化された場合も、DPDPAの適用対象となることに留意する（3条（a）（ii））。
    - DPDPAの適用開始前に既に取得しているデジタル個人データについても把握する必要があることに留意する（5条（2））。
    - 子供の個人データを処理する場合には、追加的な義務が課されていることに留意する（9条）。
  - 当該デジタル個人データの処理目的
  - 当該デジタル個人データの保持期間
    - 当該デジタル個人データについて法定の保管期間が定められている場合にはその旨を明記する（8条（7））
  - 当該デジタル個人データの移転状況

- 移転の有無、移転先、移転の目的等を整理する。

- データマッピングは、これらの情報に基づき、処理業務の一覧（処理記録）を作成し、法的評価の前提となる事実を的確に把握することを目的とする。

- 実務上は、データマッピング質問票への回答と関係者へのインタビューを併用して実施し、主管部門（データ保護部門又は法務部門等）が全体を取りまとめることが望ましい。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-1：データマッピング（事実調査）の実施：データマッピング質問票（サンプル）1/3

	データ処理の目的	データが処理されるファイリングシステム	個人データのカテゴリー	データ主体	データの保持	
質問	1	2	3	4	5.1	5.2
	なぜ、インドに関連した個人データが処理されているのか説明してください（データ処理の目的） 各目的を、はっきりと特定し、詳細に規定するとともに、個別に説明してください。例えば、従業員データも、異なる目的のために処理されているかと思います（例：給与の処理のため、建物への入退室管理のため、業績評価のため、費用清算のため).	当該インド内の個人データが処理される登録システム/サポート/プログラム/データベース/フォーマット/媒体について説明してください。（例：紙ファイル、Eメール、エクセル、CRMシステム、SAPシステム）	当該目的のために収集される**個人データ**の種類を挙げてください。（例：名前、住所、電話番号、職業、クレジットカード番号、顧客番号）	誰の**個人データ**が**処理**されているか説明してください。 A)個々の「**データ主体**」を挙げてください。（例：従業員、顧客/エンドユーザー、ビジネスパートナーの担当者、子供） B) 各**データ主体**の種類ごとに、データ処理の対象となる個人の概数を教えてください。	あなたのチーム／事業部において**データ処理**を行う必要のある期間を教えてください。 当該**処理**期間が、法定要件と関連するものかどうかについて、記載してください。（例：税法）	実際に当該**個人データ**が保管されている期間を教えてください。（実際に保管されてすぐに引き出せるか、アーカイブされているかを含む。）
回答例1 - 人事（給与処理）	例：インドの[会社]　毎月の従業員の給与処理	例： - エクセル（トラッキングシート） - 人事マネジメントソフト	例： - 従業員の氏名 - 住所 - ソーシャルセキュリティ番号 - 給与 - 銀行口座	例： - インドの[会社名]の従業員 - 47名	例： - 個人データは、要求があった後最大X年間は保管が必要である（適用のある税法等）	例: - 全てのデータ: 永久に.
回答例2 - 顧客のためのCRMシステム	例:　(当社の)インド拠点は、直接顧客から取得したユーザー及び顧客データを顧客管理システム（CRM）システムにおいて処理する。インド拠点の直接顧客はCRMデータベース及びサービスによって提供されるソフトウェアインターフェースを用いる（例：請求書など）	例: -　CRMシステム（顧客やユーザーによって用いられる直接顧客の顧客管理ソフトウェア）	例: - 姓名 - 住所 - 電話番号 - 電子メールアドレス - 購買履歴	例： - 当社の直接の顧客の最終顧客及びユーザー - インド拠点の直接顧客によって15,000の顧客、ユーザーが記録されている。	例： - 直接顧客向けに、CRMデータを完全かつ最新のものにするための間ずっと	例: - すべてのデータ：永続的

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-1：データマッピング（事実調査）の実施：データマッピング質問票（サンプル）2/3

	法的根拠			個人データの流入（In-flows）	データ主体への情報提供	
質問	6.1	6.2	6.3	7	7.1	7.2
	個人データの処理については、**データ主体**から事前に同意が取得されていますか？（例：同意書フォーム、オンラインのチェックボックス等） 当該同意が要求され、又は取得される際に使用されるフォーマットを提出してください。	**個人データの処理**は特別の法律に基づく義務によるものですか。（例：不正防止法、税法） 当該データの処理を義務付けている法律を特定してください。	**個人データの処理**は、その他の理由に基づくものですか。（例：事業を行うため等） 理由を説明するに当たっては、可能な限り正確に記載をしてください。	個人データをどこから入手したのか説明してください。入手経路を説明してください。（例：従業員から、直接の顧客から、ウェブサイト上で） 他の法人からインド所在者の個人データを入手している場合には、当該法人の名称と所在国を教えてください。	**個人データ**をデータ主体から直接取得している場合、当該**個人データの処理**に関する情報をデータ主体に提供していますか。（例：情報通知、パンフレット） もし回答が「はい」の場合、かかる書類のサンプルを提供してください。	**個人データ**を**データ主体**から直接取得して<u>いない</u>場合、**データ主体**が、貴社における当該**個人データの処理**について認識しているかどうかわかりますか。（例：第三者による情報通知等） もし回答が「はい」の場合、かかる書類のサンプルを提供してください。
回答例1 - 人事（給与処理）	例： - いいえ	例： - はい、雇用法に基づいている。	例： - はい（従業員に対して給与を支払うために必要）	例： - 従業員	例： ない、雇用契約において（義務履行のためのデータ処理に関する一般的なディスクレーマを記載）	例： 該当なし
回答例2 - 顧客のためのCRMシステム	例： - はい。（同意はインド拠点の直接顧客から取得された同意フォームによる）	例： - 該当事項なし	例： - おそらく（CRMシステムは顧客及びユーザーのニーズと要求を予期するために有用である）	例： - 当社のCRMシステムにデータを入力する当社の直接顧客	例： - 該当事項なし	例： - インド拠点は、直接顧客やユーザーが、自身のデータについて当社のインド拠点のCRMシステムの中で処理され、インド域外に移転されていることについて知らされているか把握していない

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-1：データマッピング（事実調査）の実施：データマッピング質問票（サンプル）3/3

	データ受託者／データ処理者としての役割			可能性のある受領者のカテゴリ	
質問	8.1	8.2	8.3	9.1	9.2
	貴社でのデータの処理は貴社がデータ処理者として、他社に対するデータ処理サービスの一環で行っていますか。（例：他社、すなわちデータ受託者のためにデータ処理を行っている。）	貴社がデータ処理者として行動している場合には、貴社がデータ処理を提供している会社を教えてください。（データ受託者名、貴社が提供しているサービスの内容、及び当事者間の合意書ないしサンプルを提供してください。）	貴社がデータ受託者として行動している場合、プライバシーポリシー、内部データ保護規程その他の書類／ガイダンス等を作っているか教えてください。 そのような書類のサンプルを提出してください。	**個人データ**が、他の法人に対して移転され、又は他の法人からアクセス可能な状況にあるか、教えてください。（例：他のグループ会社、ベンダー、サービス業者、顧客） もし回答が「はい」の場合、以下の二つを教えてください。 i)グループ会社（例：HQ、子会社、関連会社） ii)第三者（例：ベンダー、パートナー、サービス業者）	各法人について、当該**個人データの移転**に適用されるデータ処理に関する合意書、条項、又はポリシー等があるか教えてください。 もしそのような合意書、条項又はポリシーがあれば、そのサンプル／写しを提供してください。
回答例1 - 人事（給与処理）	例： - データ処理者として行動していません；インドの[会社名]はデータ受託者として行動しています。	例： 該当なし（[会社名]はデータ受託者として行動しています。）	例： - いいえ	例: - はい: 1. X社 (データを保存し処理しているサーバーを所有している。) 2. Y社 (サイバーセキュリティに関するアドバイザーであり、データのサンプルに時々アクセスする) 3. Z社 (給与支払サービス業者)	例: 1. X社：はい、サーバー業務を提供している会社とのサービス提供合意書。 2. Y社 ：いいえ 3. Z社 ：はい
回答例2 - 顧客のためのCRMシステム	例： - はい。データ処理者として関与。	例: - 当社は、CRMサービスが提供される会社に対し、直接の顧客の個人データについて、データ処理者として処理を行っている。 インド拠点の顧客との間の添付のサプライ及びサービス契約参照	例： - 該当事項なし	例： - はい。 1. インド本社（評価及び販売分析目的のために必要に応じて） 2. X社（データが保管され、処理されるサーバーを保有している） 3. Y社（一定のデータサンプルに対して時々アクセスを行うサイバーセキュリティーについてのアドバイザー及びサービス提供会社） 4. インド拠点の個々の顧客（インド拠点から提供されているCRMシステム上の自身の顧客及びユーザーに関するデータへのアクセス）	例： - はい。 1. インド本社-いいえ。 2. X社-はい。サーバーサービスを提供する会社とのサービス契約の中で 3. Y社-いいえ。 4. インド拠点の個々の顧客：はい。インド拠点の個々の顧客との供給およびサービス契約の中で

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：データマッピングの結果得られた事実に基づく法的評価

1. 自社のDPDPA上の位置づけの整理及び対応事項の検討

(1) 役割の整理

■ データマッピングの結果を踏まえ、自社が以下のいずれに該当するか（又は複数の立場を併せ持つか）を整理する。

- ① データ受託者
- ② 重要なデータ受託者
- ③ データ処理者

■ 自社がデータ処理者に該当する場合、DPDPA上、データ処理者に対して直接の義務は課されないものの、データ受託者がデータ処理者を関与させるためには有効な契約が必要とされる点に留意する（8条（2））。したがって、実務上は、データ処理者としても、データ受託者からの契約要請（セキュリティ措置、侵害対応、保持・削除、監査等）に対応できる体制整備が必要となる。

(2) 重要なデータ受託者に指定された場合の追加的義務

■ 自社が重要なデータ受託者に指定された場合には、通常のデータ受託者の義務に加えて、追加的な義務が課せられる。主な追加的義務としては、以下が挙げられる。

- データ保護オフィサーの選任
- 独立データ監査人の選任及び監査の実施
- 定期的なデータ保護影響評価（DPIA）の実施及び定期監査

■ また、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観点から、将来的に重要なデータ受託者に指定される可能性があるかについても検討する。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：データマッピングの結果得られた事実に基づく法的評価

2. 個々の処理の法的根拠等の整理

- データマッピングで特定された各処理（処理目的・データ項目・関係者・移転・保持等）ごとに、処理の法的根拠、必要な通知・同意、社内手続（撤回対応、侵害対応等）を整理する。

- 日本企業の通常の処理に関しては、主として、以下のいずれかが処理の根拠として想定される。

  - ① データ主体の事前の同意

  - ② 特定された目的（その目的のためにデータ主体が自発的に個人データを提供し、かつ、データ主体がデータ受領者に対して利用に同意しない旨を表明していないもの）

  - ③ 雇用の目的又は雇用者を損失・責任から保護することに関する目的（例：企業スパイの防止、営業秘密等の秘密性の維持、従業員たるデータ主体が求めるサービス・利益の提供）

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：データマッピングの結果得られた事実に基づく法的評価

- データマッピングを実施した後、その結果として得られた事実に基づき、デジタル個人データの処理との関係で、DPDPAの適用に係る法的評価を行う。実務上は、外部の専門家がデータマッピング結果に基づくアセスメントレポートを作成する形で行われることが多い。

- 次に、自社のDPDPA上の位置づけを整理し、それに基づく対応事項を検討する。具体的には、(1) データ受託者、(2) 重要データ受託者、(3) データ処理者としての役割を整理する。自社がデータ処理者に該当する場合、DPDPA上の直接義務は課されないが、データ処理についてデータ受託者との間で有効な契約が必要とされる点に留意する（8条(2)）。

- また、自社が重要データ受託者に指定された場合、データ受託者としての義務に加えて、少なくとも以下の追加義務が課される。このため、処理する個人データの量および機微性、データ主体の権利に対するリスク等の観点から、重要データ受託者に指定される可能性があるかを検討する必要がある。
  - データ保護オフィサーの選任
  - 独立データ監査人の選任および監査の実施
  - 定期的なデータ保護影響評価および定期監査

- さらに、個々の事実に基づき、処理の法的根拠（DPDPA上の「同意」または「正当な理由」）等を整理する。日本企業における通常の処理については、主として次の類型が根拠として想定される。
  - (1) データ主体の同意（Noticeに基づく明示の同意）
  - (2) 正当な理由（Certain legitimate uses）—データ主体の自発的提供に基づく処理データ主体が、特定された目的のために自発的に個人データを提供し、かつ、データ受託者に対して当該利用に同意しない旨を表示していない場合には、当該特定目的の範囲で処理が正当化され得る（7条(a)）。
  - (3) 正当な理由（Certain legitimate uses）—雇用目的等に基づく処理雇用の目的、または雇用者を損失・責任から保護する目的（例：企業スパイの防止、営業秘密・知的財産・機密情報等の秘密性の維持、従業員たるデータ主体が求めるサービスまたは利益の提供）に関連する処理は、正当な理由として位置付けられ得る（7条(i)）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（データ受託者の義務）

■ データ受託者の義務と義務違反の場合の制裁金レベルの関係性は以下の通りである。

データ受託者の義務	左記義務に違反した場合の制裁レベル
個人データの侵害を防止するために合理的なセキュリティ保護措置の実施（8条（5））	25億インドルピー（約43億円）以下
個人データの侵害が発生した場合の通知等（8条（6））	20億インドルピー（約34億円）以下
子供（18歳未満の者）の個人データを処理する場合、親・後見人の検証可能な同意取得等（9条）	20億インドルピー（約34億円）以下
通知により重要なデータ受託者に指定された場合の追加的義務の履行（10条） データ保護オフィサーの選任、独立データ監査人の選任、定期的なデータ保護影響評価の実施等	15億インドルピー（約26億円）以下
デジタル個人データの処理に係る適法性（根拠）の確保（4条（1））、すなわち、データ主体による事前の同意（要通知）、又は、法定された一定の正当な利用（certain legitimate uses）の確保	5億インドルピー（約9億円）以下
DPDPA及びDPDP規則遵守を確保するために適切な技術的・組織的措置の実施（8条（3）及び（4））	
データ処理者との間の有効な契約の確保（8条（2））	
同意が撤回された場合や個人データが不要となった場合の個人データの消去（8条（8））	
データ主体からの質問・苦情、データ主体による権利（アクセス権等）の行使に対処するための体制の整備（8条（9）及び（10）、11条、12条、13条）	
インド政府が個人データの処理のためのインド領域外への移転を制限した場合における制限遵守（16条（1））	
障がい者の個人データを処理する場合、後見人の検証可能な同意取得等（9条）	

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（データ受託者の義務）

個人データの処理に係る適法性（根拠）の確保（4条（1））
■ いかなる者も、DPDPAの規定に従い、**次のいずれかに該当する適法な目的のためにのみ**、データ主体の**個人データを処理**することができる ① **データ主体が同意**を与えたもの ➢ データ主体に同意を求めるに際しては、同時に又はあらかじめ、データ主体に対し、（同意の対象となる）個人データ、処理目的、データ主体が有する権利の行使方法、及び、DPBIへの苦情申立ての方法を**通知**する必要がある（5条（1）） ➢ データ主体は、いつでも**同意を撤回する権利**を有し、その場合、データ受託者は処理を停止する義務を負う（6条（4）及び（6）） ➢ DPDPAの適用開始前に個人データの処理につきデータ主体の同意を得ている場合は、上記の事項を通知する（5条（2）） ② 一定の**正当な利用**（詳細は7条に規定、後述） • 個人データの「処理」とは、デジタル個人データについて行われる、完全に又は部分的に自動化された、一の又は一連の操作をいい、次のような操作を含む（2条（x））：取得、記録、仕分け、構造化、保管、適合化、復旧、利用、調整・組み合わせ、索引付け、共有、送信による開示、配布その他の方法による提供、制限、消去又は廃棄

データ受託者の一般的な義務（8条）
■ データ受託者は、自己が行う処理、または自己のためにデータ処理者が行う処理について、DPDPAおよびDPDP規則を遵守する責任を負う。この責任は、これを否定する合意が存在するか否か、またはデータ主体によるDPDPA上の義務の不履行があるか否かにかかわらず、免除されない。
■ データ受託者は、有効な契約に基づく場合にのみ、データ処理者を従事させ、選定し、使用し、またはその他の形で関与させることができる（8条(2)）。特に、データ主体への商品またはサービスの提供に関連する活動のために、データ処理者がデータ受託者のために個人データを処理する場合には、当該契約に基づき適切に関与させる必要がある。
■ また、データ処理者が処理する個人データが、次のいずれかに該当する場合には、データ受託者は、当該個人データの完全性、正確性および一貫性を確保しなければならない。 ■ 当該個人データが、データ主体に影響を与える決定を行うために利用される可能性がある場合 ■ 当該個人データが、他のデータ受託者に開示される可能性がある場合

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（データ受託者の義務）（前スライドからの続き）

データ受託者の一般的な義務（8条）（続き）
■ DPDPAおよびDPDP規則の規定の実効的な遵守を確保するため、データ受託者は、適切な技術的および組織的措置を講じなければならない（8条(1)）。
■ さらに、データ受託者は、個人データの侵害を防止するための合理的な安全管理措置（合理的なセキュリティ保護措置）を講じることにより、自己が所有し、または自己の管理下にある個人データを保護しなければならない。この義務は、データ受託者が自ら行う処理に限られず、データ受託者のためにデータ処理者が行う処理も含む（8条(5)、DPDP規則6条(1)）。
■ ここで「個人データの侵害」とは、次の事象であって、個人データの秘密性、完全性または可用性を損なうものをいう（2条(u)）。 ① 個人データの不正な処理 ② 個人データの偶発的な (i) 開示、(ii) 取得、(iii) 共有、(iv) 利用、(v) 変更、(vi) 廃棄、または (vii) アクセスの喪失 ■ データ受託者が個人データの侵害を認識した場合には、 (1) データ保護委員会（DPBI）および (2) 影響を受けた各データ主体 に対して、DPDP規則で定められた内容および方法により、遅滞なく通知しなければならない（DPDP規則7条(1)、7条(2)）。 ■ さらに、データ受託者は、侵害を認識してから72時間以内（またはDPBIが書面により認めた、これより長い期間内）に、所定の追加情報をデータ保護委員会に通知しなければならない（DPDP規則7条(2)(b)）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（データ受託者の義務）（前スライドからの続き）

データ受託者の一般的な義務（8条）（続き）
■ 施行中の法律に従うために当該個人データの保管が必要な場合を除き、データ受託者は、次のいずれか早い時点で個人データを消去しなければならない（8条(7)）。 ➢ (i) データ主体が当該個人データの処理に係る同意を撤回した場合 ➢ (ii) 当該個人データが、もはや特定された目的のために供されていないとみなすことが合理的である場合 ■ この場合、データ受託者は、自己が保有する個人データを消去するとともに、処理のために当該個人データを提供したデータ処理者に対しても、当該個人データを消去させなければならない（8条(7)）。 ■ DPDP規則では、所定の期間にわたり、データ主体が特定された目的の遂行のためにデータ受託者に接触せず、かつ、当該処理に関連していかなる権利も行使しない場合には、当該個人データは、もはや特定された目的のために供されていないものとみなされる旨が規定されている。 ■ ここでいう「接触」とは、特定された目的の遂行のために、対面で、または電子的もしくは物理的な通信手段によって、データ主体の側からデータ受託者に対して開始される接触をいう。また、データ主体の側から開始されたものではない期間については、データ主体がデータ受託者に接触していないものとみなされる（8条(11)）。
■ データ受託者は、データ主体の個人データの処理に関する質問に対し、データ受託者に代わって回答することのできる者の業務連絡先を、DPDP規則で定められた方法により公表しなければならない。重要データ受託者に該当する場合には、選任されたデータ保護オフィサーの業務連絡先を公表しなければならない。
■ さらに、データ受託者は、データ主体からの苦情に対処するため、苦情の受付、調査、対応および是正措置を含む実効的なメカニズムを構築し、適切に運用しなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（追加的な義務：子供等の個人データ）

- 子供又は（適法な後見人のいる）障がい者の個人データを処理する場合、データ受託者は、処理に先立って、親又は適法な後見人から検証可能な同意を取得しなければならない（9条（1））。

- 子供の個人データに関しては、次の行為が禁止されている（9条（2）及び（3））。
  - 子供の福利に有害な影響を及ぼす可能性の高い個人データの処理（9条（2））
  - 子供のトラッキング、行動モニタリング、子供に対するターゲット広告（9条（3））

- もっとも、これらの追加的な義務については、規則又は政府の通達により、一定の適用除外又は緩和が設けられ得る（9条（4）及び（5））。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（追加的な義務：子供等の個人データ）

- データ受託者は、子供の個人データを処理する前に、親の検証可能な同意を取得するための適切な技術的及び組織的措置を講じなければならない。また、自己を親であると識別する個人が、必要に応じて、インドで施行されている法律の遵守のために、識別可能な成人（18歳に達した個人）であることを確認するため、適切な注意義務を果たさなければならない（規則10条（1））。

- 当該確認は、少なくとも次の情報を参照して行うものとする（規則10条（1））。
  - データ受託者が保有する、信頼できる身元及び年齢に関する詳細情報
  - 法律により、又は中央政府若しくは州政府から当該情報の管理を委託された機関（又は当該機関により当該情報の発行のために任命若しくは許可された者）が発行した、本人が自発的に提供する身元及び年齢に関する詳細情報、又はそれに対応付けられた仮想トークンであって、デジタルロッカーサービスプロバイダーによって確認され、提供された当該情報又はトークンを含むもの

- また、データ受託者は、障がい者の法的保護者であると自己を識別する個人から検証可能な同意を取得する場合には、当該保護者が、保護者制度に適用される法律に基づき、裁判所、指定機関又は地方レベルの委員会によって任命されていることを確認するため、適切な注意義務を果たさなければならない（規則10条（2））。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（追加的な義務：重要なデータ受託者）

■ 重要なデータ受託者の追加的な義務として、以下のものが挙げられる（10条）。

重要なデータ受託者の義務（10条）
■ 重要データ受託者は、次のすべての要件を満たすデータ保護オフィサーを選任しなければならない。 ➢ DPDPAの規定に基づき、重要データ受託者を代表する者であること ➢ インドを拠点とする者であること ➢ 重要データ受託者の取締役会またはこれに相当する管理機関に対して責任を負う個人であること ➢ DPDPAの規定に基づく苦情対応メカニズムの窓口となること
■ また、重要データ受託者は、独立データ監査人を選任しなければならない。独立データ監査人は、データ監査を実施し、重要データ受託者によるDPDPAの遵守状況を評価する。
■ さらに、重要データ受託者は、少なくとも次の措置を講じなければならない。 ➢ 定期的なデータ保護影響評価 ◆ 次の事項から構成されるプロセスでなければならない。 ✓ ① データ主体の権利および当該個人データの処理目的の説明 ✓ ② データ主体の権利に対するリスクの評価および管理 ✓ ③ その他、当該プロセスに関してDPDP規則に定められた事項 ➢ 定期的な監査 ➢ その他、DPDPAの規定に合致する措置であって、DPDP規則に定めるもの

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（追加的な義務：重要なデータ受託者）

■ DPDP規則で定められた、重要なデータ受託者の追加的な義務として、以下のものが挙げられる（規則12条）。

DPDP規則で定められた重要なデータ受託者の義務（規則12条）
■ （1）重要なデータ受託者は、当該重要なデータ受託者として通知された日又は当該分類に含まれることが通知された日から起算して12か月ごとに、データ保護影響評価及び監査を実施し、本法及び本法の下で制定された規則の効果的な遵守を確保しなければならない。 ■ （2）重要なデータ受託者は、データ保護影響評価及び監査を実施する者に対し、当該データ保護影響評価及び監査における重要な所見を含む報告書を作成させ、DPBIに提出させなければならない。 ■ （3）重要なデータ受託者は、自己がホスティング、表示、アップロード、修正、公開、送信、保存、更新又は共有のために使用するアルゴリズム・ソフトウェアについて、データ主体の権利にリスクを及ぼすおそれが低いこと（すなわち、リスクを生じさせる可能性が高くないこと）を確保するため、適切な注意義務を果たさなければならない。 ■ （4）重要なデータ受託者は、中央政府が設置した委員会の勧告に基づいて指定した個人データについて、当該個人データ及びその流れに関するトラフィックデータがインド領域外に移転されないという制限の下で処理されることを確保するため、必要な措置を講じなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（処理の法的根拠（処理目的））

■ いかなる者も、DPDPAの規定に従い、次のいずれかに該当する適法な目的のためにのみ、データ主体の個人データを処理することができる（4条（1））
① データ主体が同意を与えたもの
② 以下の、一定の正当な利用（certain legitimate uses）（7条）

一定の正当な利用（処理目的）（7条）
■ 次の要件を満たす**特定された目的**のため ① その目的のために**データ主体が自発的に個人データを提供**し、かつ、 ② データ主体がデータ受領者に対して**利用に同意しない旨表明していない**もの ➢ 「特定された目的」とは、DPDPA及び規則に従って**データ受託者がデータ主体に提示した通知に記載された目的**をいう（2条（za）） ◆ 個人Xが薬局Yで商品を購入するに際し、自発的にYに個人データを提供し、YがXの携帯電話にメッセージを送信して購入代金の受領を確認するよう求めた場合、Yは領収書を送信する目的でXの個人データを処理することができる。 ◆ 個人Xは、不動産仲介業者Yに電子メッセージを送信して、自己に適した賃貸住宅探しの手伝いを求め、その目的のために自己の個人データを提供した。この場合、Yは、賃借可能な物件の詳細を特定しXに通知するためにXの個人データを処理することができる。その後、XがYの支援はもはや必要ない旨連絡したときには、YはXの個人データの処理を中止しなければならない。
■ 一定の条件を満たす場合において、公的機関等がデータ主体に対して、所定の補助金、給付金、サービス、証明書、ライセンス、又は許可証を提供、又は発行するため
■ インドで施行中の法律に基づき、又は、インドの主権・統一性、国家安全保障のために、公的機関等がその機能を果たすため

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-2：事実に基づく法的評価
背景情報（処理の法的根拠（処理目的））（前スライドからの続き）

一定の正当な利用（処理目的）（7条）（続き）
■ インドで施行中の法律に基づき、公的機関等に対して情報を開示する義務負う者が当該義務を履行するため（施行中の他の法律の当該情報の開示に関する規定に従って、当該処理を実施することを条件とする）
■ インドで施行中の法律に基づき下された判決・命令、又は、インド国外で施行中の法律に基づき下された契約上の請求若しくは民事上の請求に関する判決・命令に従うため
■ データ主体又は他の個人の生命に対する脅威又は健康に対する差し迫った脅威を伴う医療緊急事態に対応するため
■ 疫病の流行、疫病の発生、又はその他公衆衛生に対する脅威がある場合に、医療又は保険サービスを個人に提供するための措置を講じるため
■ 災害時又は治安崩壊時に、個人の安全を確保し、援助又はサービスを提供するための措置を講じるため
■ (i)**雇用**の目的、又は、(ii)雇用者を損失・責任から保護すること（例：企業スパイの防止、営業秘密等の秘密性の維持、**従業員たるデータ主体の求めるサービス・利益の提供**）に関する目的のため

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成

■ データ主体又はデータ処理者との間の対外関係におけるDPDPA遵守の観点から、データマッピング及び法的評価の結果に基づき、対外的に提示することとなる以下の文書を作成し、又は見直す必要がある。

① プライバシーポリシー（通知）

- 個人データの処理について同意を取得する前提として、データ主体に対する情報開示を行う必要がある。
- DPDPAの適用開始前に、既にデータ主体から個人データの処理について同意を取得している場合であっても、DPDPA及びDPDP規則に基づく通知を行う必要がある。
- 通知の方法及び内容については、DPDP規則において詳細に規定されており、特に、
  - 他の情報から独立して提示されること
  - 平易かつ理解可能な言語で記載されること
  - 個人データの項目別説明、処理目的、提供される又は可能となる商品・サービスの内容が含まれること
  - 同意撤回、権利行使及びDPBIへの苦情申立ての方法が示されること

  が求められる。
- また、一定の正当な利用の一つである「特定された目的」を援用する場合であっても、通知において当該処理目的を明確に記載しておくことが不可欠である。

② 同意書

- データ主体の同意を個人データ処理の法的根拠として処理を行う場合には、DPDPA及びDPDP規則に適合した同意取得の仕組み及び同意文言を整備する必要がある。
- 同意は、自由、具体的、十分な情報に基づき、無条件かつ明確な積極的行為によって与えられるものでなければならず、同意撤回は付与時と同等の容易さで可能であることが求められる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成

■ データ主体又はデータ処理者との間の対外関係におけるDPDPA遵守の観点から、データマッピング及び法的評価の結果に基づき、対外的に提示することとなる以下の文書を作成し、又は見直す必要がある。

③ データ処理者との間の処理契約
- データ受託者がデータ処理者を使用する場合には、DPDP規則において定められた合理的なセキュリティ保護措置等を反映した、有効な処理契約を締結する必要がある。
- 当該契約には、個人データの安全管理、侵害対応、保持・削除等に関する事項を盛り込むことが求められる。

④ 個人データ侵害発生時の通知文書（データ主体向け）
- 個人データの侵害が発生した場合、DPDPAは、データ受託者に対し、影響を受ける各データ主体に対する通知を義務付けている。
- 当該通知には、侵害の内容、想定される影響、講じた又は講じる予定の緩和措置、及びデータ主体が自己の利益を保護するために取り得る措置等を含める必要がある。
- DPBIへの通知については、DPDP規則により、その形式及び方法が具体的に定められており、所定の電子的手段（ポータル）を通じて行うことが想定されている。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（プライバシーポリシー（通知））

- 個人データを処理するためにデータ主体に同意を求めるに際しては、データ受託者は、同意の取得と同時に又はこれに先立って、データ主体に対し、以下の事項を通知しなければならない（DPDPA 5条（1））。

  - （同意の対象となる）取得され、又は取得される予定の個人データの項目及びその処理目的
  - データ主体がDPDPAに基づき有する権利を行使する方法
  - データ主体がインドデータ保護委員会（DPBI）に対して苦情を申し立てる方法

- この通知は、他の情報とは独立して提示され、平易かつ理解可能な言語で記載される必要があり、また、データ主体が自己の個人データの処理について説明を受けた上で同意できるよう、個人データの項目別説明、処理目的、及び当該処理によって提供され、又は可能となる商品又はサービスの内容を含めなければならない（DPDP規則3条）

  - 【例】個人Xが、銀行Yのモバイルアプリ又はウェブサイトを利用して銀行口座を開設するに際し、Xは、銀行口座開設に関する法律に基づく顧客確認（Know-Your-Customer）の要件を満たすため、Yによるライブ映像ベースの顧客確認プロセスにおける個人データの処理を選択した場合、Yは、個人データの提供を求めると同時に、又はこれに先立って、取得し処理する個人データの項目及びその処理目的をXに通知しなければならない

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（プライバシーポリシー（通知））

- また、DPDPAの適用開始前に、既にデータ主体から個人データの処理について同意を得ている場合であっても、データ受託者は、合理的に実行可能な限り早期に、上記と同一の事項をデータ主体に知らせる通知を行わなければならない（DPDPA 5条（2）（a））。

- この場合、データ受託者は、データ主体が当該同意を撤回しない限り、個人データの処理を継続することができる（DPDPA 5条（2）（b））。

  - 【例】個人Xが、DPDPAの適用開始前に、電子商取引サービス事業者Yが運営するオンラインショッピングアプリ又はウェブサイトにおける個人データの処理について同意していた場合、Yは、実行可能な限り早期に、電子メール、アプリ内通知その他の有効な方法により、処理されている個人データの項目及びその処理目的を記載した情報をXに提供しなければならない。

- さらに、データ受託者は、データ主体に対し、上記の通知事項の内容を、英語又は憲法別表第8に定める言語（アッサム語、ベンガル語、グジャラート語、ヒンディー語等の22言語）で閲覧する選択肢を与えなければならない。

- 加えて、DPDP規則により、当該通知には、同意の撤回、DPDPAに基づく権利の行使及びDPBIへの苦情申立てを行うためのリンク又はその他の手段を含めることが求められている（DPDP規則3条）。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（プライバシーポリシー（通知））（前スライドからの続き）

- 一定の正当な利用の一つである特定された目的（その目的のためにデータ主体が自発的に個人データをデータ受託者に提供し、かつ、データ主体が当該データ受託者に対して当該個人データの利用に同意しない旨を表明していないもの）（7条（a））により個人データの処理を行う場合であっても、「特定された目的」は、定義上、データ受託者がデータ主体に対して行う通知に記載された目的（2条（za））であることから、当該通知が行われていることが前提となる

- DPDP規則により、データ受託者がデータ主体に対して行う通知は、次の要件を満たさなければならない（規則3条）
  - (a) 当該データ受託者が提供した、提供している、又は提供する可能性のある他のいかなる情報とも独立して提示され、理解可能であること。
  - (b) 明確かつ平易な言語で、データ主体が自身の個人データの処理について、具体的かつ十分な情報に基づいた同意を与えられるように必要な詳細を公正に説明すること。この通知には、少なくとも以下の事項を含めなければならない。
    - (i) 当該個人データの項目別の説明
    - (ii) 当該処理の特定された目的及び、当該処理によって提供される商品若しくはサービス又は可能となる利用の項目別の説明
  - (c) 当該データ受託者のウェブサイト又はアプリ（又はその両方）への特定の通信リンク、並びに、データ主体が以下を行うために使用できるその他の手段（該当する場合）の説明を含むこと。
    - (i) 当該同意の撤回（その撤回の容易さは、同意が与えられた際の容易さと同等であること）
    - (ii) 本法に基づく自身の権利の行使
    - (iii) DPBIへの苦情の申立て

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：プライバシーポリシー（実例）

- DPDPAに対応したプライバシーポリシーの作成に必要となる情報は、データマッピング質問票を通じて体系的に収集・分析することが可能である。当該データマッピング及び法的評価を行えば、DPDPAの専門家の側で、DPDPA及びDPDP規則に適合したプライバシーポリシーのドラフトを作成することができる。

- 依頼者である企業は、
  - 専門家が作成したプライバシーポリシーのドラフトについて、自社の実際の事業内容・業務運用との整合性の観点から確認を行い、
  - 内容を確定した上で公開し、
  - その後は、法令改正、事業内容の変更又は個人データの取扱いの変更等に応じて、定期的な見直し（メンテナンス）を行う

  という役割を担うことになる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：プライバシーポリシー（実例）

- DPDPA対応プライバシーポリシーの構成例として、TATA Motors Limitedが公表しているプライバシーポリシーが参考となる。（https://fleetverse.tatamotors.com/privacy-policy）

- 当該プライバシーポリシーは、概ね以下の項目から構成されている。
  - Objective / Purpose / Scope（目的・適用範囲）
  - Privacy Policy（総則）
  - Personal data that we collect（取得する個人データ）
  - How we use your personal data（個人データの利用目的）
  - When we share personal data（個人データの第三者提供）
  - Where we store and process personal data（保存・処理場所）
  - How we secure personal data（安全管理措置）
  - Cookies
    - Strictly necessary cookies
  - Children（子どもの個人データ）
  - Your rights and your personal data（データ主体の権利）
  - How long do we keep your personal data（保持期間）
  - Changes（変更）
  - Limitations（制限事項）
  - Your Specific Obligations（データ主体の義務）
  - Governing law / Jurisdiction（準拠法・管轄）
  - Question / Contact Information（問い合わせ先）

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（同意及び同意書）

- 同意は、次の要件を満たすものでなければならない（DPDPA 6条（1））。
  - 十分な情報を与えられた上で、自由になされた、具体的で、無条件かつ曖昧でないものであり、明確な肯定的行為によって与えられること
  - 特定された目的のために、自己の個人データを処理することに合意する意思を表明するものであること
  - 当該個人データについて、当該特定された目的のために必要な処理に限定されること

【例】
個人Xが遠隔医療アプリYをダウンロードするに際し、YがXに対し、(i) 遠隔医療サービスを提供するための個人データの処理、及び(ii) 携帯電話の連絡先リストへのアクセスについて同意を求め、Xがその両方について同意を表明した場合であっても、携帯電話の連絡先リストは遠隔医療サービスを提供するために必要ではないことから、Xの同意は、遠隔医療サービスを提供するための個人データの処理に限定されることとなる。

- また、同意のうち、DPDPA若しくはDPDP規則、又はインドで施行中の他の法律の規定に違反する部分は、その違反の範囲において無効となる（DPDPA 6条（2））。

【例】個人Xが、保険会社Yのモバイルアプリ又はウェブサイトを利用して保険契約を購入するに際し、(i) 保険証券の発行のためにYがXの個人データを処理すること、及び(ii) DPBIに対して苦情を申し立てる権利を放棄することについてYに同意を与えた場合、(ii) に係る同意部分は、DPDPAに反するため無効となる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（同意及び同意書）

- さらに、DPDPA及びDPDP規則に基づく同意の要請は、すべて、次の要件を満たす方法で行われなければならない（DPDPA 6条（3））。
  - 明確かつ平易な言語で提示されること
  - 英語又は憲法別表第8に定める言語により、当該同意要請の内容にアクセスする選択肢をデータ主体に与えること
  - データ主体がDPDPAに基づく権利を行使するために行う連絡に対応する権限を、データ受託者から付与された者の連絡先を提供すること
  - （重要なデータ受託者の場合には、データ保護オフィサーの連絡先を含む）

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（同意及び同意書）（前スライドからの続き）

- 個人データの処理がデータ主体の同意を根拠として行われている場合、データ主体は、いつでも同意を撤回する権利を有する（DPDPA 6条（4））。同意の撤回は、同意の付与と同程度に容易でなければならない。

- また、DPDP規則により、データ受託者がデータ主体に対して行う通知には、データ主体が同意撤回を行うために使用できるウェブサイト又はアプリへの特定の通信リンクその他の手段が示されなければならず、撤回の容易性は同意付与時と同等であることが求められる（DPDP規則3条(c)(i)）。

- データ主体が同意を撤回した場合、データ主体は同意撤回の結果を受け入れなければならないが、撤回前の当該同意に基づく個人データの処理の適法性には影響を与えない（DPDPA 6条（5））。

  【例】個人Xは、電子商取引サービス事業者Yが運営するオンラインショッピングアプリ又はウェブサイトのユーザーであり、自己の注文を実行する目的でYが個人データを処理することに同意し、商品を注文するとともに代金を支払った。この場合において、Xが同意を撤回したとき、Yは、Xがアプリ又はウェブサイトを利用して新たに発注することを停止することはできるが、既にXが発注し代金を支払った商品を供給するための処理を停止することはできない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（同意及び同意書）（前スライドからの続き）

- さらに、データ主体が個人データの処理に係る同意を撤回した場合、データ受託者は、合理的な期間内に、当該データ主体に係る個人データの処理を中止し、かつ、データ処理者にも当該個人データの処理を中止させなければならない（DPDPA 6条（6））。ただし、DPDPA及びDPDP規則又はインドにおいて施行中の法律に基づき、データ主体の同意がなくとも当該処理を行うことが要請され、又は認められている場合はこの限りでない。

  【例】電気通信サービスプロバイダーXは、データ処理者Yとの間で、Xの顧客に電話料金の請求書を電子メールで送信するための契約を締結している。Xの顧客Zは、従前、請求書を電子メールで送付するための個人データの処理について同意を与えていたが、Xのモバイルアプリをダウンロードし、当該アプリ上でのみ請求書を受け取ることを選択した。この場合、Xは、電子メールで請求書を送付するためにZの個人データを処理することにつき、自らこれを中止するとともに、Yにもこれを中止させなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（同意及び同意書）（前スライドからの続き）

- データ主体は、同意管理者を通じて、データ受託者に対する同意の付与、管理、見直し又は撤回を行うことができる（DPDPA 6条（7））。同意管理者は、DPBIに登録された者であり、データ主体がアクセス可能で透明性があり相互運用可能なプラットフォームを通じて、同意に関する行為を行えるようにする単一の窓口として機能する。

- また、データ主体による同意が個人データ処理の根拠とされている場合において、手続においてこの点に関する疑義が生じたときは、データ受託者は、次の事項を証明する義務を負う（DPDPA 6条（10））。

  - データ受託者からデータ主体に対し、DPDPA及びDPDP規則に従った通知が行われたこと

  - 当該データ主体によって、DPDPA及びDPDP規則に従い、データ受託者に対して同意が与えられたこと

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：同意書（サンプルイメージ）（前スライドからの続き）

DPDPA Privacy Notice and Consent Form

- Company Y (the “Company”, “we”, “us”, or “our”) collects and processes personal data as a Data Fiduciary in accordance with the Digital Personal Data Protection Act, 2023 of India (“DPDPA”) and the Digital Personal Data Protection Rules, 2025 (“DPDP Rules”).

- This Privacy Notice and Consent Form (the “Form”) is provided independently of any other information and in clear and plain language to enable you to make an informed decision regarding the processing of your personal data.

1. Purpose of this Form
In connection with the provision of telemedicine services to you, and to ensure compliance with the DPDPA and the DPDP Rules, we seek your prior, informed, and explicit consent for certain personal data processing activities described in this Form.

2. Voluntary Nature of Consent
Your consent to each of the processing activities described in this Form is entirely voluntary.
If you choose not to consent to any or all of the processing activities, no adverse or detrimental effect will result. However, in such case, we may be unable to process your personal data for the specific purposes or in the manner for which consent is sought.

3. Description of Processing Activities
Details of the personal data processed, the itemized categories of personal data, the specified purposes of processing, and the services enabled by such processing are set out in the table below.
Please review each processing activity carefully and indicate your consent by selecting the corresponding option.

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：同意書（サンプルイメージ）（前スライドからの続き）

DPDPA Privacy Notice and Consent Form (Continued)

4. Data Principal's Rights

As a Data Principal under the DPDPA, you have, among others, the right to:

- withdraw your consent at any time, with the ease of withdrawal being comparable to the ease with which consent was given;
- exercise your rights under the DPDPA; and
- lodge a complaint with the Data Protection Board of India ("DPBI").

You may exercise these rights or withdraw your consent by using the following means:

- [Insert specific website or app link for consent withdrawal and rights requests]or by contacting us at
- [insert contact details / Data Protection Officer details, if applicable].

5. Withdrawal of Consent

Withdrawal of consent shall not affect the lawfulness of processing carried out prior to such withdrawal. Upon withdrawal, we will cease processing your personal data within a reasonable time, unless continued processing is required or permitted under applicable law.

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：同意書（サンプルイメージ）（前スライドからの続き）

DPDPA Privacy Notice and Consent Form (Continued)

Consent Declaration

I, X, confirm that I have read and understood the contents of this Privacy Notice and Consent Form.

I hereby freely, specifically, and unambiguously consent, by a clear affirmative action, to the processing of my personal data for the specified purposes indicated below, by checking the relevant boxes.

Processing Activity	I Agree	I Do Not Agree
[Processing Activity 1]	☐	☐
[Processing Activity 2]	☐	☐
[Processing Activity 3]	☐	☐

By clicking the “I Agree” button below, I indicate my consent as described above.

☐ I Agree ☐ I Do Not Agree

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（処理契約）

- DPDPAは、データ処理者の使用に関連して、データ受託者に対し複数の義務を課している。したがって、データ受託者は、データ処理者との間で、これらの義務に対応する条項（実施内容に加え、履行の確認方法・監査可能性を含む）を盛り込んだ処理契約を締結することが必要となる。
  - データ受託者は、自己が行う処理のみならず、自己のためにデータ処理者が行う処理についても、DPDPA及びDPDP規則を遵守する責任を負う（8条（1））。
  - 個人データの侵害が生じた場合には、当該侵害がデータ処理者の環境下で発生したものであっても、データ受託者に対し、DPBI及び影響を受けたデータ主体への通知義務が生じ得る。また、DPDP規則により、通知の内容・方法（初期通知及び72時間以内の詳細報告を含む）が具体化されているため、処理契約において、データ処理者からデータ受託者への即時報告義務、情報提供項目、協力義務等を明確化しておく必要がある。
  - データ受託者は、有効な契約に基づいてのみ、（データ主体への商品又はサービスの提供に関連する活動のため、データ受託者のために個人データを処理する者として）データ処理者を従事させ、選定し、使用し、又はその他の形で関与させることができる（8条（2））。
  - データ受託者は、自己が行う処理又は自己のためにデータ処理者が行う処理の双方を含め、個人データの侵害を防止するために合理的なセキュリティ保護措置を講じることにより、自己が所有し、又は自己の管理下にある個人データを保護しなければならない（8条（5））。さらに、DPDP規則により、合理的なセキュリティ保護措置の最低基準（暗号化、アクセス制御、ログ記録・監視、バックアップ、ログ及び個人データの一定期間保持、契約条項の整備等）が具体化されているため、処理契約においても、当該最低基準に沿った技術的・組織的措置、監査・証跡、下請管理等を明確に規定する必要がある。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成
背景情報（処理契約）

- DPDPAは、データ処理者の使用に関連して、データ受託者に対し複数の義務を課している。したがって、データ受託者は、データ処理者との間で、これらの義務に対応する条項（実施内容に加え、履行の確認方法・監査可能性を含む）を盛り込んだ処理契約を締結することが必要となる。
  - （施行中の法律に従うために保管が必要な場合を除き）データ受託者は、次のいずれか早い時点で、自ら個人データを消去するとともに、データ処理者にも、データ受託者が処理のために提供した個人データを消去させなければならない（8条（7））。
    - (i) データ主体が同意を撤回した場合
    - (ii) もはや特定された目的のために供されていないとみなすことが合理的である場合

    ただし、DPDP規則により、（目的達成後又は同意撤回後であっても）一定の個人データ・トラフィックデータ・処理ログを少なくとも1年間保持すべきことが求められる場面があるため、処理契約上も、削除義務と保持義務の整合（削除例外、保留（legal hold）、ログ保持、削除証明等）を明確にしておく必要がある。
  - データ主体が個人データの処理に係る同意を撤回した場合、データ受託者は、合理的な期間内に、当該データ主体に係る個人データの処理を中止するとともに、データ処理者にも当該個人データの処理を中止させなければならない（6条（6））。したがって、処理契約には、同意撤回の通知フロー、処理停止の手順、停止完了の確認方法を組み込む必要がある。
  - 中央政府は、通達により、データ受託者による個人データの処理のためのインド領域外への移転を制限することができる（16条（1））。したがって、処理契約においては、越境移転が想定される場合、移転先、再移転、政府命令への対応（移転停止、データ返還・国内保管への切替等）を規定しておくことが望ましい。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：処理契約（サンプルイメージ）

- DPDPA上の処理契約に関する要件は、少なくとも現時点においては、GDPRにおける処理契約（Article 28）に求められる要件の水準を超えるものとは整理されていない。このため、GDPR対応のために使用してきた欧州委員会の決定に基づく処理契約のひな型を基礎として用いること自体は、DPDPAとの関係でも、原則として大きな問題を生じさせないと考えられる。

- もっとも、インドの監督当局が、GDPRにおける欧州委員会決定のように、処理契約の公式なひな型又は標準条項を公表するかどうかは現時点では明らかでない。そのため、実務上は、欧州委員会が決定したGDPR対応の処理契約をベースとしつつ、DPDPA及びDPDP規則の規定（特に、侵害通知、保持・削除、越境移転、合理的セキュリティ措置等）を踏まえて必要な修正を加えた上で処理契約を作成・使用するという進め方が、合理的であると考えられる。

- DPDP規則に準拠した処理契約とは、要するに、データ受託者が、データ処理者に対し、DPDPA及びDPDP規則を遵守する形で個人データを処理することを確保するための義務を契約上負わせるものである。

- DPDP規則に準拠した処理契約を締結するにあたり、データ受託者及びデータ処理者の双方において、具体的な内容を記入することが想定される主な項目は、以下のとおりである。

- 処理契約の作成及び締結に備え、データマッピング質問票を活用して、利用しているデータ処理者を網羅的に把握するとともに、それぞれの処理者が講じている技術的・組織的措置の内容を確認し、処理契約に具体的に記載できるよう準備を行うことが重要である。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-1-3：コンプライアンス文書の作成：処理契約（サンプルイメージ）

ANNEX I

- 当事者のリスト
  - データ受託者
    - 名称
    - 所在地
    - コンタクトパーソンの氏名、肩書及び連絡先
    - 署名及び日付
  - データ処理者
    - 名称
    - 所在地
    - コンタクトパーソンの氏名、肩書及び連絡先
    - 署名及び日付

ANNEX II

- 処理の内容
  - 個人データが処理されるデータ主体の種類
  - 処理される個人データの種類
  - 処理されるセンシティブ個人データの種類
  - 処理の主題及び性質
  - データ受託者に代わって個人データが処理される目的
  - 処理の期間
  - 処理者による処理の内容、主題、性質及び期間

ANNEX III

- 技術的・組織的措置
  - 個人データのセキュリティを確保するための技術的・組織的措置（DPDP規則に基づく合理的セキュリティ保護措置を含む）

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
概要

- データマッピングによりデータフローを把握し、当該事実調査の結果に基づいて対外的なコンプライアンス対応（プライバシーポリシー、通知、同意文書、処理契約等）を実施するプロセスと並行して、社内体制及び関連する社内規程（マニュアル等を含む）の整備、見直し又は更新といった内部的なコンプライアンス対応を行うことも不可欠である。

- 社内規程の具体的な内容については、DPDPA及び既に告示されたDPDP規則を参照した上で検討する必要があり、これらの法令の規定から想定される主要な対応事項としては、少なくとも以下のものが挙げられる。
  - 個人データのセキュリティに関する手続及び実務に係る社内規程の作成又は見直し（DPDP規則に基づく合理的なセキュリティ保護措置、アクセス管理、ログ管理等を含む）
  - データ主体からの請求、並びに同意の撤回又は同意しない旨の表明に対応するための社内体制及び社内規程の整備
  - データ主体対応のための窓口の設置、並びに社内における連絡・対応体制の整備
  - データ主体の権利行使への対応に関するマニュアルの作成（任意であり、必ずしも必須ではないが、実務上は有用である）
  - 本人確認手続に関する社内ルールの整備（同意管理者、親、法的後見人又は指名された者を通じて請求が行われる場合に、当該者が権限を有する者であることの確認を含む）
  - 同意の撤回又は同意しない旨の表明に関する対応手続の整備（受付窓口、社内連絡フロー、処理停止手続、及びデータ処理者を使用している場合の当該データ処理者への連絡・対応手続を含む）
  - 個人データ侵害発生時の対応マニュアルの作成（内部における報告手続、DPBIへの通知、影響を受けるデータ主体への通知に関する手続を含む）
  - 苦情及び紛争対応体制並びに対応手続の整備（質問に対応できる者の選任、その業務上の連絡先の公表を含む）
  - データ主体がDPBIに苦情を申し立てた場合を想定した社内対応体制の検討
  - DPDPA及びDPDP規則に関する必要な研修プログラムの企画及び実施

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備：データ保護マネジメントシステム規程（サンプル）

Guidance on the Data Protection Management System of Company X for the India's DPDPA Compliance

I. INTRODUCTION

Company X and certain of its subsidiaries (the "**Company X's Indian Entities**") need to comply with the India's DPDPA and DPDP Rules in processing/transferring personal data of those who are in India. In order to ensure compliance with the India's DPDPA, the Company X has set up a Data Protection Management System ("**DPMS**"), the internal structure of which is described in this Document.

II. PURPOSE OF THE DOCUMENT

This Document applies to certain persons working at Company X and to all persons working at the premises of the Company X's Indian Entities, including employees (e.g., full-time, part-time, contract, temporary, fixed-term and all other employees), officers (e.g., directors, executive officers and managers) and other staff (e.g., contractors and agents) (collectively, for the purposes of this Document, "**Employees**").

The purpose of this Document is to provide Employees with guidance on how to comply with the India's DPDPA in processing personal data of those who are in India and in transferring personal data from the Company X's Indian entities to non-Indian entities.

In particular, this Document provides guidance on:

- The place of Employees within the internal structure of the DPMS.

For further information, see Chapter III.

- The role of Employees regarding the three types of internal procedures of the DPMS concerning Employees:

1) Procedures to identify, and start new processing activities/transfers, and modify existing processing activities/transfers;
2) Procedures to handle Data Principal requests; and
3) Procedures to handle Personal Data Breaches.

For further information, see the corresponding section of Chapter IV.

III. THE INTERNAL STRUCTURE OF THE DPMS

IV. THE INTERNAL PROCEDURES OF THE DPMS

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
個人データのセキュリティ手続き・実務に係る社内規程の作成・見直し

■ DPDP規則によって定められた合理的なセキュリティ保護措置の詳細は以下の通りである（規則6条（1））。

合理的なセキュリティ保護措置（規則6条（1）） データ受託者は、自己が保有し、または自己の管理下にある個人データについて、自己が行う処理、または自己のためにデータ処理者が行う処理に関して、個人データ侵害を防止するために合理的なセキュリティ保護措置を講じなければならない。これらの措置には、少なくとも次に掲げる事項が含まれる。
(1) 当該個人データの暗号化、難読化またはマスキング、または当該個人データに対応付けられた仮想トークンの使用を含む、適切なデータセキュリティ措置
(2) 当該データ受託者または当該データ処理者が使用するコンピュータ資源へのアクセスを制御するための適切な措置
(3) 当該個人データへのアクセスの可視性を確保するため、適切なログの記録、監視およびレビューを通じて、不正アクセスの検出、調査および再発防止のための是正措置を可能にすること
(4) 当該個人データの機密性、完全性または可用性が、個人データの破壊、アクセス喪失その他の理由により損なわれた場合であっても、バックアップその他の手段により継続的に処理を行うための合理的な措置
(5) 不正アクセスの検出、調査および再発防止のための是正措置、ならびに個人データ侵害が発生した場合の継続的な処理を可能にするため、現行法の遵守により別途保持が必要とされる場合を除き、当該ログおよび個人データを1年間保持すること
(6) 当該データ受託者と当該データ処理者との間で締結される契約において、合理的なセキュリティ保護措置を講じるための適切な規定を設けること
(7) セキュリティ保護措置の効果的な遵守を確保するための適切な技術的および組織的措置

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
データ侵害発生時の対応マニュアルの作成

■ DPDP規則によって定められた個人データ侵害の通知義務の詳細は以下の通り（規則7条）。個人データの侵害を防ぐための十分な保護措置を講じられなかった場合のDPDPA上の制裁金は25億インドルピー（約43億円）以下。

影響を受けたデータ主体への通知義務（規則7条（1））

- データ受託者は、個人データ侵害を認識した場合、自己の知る限りの範囲で、影響を受けた各データ主体に対し、当該データ受託者に登録されたユーザーアカウント又はその他の連絡手段を通じて、簡潔、明確かつ平易な方法で、遅滞なく通知しなければならない。通知には、少なくとも次の事項を含めなければならない。
  (a) 侵害の内容（その性質、範囲、発生の時期及び場所を含む）の説明
  (b) 当該侵害から生じる可能性のある、データ主体に関連する結果
  (c) リスクを軽減するためにデータ受託者が講じた又は講じている措置（該当する場合）
  (d) 自己の利益を保護するためにデータ主体が講じることができる安全対策
  (e) データ主体からの問い合わせに対応できるデータ受託者の代表者の業務連絡先情報
- ここで「ユーザーアカウント」とは、データ主体がデータ受託者に登録したオンラインアカウントを指し、データ主体が当該データ受託者のサービスにアクセスできるプロフィール、ページ、ハンドル名、電子メールアドレス、携帯電話番号その他これらに類するものを含む。

DPBIへの通知義務（規則7条（2））

- データ受託者は、個人データ侵害を認識した場合、DPBIに対して以下の事項を通知しなければならない。
  (a) 侵害の内容（その性質、範囲、発生の時期及び場所、並びに想定される影響を含む）の説明を、遅滞なく通知すること。
  (b) 侵害を認識してから72時間以内、又はこの目的のために書面による要請に基づきDPBIが認めたより長い期間内に、少なくとも次の事項を通知すること。
    (i) (a)の説明に関する最新かつ詳細な情報
    (ii) 侵害に至った事象、状況及び原因に関する概要の事実
    (iii) リスクを軽減するために講じた又は提案されている措置（該当する場合）
    (iv) 侵害を引き起こした者に関する調査結果（該当する場合）
    (v) 当該侵害の再発防止のために講じた是正措置(vi) 影響を受けたデータ主体に対して行った通知に関する報告書

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
背景情報（データ主体の権利①：アクセス権、訂正及び消去の権利）

■ DPDPA上、データ主体には、以下の権利が認められており、データ受託者は、権利行使に対応する必要がある。

権利	内容
アクセス権（11条）	✓ データ主体は、個人データの処理について以前に同意（7条（a）の特定された目的に係る同意を含む。）を与えたデータ受託者に対し、所定の方法で請求することにより、当該データ受託者から以下の情報を提供される権利を有する ① 当該データ受託者によって処理されている個人データの概要、及び当該個人データに関して当該データ受託者によって行われている処理行為 ② 当該データ受託者が個人データを共同利用する他の全てのデータ受託者及びデータ処理者の身元、並びに共同利用される個人データの説明、及び ③ 当該データ主体の個人データ及びその処理に関連するその他の情報（規則に規定されるもの） ✓ 上記②及び③は、データ受託者が、法令により当該個人データを取得する権限を有する他のデータ受託者との間で、当該他のデータ受託者が書面で行った要請に基づき、犯罪・サイバー事件の予防・発見・調査、又は、犯罪の訴追・処罰を目的として、個人データを共有する場合には、適用されないものとする
訂正及び消去の権利（12条）	✓ データ主体は、以前にその処理につき同意（7条（a）の同意を含む。）した個人データについて、施行中の法律に基づく要件ないし手続に従って、訂正、補完、更新及び消去を受ける権利を有する ✓ データ受託者は、データ主体から訂正、補完又は更新の請求を受けた場合、次のことを行う • 不正確な又は誤解を招くような個人データを訂正する • 不備のある個人データを補完する • 個人データを更新する ✓ データ主体は、データ受託者に対し、所定の方法により、自己の個人データの消去を請求するものとし、データ受託者は、当該請求を受領した場合、特定された目的又は施行中の法令を遵守するために当該個人データを保有する必要がある場合を除き、当該データ主体の個人データを消去するものとする

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
背景情報（データ主体の権利②：苦情処理の権利、指名権）

■ DPDPA上、データ主体には、以下の権利が認められており、データ受託者は、権利行使に対応する必要がある。

権利	内容
苦情処理の権利（13条）	✓ データ主体は、次のことに関するデータ受託者又は同意管理者の作為又は不作為につき、データ受託者又は同意管理者から容易に利用可能な苦情の救済手段を提供される権利を有する ① 自己の個人データに関するデータ受託者又は同意管理者の義務の履行 ② DPDPA及び規則に基づく自己の権利の行使 ✓ データ受託者又は同意管理者は、上記の苦情に対して、その苦情を受領した日から定められた期間内（データ受託者の全てについて定められる場合とデータ受領者の部類によって定められる場合があり得る）に回答しなければならない ✓ データ主体は、DPBIに訴える前に、本条に基づく苦情の救済の機会を尽くさなければならない
指名権（14条）	✓ データ主体は、データ主体が死亡した場合又は無能力となった場合において、DPDPA及び規則に従ってデータ主体の権利を行使する他の個人を所定の方法で指名する権利を有する • 「無能力」とは、心神喪失又は身体虚弱のために、本法又はこれに基づく規則の規定に基づいてデータ主体の権利を行使することができないことをいう

■ 実務上は、外国の包括的データ保護法においては、このようなデータ主体の権利行使への対応をスムーズに行うために、各権利行使があった場合の対応を規定する「権利行使対応マニュアル」を定める場合もあり、DPDPA対応においても同様の対応を行うことも考えられる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 2-2：社内規程・体制等の整備
背景情報（データ主体の権利③：データ受託者・同意管理者の義務等）

■ DPDP規則上、データ主体の権利との関係で、データ受託者・同意管理者について以下のような義務等が規定されている（規則13条）。

	内容
情報提供義務（1項）	データ主体が本法に基づく権利を行使できるようにするため、データ受託者及び（該当する場合）同意管理者は、次に掲げる事項を、そのウェブサイト又はアプリ、又はその両方に掲載しなければならない。 (a) データ主体が当該権利を行使するために利用できる手段の詳細 (b) サービス利用規約に基づきデータ主体を識別するために必要とされるユーザー名その他の識別子等の詳細情報（該当する場合） この規則13において「識別子」とは、データ受託者がデータ主体を識別するために発行する任意の文字列をいい、顧客識別ファイル番号、顧客取得フォーム番号、申請参照番号、登録ID又はライセンス番号その他当該識別を可能にするものを含む。
要求方法（2項）	データ主体は、本法に基づく自己の個人データに関する情報へのアクセス及び消去の権利を行使するために、過去に個人データの処理について同意を与えたデータ受託者に対し、当該データ受託者が当該権利行使のために公表した手段及び必要情報を用いて、要求を行うことができる。
安全管理義務（3項）	すべてのデータ受託者及び同意管理者は、そのウェブサイト又はアプリ（又はその両方）において、データ主体の苦情対応のための苦情処理システムに基づく対応期間を公表し、当該期間内に効果的に対応できるよう、適切な技術的及び組織的措置を実施しなければならない。
権利行使のための個人指名（4項）	データ主体は、本法に基づく指名の権利を行使するため、データ受託者の利用規約及び適用される法令に従い、当該データ受託者が当該権利行使のために公表した手段及び必要情報を用いて、1人又は複数の個人を指名することができる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 3：コンプライアンス措置の実施

- Step 2-1-3で作成・更新したプライバシーポリシー（通知）を自社ウェブサイト又はアプリ（又はその両方）に掲載し、DPDP規則に適合する形で、通知を他の情報から独立して提示し、必須記載事項（個人データの項目別説明、特定された目的、権利行使・同意撤回・DPBIへの苦情申立ての手段／リンク等）を含める。必要に応じてデータ主体に対して個別のプライバシー通知を実施する。

- データ主体の同意に基づき個人データを処理する場合等、必要に応じてデータ主体からの同意を取得する。同意の撤回は同意付与と同程度に容易であることを確保し、撤回導線（ウェブサイト／アプリ上のリンク等）を運用に組み込む。

- データ受託者は、データ処理者を使用する場合、データ処理者との間で処理契約を締結する。処理契約には、DPDP規則に基づく合理的セキュリティ保護措置（最低要素を含む）、侵害発生時の即時報告・協力、ログ及び個人データの1年保持を含む保持・削除の整合、同意撤回時の処理停止、下請管理等を明記する。

- 個人データの処理に係る社内規程、データ侵害発生時の対応マニュアル等を社内展開し、関係者に周知徹底する。侵害対応マニュアルには、影響を受けたデータ主体への遅滞ない通知、DPBIへの遅滞ない初期通知および72時間以内の詳細報告（延長の可能性を含む）を組み込む。

- データ主体からの権利行使対応の担当者等に権利行使対応マニュアルを周知する。ウェブサイト／アプリ上に権利行使手段、識別子（該当する場合）等を掲示し、苦情処理システムの対応期間（90日）に沿って処理できる体制・手順を整備する。

- 必要に応じ、関係者に対する研修等を行う。研修内容には、通知・同意（撤回含む）、侵害時対応（期限・二段階報告）、データ処理者管理（契約・監査・連絡手順）、権利行使・苦情対応（対応期間）を含める。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

Step 4：継続的なコンプライアンス対応

- データ主体からの権利行使（アクセス、消去、指名等）及び同意の撤回又は同意しない旨の表明に適切に対応する。
  - この際、DPDP規則に基づき、公表した手段・手続に従って処理を行い、苦情対応については所定の対応期間（90日）内に対応できる体制を維持する。

- 個人データの侵害が発生した場合には、社内の対応マニュアルに基づき対処する。
  - 具体的には、影響を受けたデータ主体への遅滞ない通知、及び、DPBIへの**遅滞ない初期通知並びに72時間以内の詳細報告（必要に応じた延長申請を含む）**を適切に実施する。

- 継続的に従業員に対する研修を実施する。
  - 研修内容には、権利行使・同意撤回対応、個人データ侵害時の対応手順、データ処理者管理、及び苦情・紛争対応の基本事項を含める。

- 今後、改正又は新たに発出される可能性のある規則、通達その他の当局ガイダンス（個人データのインド域外移転を制限する国又は地域の指定等を含む）について、随時最新情報を確認し、必要に応じて、プライバシーポリシー、通知文書、処理契約、社内規程その他のコンプライアンス文書の見直し及び更新を行う。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

III.インド2025年デジタル個人データ保護規則

© S&K Brussels LPC 2023-2025 All Rights Reserved.

主要ポイント

- DPDP規則は18か月にわたり段階的に施行され、通知および同意、個人データ侵害の通知、セキュリティ保護措置、ならびに検証可能な親権者同意に関する主要な運用上の義務は、2027年5月13日に開始する。
- インド・データ保護委員会（データ保護委員会）に関する規則は直ちに効力を生じる。これにより、データ保護委員会をできるだけ早期に立ち上げることが可能となる。
- 主要プラットフォームに対する「3年間の非アクティブ」ルールに加え、すべてのデータ受託者に対して、新たに最低1年間の保持義務（最低保持要件）が追加された。
- 子どものデータに関する適用除外が小幅に拡大され、有害コンテンツへの曝露防止のためのリアルタイム位置特定および監視が含まれるようになった。
- 重要データ受託者は、年次のデータ保護影響評価（DPIA）および監査を実施し、データ処理に用いられるアルゴリズム・ソフトウェアがデータ主体の権利に対するリスクを生じさせるおそれが低いことを確保しなければならない。
- 利用者の苦情申立て（グリーバンス）への対応について、90日の固定期限がDPDP規則に導入された。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

主要ポイント

- 1. 実施時期（規則1）
- 2. 同意取得のための通知の提供方法・形式（規則3）
- 3. 同意管理人の運用（規則4および別表第1）
- 4. 政府機関による個人データ処理（規則5および別表第2）
- 5. 合理的なセキュリティ保護措置（規則6）
- 6. 個人データ侵害の通知（規則7）
- 7. 特定目的のためのデータ保持（規則8および別表第3）
- 8. 子どもおよび障害のある者のデータの処理（規則10、11、12）
- 9. 重要データ受託者に対する追加義務（規則13）
- 10. データ主体の権利行使（規則14）
- 11. データの越境移転（規則15）
- 12. インド・データ保護委員会（規則17～21）
- 13. 上訴審判所への不服申立て（規則22）
- 14. 情報提出要求に関する政府権限（規則23）

© S&K Brussels LPC 2023-2025 All Rights Reserved.

1. 実施時期（規則1）

- DPDP規則は段階的施行アプローチを採用する（下表参照）。第1段階、すなわちデータ保護委員会の設置は直ちに効力を生じる。第2段階は同意管理人を対象とし、12か月後に運用開始となる。第3段階はその他すべての規定が効力を生じる段階であり、18か月後に開始する。下表は、これら3段階の概要を示す。
- 会員は、これらの時期がなお変更され得ることに留意すべきである。特に、電子・情報技術大臣アシュウィニ・ヴァイシュナウは、MeitYがこれらの遵守期限の短縮について産業界との協議を行っており、現在の12～18か月の実施期間を短縮する改正を行う可能性があることを示している。

段階	対象となるDPDPAの条文	対象となるDPDP規則	施行日	重点領域
第1段階（即時）	DPDPA第1条(2)、第2条、第18条～第26条、第35条、第38条～第43条、第44条(1)および(3)	規則1、2、17～21	2025年11月13日	データ保護委員会の制度的立上げ
第2段階（12か月後）	DPDPA第6条(9)および第27条(1)(d)	規則4	2026年11月13日	同意管理人—登録および義務
第3段階（18か月後）	DPDPA第3条～第5条、第6条(1)～(8)および(10)、第7条～第17条、第27条（第27条(1)(d)を除く）、第28条～第34条、第36条、第37条、第44条(2)	規則3、5～16、22、23	2027年5月13日	実体的遵守—同意取得のための通知、合理的なセキュリティ保護措置、データ主体の権利、侵害報告、紛争

© S&K Brussels LPC 2023-2025 All Rights Reserved.

2. 同意取得のための通知の提供方法・形式（規則3）

- 同意は、DPDPAにおける個人データ処理の主要な根拠であり続ける。DPDPA第5条の下で、同意は、データ主体に提供される通知を通じて取得されなければならない。これに関連して、DPDP規則3条は、データ受託者（すなわち管理者／組織）に対し、他のいかなる情報からも独立して理解できる、明確で単独の通知を発出することを求める。各通知には、以下を含めなければならない。
  - 収集される個人データの項目別説明
  - 処理の特定目的、および処理によって可能となる商品・サービス・利用形態の具体的説明
  - 同意の撤回、権利行使、ならびにデータ保護委員会への苦情申立てを可能にする連絡用リンク

- 通知に求められる詳細度は、関連情報を、文脈上最も適切なタイミングで提示する「ジャスト・イン・タイム」通知モデルにインドを近づける可能性もある。ユーザー体験チームは、利用者の関与を損なったりコンバージョンを悪化させたりすることなく、かつ、目的および関連処理について「具体的」な説明を要求する要件を満たしつつ、粒度の細かい単独のプライバシー通知を提供するサインアップ／オンボーディングのフローを設計する必要があるかもしれない。

- また、DPDPAは、公に利用可能なデータを法の適用範囲から除外している点も指摘に値する。これには、データ主体が公に利用可能とした個人データ、または法的義務により公に利用可能とされた個人データが含まれる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

3. 同意管理人の運用（規則4および別表第1）

- 同意管理人（CM）は、インドのデータ保護法制において比較的独自性のある概念である。DPDPA2条(g)の下で、同意管理人とは、データ主体が同意を付与し、管理し、見直し、撤回し、または追跡できるようにする主体をいう。
  - このモデルは、インド準備銀行のアカウント・アグリゲーター制度、国家保健庁の下での健康情報交換における同意アーキテクチャ、農業省が開発したAgriStack同意モデルといった既存の分野別枠組みに依拠している。
  - DPDPAは、同意管理人を初めて法律上認知したという点で歴史的である。
- 同意管理人は、データ保護委員会が定める技術的・運用上の標準に適合する、アクセス可能で透明で相互運用可能なプラットフォームを運用しなければならない。DPDP規則4条は、同意管理人の登録、機能、遵守義務の枠組みを定める。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

3. 同意管理人の運用（規則4および別表第1）
登録要件

- DPDP規則4条の下で、主体が同意管理人として活動できるのは、データ保護委員会から正式な登録を取得した後に限られる。別表第1のパートA（同意管理人の登録条件）は、申請者が以下を満たすべきことを定める。
  - インドで設立された会社であること
  - 最低純資産が2000万インドルピー（約3400万円）であること
  - データ保護委員会が定める標準に適合した相互運用可能な同意管理プラットフォームを運用するための十分な技術的・運用上の能力を示すこと
- 登録後、同意管理人は「データ・ブラインド」なシステムを運用しなければならない。すなわち、同意管理人のプラットフォームを通じて当事者間で共有される個人データが、同意管理人にとって読取可能でないことを確保しなければならない。同意管理人は、相互運用性も確保し、データ保護委員会の標準に従って、同意に関する各アクションをデータ受託者およびデータ主体の双方に通知しなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

3. 同意管理人の運用（規則4および別表第1）
義務およびガバナンス

■ 別表第1のパートB（同意管理人の義務）は、同意管理人に対し、（他の義務に加え）以下を求める。

- DPDPAおよびDPDP規則に基づくセキュリティ、報告、監査要件に関するものを含め、適切なデータ保護措置を実装すること
- 同意管理人が提供するサービスへデータ主体がアクセスする主要手段として、ウェブサイトおよび／またはアプリを整備し維持すること
- 同意を管理する対象となるデータ受託者との利益相反（取締役、主要人員、所有構造の水準を含む）を回避すること
- 同意取引および関連通知の記録を少なくとも7年間保持すること
- 同意管理人の支配権の変更（売却または合併など）を行う前に、データ保護委員会の事前承認を得ること

© S&K Brussels LPC 2023-2025 All Rights Reserved.

3. 同意管理人の運用（規則4および別表第1）
遵守の時期

- 規則4は、規則の公表から12か月後に運用開始となる。これは、データ保護委員会が登録および監督の仕組みを整備するための時間、ならびに同意管理人候補がシステムとガバナンス・プロセスを準備するための時間の双方を確保する趣旨である。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

4. 政府機関による個人データ処理（規則5および別表第2）

- DPDP規則5条および別表第2は、政府機関およびその関係機関が、補助金、給付、サービス、証明書、ライセンス、許可を提供する際に個人データを処理する方法を規律する枠組みを定める。別表第2は、DPDPA第7条(b)の下で権限付与された機能のために個人データを処理する際に、当該当局が従うべき最低基準を設定する。

- これらの規定の下で、政府による処理は適法であり、目的が特定され、かつ、権限付与された機能のために真に必要な範囲に限定されなければならない。当局は、個人データが完全、正確、一貫していることを確保するための合理的努力を行わなければならず、また、提示された政府目的を達成するため、または他の法的義務を満たすために必要な期間に限り保持しなければならない。

- 別表第2は（データ処理者を通じて処理が行われる場合を含め）個人データ侵害を防止するための合理的なセキュリティ保護措置を実装することを当局に求める。DPDPA第7条(b)に基づく処理が行われる場合、データ主体には通知が行われ、連絡先の明確な提示およびDPDPA上の権利を行使するためのアクセス可能な手段が提供されなければならない。別表第2は、処理の目的および手段を決定する政府当局に説明責任を負わせ、これらの基準への完全な適合を確保することを求める。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

5. 合理的なセキュリティ保護措置（規則6）

- 規則6は、すべてのデータ受託者に対し、その保有または管理下にある、あるいは自身または自己のためにデータ処理者が処理している個人データを保護する明確な義務を課す。DPDPA第8条(5)は、個人データ侵害を防止するため「合理的なセキュリティ保護措置」を講じることをデータ受託者に求めるが、DPDPA自体は、これらの保護措置が下位法令で更に詳細化されることを示していなかった。これらの保護措置を実装しない場合、最大で25億インドルピー（約43億円）の制裁金が科され得る。

- DPDP規則は、データ受託者に対し、処理ライフサイクル全体を通じて個人データの機密性、完全性、可用性を維持するよう設計された一連のセキュリティ保護措置を、最低限として採用することを求める。

- 規則6の下で、データ受託者は、以下の最低基準を実装しなければならない。
  a. 暗号化、難読化、マスキング、または仮想トークンの使用など、個人データを保護するための技術的措置
  b. 権限ある者のみが個人データへアクセスできるようにする適切なアクセス制御
  c. アクセスログの維持、および異常または無権限活動を監視できる能力
  d. 継続的監視のためのシステムを含め、無権限アクセスを検知し、調査し、是正する能力
  e. 機密性・完全性・可用性が損なわれた場合でも処理を継続できるようにする、バックアップおよび手続を含む事業継続および復旧メカニズムf. 侵害の検知、調査、是正、継続性確保を支援するため、ログおよび関連する個人データを少なくとも1年間保持すること（他の適用法令でより長い保持が義務付けられる場合を除く）
  f. データ受託者が関与させるすべてのデータ処理者に対し、規則6を完全に遵守させるための契約上の保護措置（処理契約への明示的なセキュリティおよび遵守義務の組込みを含む）
  g. 処理活動の性質、範囲、リスクに整合した適切な技術的・組織的措置の実装

© S&K Brussels LPC 2023-2025 All Rights Reserved.

5. 合理的なセキュリティ保護措置（規則6）

- 実務上、規則6に適合するためには、これまでデータ保護の枠組みに一度も適合してこなかった多くの中小企業が、技術的・組織的セキュリティ統制を大幅に構築する必要がある。
- 組織は、暗号化、細粒度のアクセス制限、セキュリティ監視システム、詳細なログ取得能力を導入または強化しなければならない。
- 包括的なインシデント対応手順を整備し、職員にセキュリティ・プロトコルの訓練を行い、信頼できるバックアップおよび継続性の取り決めを整える必要がある。
- 同様に、ログおよび一定類型の個人データについての1年保持義務は、運用コストおよびデータ保管コストを増加させ、規則6の最低基準と整合させるための社内データ保持ポリシーの更新も必要となる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

6. 個人データ侵害の通知（規則7）

- DPDPA第8条(6)は、データ受託者に対し、個人データ侵害について、データ保護委員会および影響を受けた各データ主体の双方に通知することを求める。侵害を報告しない場合、最大で20億インドルピー（約34億円）の制裁金が科され得る。規則7は、二段階の侵害報告義務を導入する。

- (1) 第1段階：初期通知（Initial Intimation）
  - 宛先：影響を受けたデータ主体
    - 期限：「遅滞なく」
    - 内容要件：侵害の説明、発生し得る結果、リスクを低減するために講じた措置、データ主体が自己の利益を保護するために取り得る安全対策、問い合わせのための連絡先情報
  - 宛先：データ保護委員会
    - 期限：「遅滞なく」
    - 内容要件：侵害の性質、範囲、発生時期および発生場所、想定される影響
- (2) 第2段階：詳細報告（Detailed Report）
  - 宛先：データ保護委員会（DPB）
    - 期限：72時間以内
    - 内容要件：原因および関連する事象に関する事実、責任を負う者に関する認定、講じた緩和措置および是正措置、データ主体に送付した通知に関する報告

- 重要性の閾値が存在しないため、軽微な事案であっても、形式上は個人データ侵害の通知義務が発生することになる。これは、影響の小さい報告でデータ保護委員会が過負荷になるおそれや、利用者側に「通知疲れ」を生じさせるおそれがある。加えて、72時間の報告期限は一部の分野別要件と異なる。例えば、インドのコンピュータ緊急対応チーム（CERT-In）は、事業体に対し、インシデントを認知してから6時間以内に報告することを求めている。この点は、企業内の既存報告プロセスにさらなる複雑性を加え得る。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

7. 特定目的のためのデータ保持（規則8および別表第3）

- DPDPAの下では、個人データは、特定目的を達成するために必要な期間、または法的義務を遵守するために必要な期間に限って保持できる。しかし、規則8の導入により、目的が達成された後または同意が撤回された後であっても、データ受託者は次のことを行わなければならない。
  - 個人データ、関連するトラフィック・データ、処理ログを少なくとも1年間保持すること
  - その後、他法令により、より長い保持期間が要求される場合を除き、当該データを削除すること

- 該当する場合、データ受託者は、データ処理者にも同一の削除および保持要件を遵守させなければならない。

- 一定類型のデータ受託者には、強化された保持ルールが適用される。対象は以下を含む。
  - インド国内で利用者が2,000万人以上のECプラットフォームおよびソーシャルメディア・プラットフォーム（仲介者）
  - インド国内で利用者が500万人以上のオンラインゲーム・サービス（仲介者）

- これらの主体については、次が適用される。
  - 利用者が非アクティブとなってから3年後に個人データを削除しなければならない。ただし、次の場合を除く。
    - アカウントへのアクセスを維持するために当該データが必要な場合
    - データ主体が仮想トークンを使用している場合
  - データ削除の前に、データ主体へ48時間前の事前通知を行わなければならない。
    - ただし、個人データ、トラフィック・データ、処理ログについて最低1年間保持する要件は引き続き適用される。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

8. 子どもおよび障害のある者のデータの処理（規則10、11、12）

- DPDPAの下では、データ受託者は、18歳未満の子どもの個人データを処理する前に親権者同意を取得しなければならない。

- 規則10は、同意を与える者が以下であることを確認するための適切な技術的・組織的措置を実装することをデータ受託者に求める。規則10は、同意者が特定可能な成人であることの確認を要求するにとどまり、親子関係の証明までは要求しない。

  1. 特定可能な成人であること
  2. 子どもの親であると自認する者であること

- 確認は、以下のいずれかの方法で行うことができる。
  - データ受託者が既に保有する信頼できる本人確認および年齢情報（親が当該プラットフォーム／サービスの既存利用者である場合）
  - 当該個人が任意に提供する本人確認または年齢情報（身分証その他の手段による）
  - 本人確認情報に紐づく仮想トークンで、インド政府により告示されたデジタルロッカー提供者などの権限ある主体が発行したもの

- 規則11は、法定後見人を有する障害のある者についての検証可能な同意を扱う。この場合、データ受託者は、後見人が裁判所、指定当局、または地方レベル委員会により適用法令の下で正式に選任されていることを確認しなければならない。規則11は、同意を受け入れる前提として、後見人に法的に付与された権限の検証を要求する。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

8. 子どもおよび障害のある者のデータの処理（規則10、11、12）

- 規則12および別表第4は、DPDPA第9条に基づく2つの主要義務について適用除外を定める。
  - 第一に、別表第4で定める特定類型のデータ受託者を、子どもの個人データの処理に関する親権者同意（DPDPA第9条(1)）の取得義務から除外する。
  - 第二に、同様の主体について、別表第4に定める限定目的のために、子どもの追跡または行動モニタリングを許容する（これらの活動は、DPDPA第9条(3)の下では通常制限される）。

- 具体的に、DPDP規則は、臨床施設および医療専門職、教育機関、ならびに託児施設およびチャイルドケア施設を、一定の目的のために処理が行われる限り、子どもの行動モニタリングまたは追跡に関する制限から適用除外とする。目的には、医療サービスの提供、教育活動の支援、子どもの安全確保が含まれる。

- なお、DPDP規則は「教育機関」を、職業教育を含む教育を施す学習機関と定義している。これがエドテック企業に及ぶかは、明示的に言及されていないため依然として不明である。

- これらの義務に適合しない場合、最大で20億インドルピー（約34億円）の制裁金が科され得る。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

9. 重要データ受託者に対する追加義務（規則13）

- DPDPAの下では、一定のデータ受託者またはその類型は、(a) 処理する個人データの量と機微性、(b) データ主体の権利に対するリスク、(c) 公共秩序、国家主権、国家安全保障、選挙民主主義に関する考慮を含む要素に基づき、中央政府により重要データ受託者として指定され得る。

- 重要データ受託者は、DPDPAの下で遵守義務が強化され、インド所在のデータ保護オフィサーを選任し、独立したデータ監査人を関与させてDPDPAへの遵守状況を評価させることなどが含まれる。これらの義務はDPDP規則でさらに具体化されている。

- 中央政府は、どのデータ受託者（または類型）が重要データ受託者に指定されるかをまだ告示していない。指定後、当該主体は以下の義務を負う。

  - a.年次の評価および監査（規則13条(1)および(2)）

    - 重要データ受託者は、重要データ受託者として告示された日から12か月ごとに、DPDPAおよびDPDP規則への遵守を確保するためのデータ保護影響評価（DPIA）を実施しなければならない。

    - 重要データ受託者は、DPDPAおよびDPDP規則への遵守を評価する独立したデータ監査も受けなければならない。

    - 重要データ受託者は、これらのDPIAおよび監査における重要な所見を取りまとめた報告書をデータ保護委員会に提出しなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

9. 重要データ受託者に対する追加義務（規則13）

- 中央政府は、どのデータ受託者（または類型）が重要データ受託者に指定されるかをまだ告示していない。指定後、当該主体は以下の義務を負う。

  - b.技術的・アルゴリズム的システムに関するデューデリジェンス（規則13条(3)）
    - 重要データ受託者は、アルゴリズム・システムを含む、個人データを処理するために用いるすべての技術的措置が、データ主体の権利に対するリスクから保護するよう設計され、試験され、検証されていることを確保するためのデューデリジェンスを実施しなければならない。
    - この義務は、個人データをホストし、表示し、アップロードし、改変し、公表し、送信し、保存し、更新し、共有するために用いられるシステムにも及ぶ。

  - c.データの越境移転制限への遵守（規則13条(4)）
    - 重要データ受託者は、政府が定める、個人データおよび関連トラフィック・データのインド国外移転に対する制限に従わなければならない。
    - これらの制限は、DPDP規則の下で設置される指定委員会の提言に基づき発出される。

- 中央政府は、（IT規則2021年の下で行われたのと同様に）大規模ソーシャルメディア・プラットフォーム、主要テック企業、ならびに金融、銀行、医療などの機微かつ高度規制の分野に属する組織を重要データ受託者として指定すると見込まれる。しかし、DPDPAは関連要素の列挙において「含む（including）」という語を用いているため、重要データ受託者に該当する主体を決定するにあたり、政府は追加基準も考慮できる広い裁量を保持する。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

10. データ主体の権利行使（規則14）

- DPDPAの下で、データ主体は以下の権利を有する。
  - 処理されている自己の個人データの要約へのアクセス
  - 自己の個人データの訂正または消去
  - 死亡または無能力の場合に権利を行使する者として他者を指名すること
  - 「容易に利用可能な手段」により苦情救済（苦情処理）を求めること
- これらの権利を可能にするため、データ受託者は以下を実施しなければならない。
  - 権利行使に関する明確な情報の公表：データ受託者は、データ主体が権利を行使する方法（手段、識別子、申請に必要な事項を含む）を説明する、明確でアクセス可能な枠組みを公表しなければならない。
    a. 支援システムとプロセスの整備：組織は、申請を受領した後に、データ主体が実質的に権利を行使できるようにする社内システムおよび手続を運用化しなければならない。
    b. 実効的な苦情救済メカニズムの提供：データ受託者および同意管理人は、苦情救済メカニズムを実装し公表し、苦情に90日以内に回答することを確保しなければならない。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

11. データの越境移転（規則15）

- DPDPAは、越境移転について「ネガティブ・リスト」方式を採用し（第16条(1)）、中央政府が特に制限しない限り、個人データを任意の法域へ移転できる。これは、厳格なデータ・ローカライゼーション要件を想定していた従前の立法草案からの大きな転換であった。しかし、2025年1月の草案規則は、将来のデータ流通条件に関する規制上の制約や不確実性を再び開き得る新規定を再導入していた。DPDP規則はこれらの規定を維持している。

- 規則15の下で、インド国外に個人データを共有または移転しようとするデータ受託者は、中央政府が発出する「一般または特別の命令」に従わなければならない。この義務は、移転された個人データが外国国家、またはその国家の機関の支配下にある者・団体によりアクセス可能となり得る状況で適用される。現時点ではそのような命令は発出されていないが、この枠組みは、越境処理に関与するデータ受託者、とりわけグローバルなサービスモデルを運用する主体にとって、運用上の課題および不確実性を生じさせ得る。

- 今後、移転制限の可能性に関する政府の発言やメッセージ、ならびにインドにおける国家安全保障や公共秩序に影響すると認識され得る重大動向が生じた場合に注意すべきである。また、重要データ受託者に対する越境データ制限を議論する指定委員会の設置に関する報道が出ることも、より広範な制限が一般のデータ受託者にも課され得る兆候となり得る。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

12. インド・データ保護委員会（規則17～21）

- DPDPAは、DPDP枠組みの執行を担う法定機関としてデータ保護委員会を設置する。データ保護委員会は「デジタル・オフィス」として機能するよう設計されている。DPDP規則は、その運用に関する詳細規定を定め、以下を含む。
  - 議長および委員の任命と資格
  - 会議、定足数、投票に関する手続
  - 委員会決定の発出、認証、伝達のプロセス

© S&K Brussels LPC 2023-2025 All Rights Reserved.

13. 上訴審判所への不服申立て（規則22）

- データ保護委員会の決定に対する不服申立ては、DPDPAの枠組みにおける上訴審判所として機能する電気通信紛争解決・上訴審判所（TDSAT）に提起しなければならない。不服申立てはデジタルで提出され、民事訴訟法ではなく自然正義の原則に従って審理され、1997年インド電気通信規制庁法の下での上訴に適用されるものと整合する手数料の支払いを要する。

- なお、TDSATは、1997年インド電気通信規制庁法により、許認可者（中央政府）と被許認可者（電気通信事業者）の間、複数の電気通信サービス提供者の間、またはサービス提供者と消費者の間の紛争を解決し、電気通信事業者および利用者双方の利益を保護することを目的とする裁判機関として設立された。データ保護紛争は性質と複雑性が異なるため、TDSATがどの程度効果的にこれらを扱い判断できるかは、今後見極める必要がある。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

14. 情報提出要求に関する政府権限（規則23）

- 中央政府は、権限を与えられた職員を通じて、データ受託者または仲介者に対し、別表第7に列挙される目的（国家安全保障および法執行機能に関する事項を含む）のために情報を提出するよう求めることができる。また、その要請の開示がインドの主権、統合、または安全を害する場合、中央政府は、その要請が行われた事実を開示しないよう当該主体に指示することもできる。

© S&K Brussels LPC 2023-2025 All Rights Reserved.

今後の見通し

- DPDP規則の告示により、DPDPAの全面的な運用化に向けた移行が正式に開始された。中央政府は、能力構築および認知向上の取り組みを継続すると見込まれる。

- もっとも、いくつかの重要事項はなお追加の明確化を要する。具体的には以下である。

  - データ保護委員会の議長および委員を任命する選考委員会の構成
  - DPDPA第10条(1)に基づく重要データ受託者の指定
  - DPDPA第16条(1)に基づき個人データ移転が禁止され得る制限対象法域の告示
  - DPDPA第17条(3)に基づき、スタートアップを含む一定のデータ受託者（または類型）が法の特定規定から除外され得る対象の特定
  - DPDPA第17条(5)に基づき、一時的適用除外が付与され得るデータ受託者の類型の特定

© S&K Brussels LPC 2023-2025 All Rights Reserved.

S&K Brussels

S&K Brussels法律事務所は、2019年にベルギーのブリュッセルで開業した日本の法律事務所であり、急速に進化する情報テクノロジーと規制の接点――データ保護・プライバシー保護、AI規制、データ利活用、宇宙活動規制などの法分野における専門性を強みとし、EU、米国、インド、日本などの主要法域に対応する国際的なリーガルアドバイザーです。

S&K Brussels Website: https://sandkbrussels.com/

この文書には、S&K Brussels法律事務所に帰属する機密情報が含まれています。本書は、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許可なく複製、翻案、公衆送信等することを禁じます。本書に記載されているサービス名及び会社名は、各社の商号、商標又は登録商標です。本書に記載されているサービスの仕様及びその他の情報は、予告なく変更されることがあります。

© S&K Brussels LPC 2023-2025 All Rights Reserved.