

インドのデータ保護制度 間もなく施行

個人データ保護法案 (2018年起草)

本資料は2018年7月草案の内容に基づくものですが、法律の最終化段階において内容が変更となる可能性もある点にはご注意ください。



概要

インドは、真のデジタルエコノミー大国になるという夢の実現に向け、また一歩前進しました。インド最高裁がプライバシーは基本的人権であるという画期的な判決を下してから約1年後の2018年7月27日、「BN Srikrishna判事委員会」(以下、「委員会」)は、個人データ保護法案(以下、「PDPB」または「法案」)の最初の草案を発表しました。

法案に「Fiduciaries (データの信託をうけた管理者、以下「管理者」)」という言葉が使われていることから分かるように、その意図はデータ管理者 (GDPRの「Controller」と同様) とデータ主体 (個人データを処理される個人、GDPRの「Data subject」と同様) の間に「信頼ベースの関係」を築くことにあります。

委員会は、データエコノミーの先進的で変化の激しい性質も考慮し、インド国内に物理的な拠点を持たなくても、インドで製品やサービスを提供している企業はPDPBの規制対象となるよう適用範囲を拡大しています。

PDPBの成立後、企業が遵守するまでには12カ月の猶予期間が設けられます。

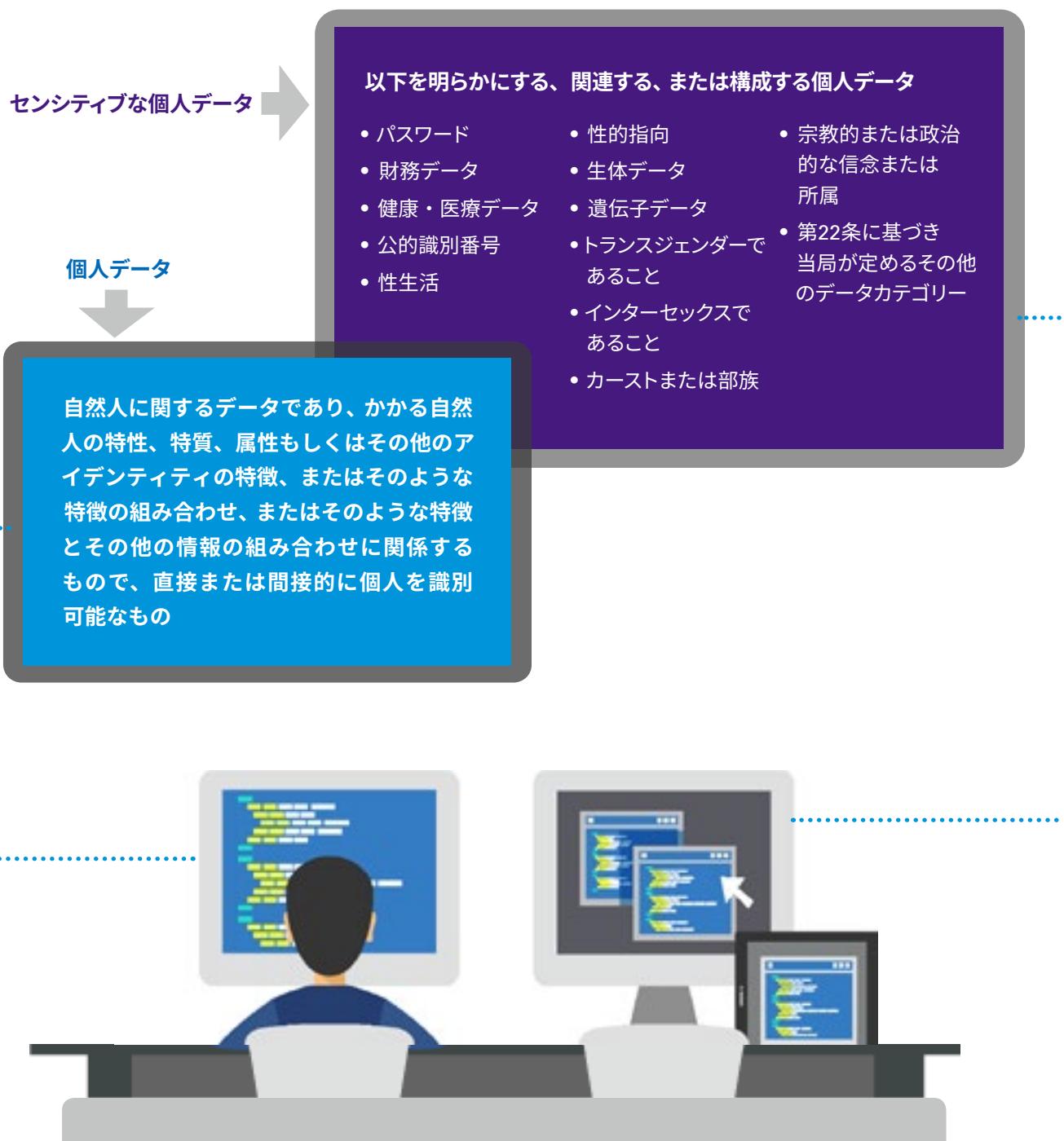


法案の主なポイント

1. インド居住者 (データ主体) の個人データを処理する組織 (データ管理者/データ処理者) に対し、透明性を維持し、記録を保存し、DPIA (データ保護影響評価) を実施し、データ保護責任者 (DPO) を任命し、侵害を迅速に通知するなどのデータ保護義務が課されます。
2. インド居住者 (子供を含む) の個人データおよびセンシティブな個人データを処理するための、法的な根拠が定義されます。法案は、当該の法的根拠を明らかにする立証責任を明確にデータ管理者に課していますが、国が行うデータ処理についてはあまり踏み込んでいません。
3. データ主体には、GDPRでデータ主体に与えられる権利と同様のデータポータビリティ権や消去権などの権利により、データ管理者によって処理される自身の個人データを管理できる権利が与えられます。
4. 透明性と説明責任を確保するために、データ主体の個人データを処理する際に、プライバシーバイデザイン、通知、非識別化、暗号化などの措置を整備するよう、データ管理者に対する提案がなされています。インド企業は、処理するデータのセキュリティ保証についてはグローバル基準と同じ土俵にありますが、プライバシーバイデザインなどの概念の実現には、さらに時間とリソースコストが必要かもしれません。
5. 法案では、個人データのコピーをインドのサーバーまたはデータセンターに保存することを義務づけるデータローカライゼーション規定が盛り込まれています。中央政府またはDPAI (インドデータ保護局) によって通知される重要個人情報と呼ばれる特定カテゴリーのデータは、インド国内にあるサーバーまたはデータセンター以外で処理してはなりません。

6. PDPBへの不遵守が判明した個人または組織に対する罰金が提案されています。不遵守に対しては、全世界の売上高の最大2～4%または5000万～1億5000万ルピー（いずれか高い方）の罰金が科される可能性があります。さらに、データ主体の権利行使に関する対応の期限を守らなかった場合、不履行が続く間、1日につき5000ルピー、最大100万ルピーの罰金が科されます。
7. 中央政府によるDPAIおよび上訴審判所の設立が提案されています。専門の上訴審判所によって、問題や当局が受けた苦情を迅速に解決できます。ただし、企業が法案に従うために遭遇する様々な問題について、当局が積極的にガイダンスを提供する必要があります。

個人データとセンシティブな個人データの要素¹



1. The Personal Data Protection Bill 2018, Government of India, July 2018

企業がPDPBを遵守するためにしなければならないこと

企業はPDPBで規定された責務に合わせて、しっかりとしたプライバシー保護の枠組みを作成する必要があります。この法案は、企業を「データ管理者 (DF)」と「重要データ管理者 (SDF)」(DPAIにより通知されます) に分類し、それぞれに次のような責務を課しています。



データ保護責任者 (DPO) — (SDF)

データ管理者は、PDPBで定められた役割を遂行するインドにおけるデータ保護責任者を、インドにデータ管理者の事業所があるかどうかにかかわらず任命しなければなりません。その役割は、データ管理者に対するPDPBに基づく責務の遂行についての助言、データ主体の個人データの処理に関連する業務のモニタリング、あらゆる記録のリストの保存、DPAIの連絡先の役割、データ主体の苦情対応などです。



データ保護影響評価 (DPIA) — (SDF)

データ管理者は、新技術または大規模プロファイリングに伴う処理の実行、遺伝子データや生体データなどのセンシティブな個人データの使用、あるいはデータ主体に重大な損害が及ぶリスクのあるその他の処理を予定している場合、DPIAを行わなければなりません。



記録の保存 — (SDF)

すべてのデータ管理者 (国を含む) は、データのライフサイクルにおける重要な処理の正確かつ最新の記録を保存し、PDPBに基づく責務を遵守していることを証明する必要があります。



データ処理者との契約要件

データ管理者は、自らに代わりデータ処理者にデータ主体の個人データを処理させる場合、有効な契約を介して実施しなければなりません。



プライバシーバイデザイン — (DF・SDF)

データ管理者は、データ主体に生じる損害を予測し、特定し、回避するようなプロセスとシステムが設計されるよう、ポリシーと対策を策定・実施する必要があります。



透明性の維持 — (DF・SDF)

データ管理者は、個人データの処理に関する一般的なポリシーについて透明性を維持し、その情報を (PDPBの規定に基づき) アクセスしやすい形式で提供するため、妥当な手段を講じる必要があります。



個人データ侵害の迅速な通知 — (DF・SDF)

データ管理者は、個人データ侵害が生じた場合、DPAIが指定する時間内でできるだけ早くDPAIに通知しなければなりません。



データ監査 — (SDF)

データ管理者は、個人データ処理のポリシーと実施内容について、年に一度、独立性を有する監査人による監査を受けなければなりません。



苦情対応の仕組みの用意 — (DF・SDF)

すべてのデータ管理者は、データ主体の苦情に対し、30日以内に効率的かつ迅速に対応する適切な手順と有効な仕組みを整備する必要があります。



その他の責務

- 同意の証明 (DF・SDF)
処理を進めるために同意が必要な場合、データ管理者はデータ主体から有効な同意を取得した上で、同意が得られたことを明示する仕組みを用意しなければなりません。
- データ主体による要求の支援 (DF・SDF)
データ管理者は、データ主体がPDPBに基づく権利を行使しやすいようにする必要があります。
- DPAIへの登録 (SDF)
重要データ管理者は、DPAIが規定する方法により、自らをDPAIに登録する必要があります。

越境移転

法案は、個人データの越境移転の規制に重点を置き、データ主体の個人データをインド国外へ移転する際に遵守すべき制限と条件を課しています。特に多国籍企業は、データ管理慣行を見直し、これらの制限に従うとともに法案で定められた条件へのコンプライアンスを確保する手段を考える必要があります。主な制限をいくつか以下に挙げます。

1. 個人データのコピーを少なくとも1部、インドにあるサーバーまたはデータセンターに保存すること。
2. 重要個人情報（中央政府により通知される）は、インド国内のサーバーまたはデータセンターでのみ処理すること。

さらに、法案では個人データの移転について、以下のような主な条件を提案しています（ただし、個人データが制限対象に該当するものではないことを条件とします）。

1. 移転が標準契約条項（DPAIが承認するもの）に従って行われる場合で、データ主体がそのような移転に対して同意または明示的な同意（センシティブな個人データの場合）を与えた場合
2. 個人データを中央政府が認定した国へ移転する場合で、データ主体が移転に対し同意または明示的な同意（センシティブな個人データの場合）を与えた場合
3. 個人データの個々の移転または1組の移転について、その必要性につき特にDPAIの承認を得た場合

法案は、個人データの越境移転を必要とする緊急事態について考慮しており、身体的な健康または救急サービスの提供のために必要な場合には、センシティブな個人データをインド国外に移転することができます。



PDPBとGDPRの比較

GDPRの主要概念は、PDPB案にも反映されています。主な類似点をいくつか挙げます（ただし、すべてを網羅しているわけではありません）。

1. GDPRにおけるデータ管理者 (Controller)、処理者 (Processor)、データ主体 (Data Subject) に対し、データ管理者 (Fiduciary)、データ処理者 (Processor)、データ主体 (Data Principal) という用語が充てられています。
2. 「適法性、公平性および透明性」、「目的の制限」、「収集の制限」、「データの品質」、「保存の制限」、「説明責任」などのGDPRの主要原則は、PDPB案にも組み込まれています。
3. PDPBによる個人の定義には、GDPRによる自然人の定義と同様、市民だけでなく居住者も含まれています。
4. 「訂正の権利」、「確認およびアクセス」、「ポータビリティの権利」、「忘れられる権利 (消去権)」など、GDPRにおけるデータ主体の主な権利は、PDPBでもデータ主体に与えられます。
5. データ管理者に課される処理記録の保存、DPIA実施、侵害の迅速な通知、DPOの任命に関する責務は、GDPRにおけるデータ管理者の責務に酷似しています。
6. 世界売上高の2%ないし4%という罰金案は、GDPRの罰金案と同様です。

これらのGDPRとの類似点のほかに、同法案には、草案作成時にインド市場への適用可能性を念頭に置いたと見られる変更点があります。それらの変更点をいくつか挙げます（ただし、すべてを網羅しているわけではありません）。

1. 雇用に関する個人データの取扱いについて、処理の法的根拠が明確に特定されています。GDPRでは、この点はさほど明示的ではありません。
2. データ管理者に対し、独立性を有する監査人による年1回の監査が義務づけられています。確立された保証プログラムおよび認定制度を採用することは、企業がこの法令要件を満たすことを明確にするものと考えられます。
3. 内部通報制度、M&A、与信評価などの妥当な目的での処理について明記されています。
4. GDPRで定義されているDPOの役割や責任と異なり、同法案によるDPOは、必要に応じて他の役職を兼ねることができます。GDPRは、利益相反を避けるため

にDPOの責任には明確な線引きをしています。同様の指針がないため、利益相反を避ける責任は企業に委ねられることになります。

5. 同法案の適用を受ける、民間企業や中央または州の省庁などの様々な関係者ごとに、法令違反の区分が明示されています。さらに、法令違反に対して多層的で詳述された罰則規定が定められています。
6. 同法案では、国家安全保障の目的、ジャーナリズムの目的、家庭内の目的での個人データの処理など、適用除外となる事項について明示されています。



今後の展望

世界は個人のプライバシーに対してますます敏感になっており、PDPBの制定は、個人データの取扱いと処理に関して「安全な国」としてインドの地位を強化すると予想されます。PDPBの導入に成功すれば、インドにおけるデータプライバシーの基礎が築かれ、インド全体の企業による個人データの認識、処理、保護の方法に文化的な変化を起こすと予想されます。また、インドがデジタルエコノミーにおいてその地位をさらに高め、世界中のデータドリブン企業にとって魅力ある投資先へと発展していくことを後押しするものと思われます。

PDPBの条項を規制、執行して権利の保護を図りつつも、個人が些細なことを根拠に行政、執行、司法の効率的な機能を妨げることがないようにするため、規制機関、法執行機関、司法制度の整備、訓練、能力強化を進めることも必要です。

民間企業は、保有している個人データの棚卸しを行うとともに、法案により定められた義務を果たす上で必要な事業の改革を遂行するために、従業員のスキルを高める必要があります。PDPBの制定から企業の遵守までには12カ月の猶予期間が与えられますが、GDPRなどの規制の実施から得た教訓を考えると、この猶予期間は十分ではないと思われます。組織の広範囲にわたるコンプライアンスを推進し、経営陣が各種不遵守の責任を問われたり、刑事上、財務上の重大な影響を受けるのを防ぐには、データ保護を経営会議の重要議題として取り上げる必要があります。

新しいプライバシー制度を主導するため、各企業はこの機会にそれぞれの責務を再考して受託責任を果たす新しい有意義な方法を見だし、個人データを収集、処理、取扱い、配布する能力に対するデータ主体の信頼を獲得するべきです。



付録

用語表

略称	説明
CBI	中央捜査局
DF	データ管理者
DPAI	インドデータ保護局
DPIA	データ保護影響評価
DPO	データ保護責任者
GDPR	一般データ保護規則
PDPB / 法案	2018年個人データ保護法案
SC	インド最高裁判所
SDF	重要データ管理者
委員会	Srikrishna判事委員会
UIDAI	インド固有識別番号庁
UOI	インド連邦



インドにおけるプライバシー権の歴史

判例	時期	出来事／マイルストーン
1954 SCR 1077	1954	プライバシー権はインド憲法によって保護されない – SC in MP Sharma v. Satish Chandra, District Magistrate, Delhi
1964 SCR (1) 332	1962	プライバシー権はインド憲法によって保護されない – SC in Kharak Singh v. State of Uttar Pradesh
1978 SCR (2) 621	1978	言論と表現の自由の範囲が拡大され、この権利はもはや国の領土の境界によって制限されるものではなく、プライバシーは個人の自由とつながるものであるとされた – SC in Maneka Gandhi v UOI
1994 SCC (6) 632	1994	プライバシー権は、請求可能な権利であり、基本的権利でもある – SC in R Rajagopal v. State of Tamil Nadu
	1995	個人データの処理と自由な移動に関して個人を保護する欧州データ保護指令（指令 95/46/EC）が発行される。
(1997) 1 SCC 301	1997	プライバシー権が通信にも拡大される – 傍受規定は内務大臣だけが発行できるものであり、傍受命令の期限は2ヵ月と制限された – SC in People's Union for Civil Liberties v. UOI
	2000	2000年インド情報技術法の公示
AIR 2010 SC 1974	2010	身体的プライバシーと精神的プライバシーが区別され、第20(3)条（自己負罪に対する権利）によりプライバシー権の関係が確立された – SC in Selvi and others v. State of Karnataka and others
	2011	2011年情報技術（妥当な安全上の慣行および手続きならびにセンシティブな個人のデータまたは情報）規則
Special Leave to Appeal (CrI) No (s).2524/2014	2014	犯罪捜査を目的として本人の同意なく生体データを使用する要請が却下される – SC in UIDAI & Anr. v. CBI
	2014	欧州議会がGDPRを採択
Special Leave to Appeal (C) No. 804/2017	2016	WhatsAppのFacebookとのデータ共有に関する新しいプライバシーポリシーが德里ー高等裁判所で争われる - Karmanya Singh Sareen v. UOI
WRIT PETITION (CIVIL) NO 494 OF 2012	2017	「プライバシー権は、第21条に基づく生命および個人の自由に対する権利の本質的な部分として、かつインド憲法第3編により保証される自由の一部として保護される」 – SC in KS Puttaswamy v. UOI。MP Sharma(1954)事件およびKharak Singh(1962)事件の判決は、インド憲法はプライバシー権を保護していないとの決定に関して覆された
RBI/2017-18/153 DPSS.CO.OD No. 2785/06.08.005/ 2017-2018	2018/ 4/6	RBI通達により、すべてのシステムプロバイダーは決済システムに関するデータをインドに保存することが義務づけられた
	2018/ 5/25	EU GDPRが発効
	2018/ 7/27	PDPBおよびBN Srikrishna元判事の報告書が発行される

主な違反と罰金の一覧表²

PDPBの条項	違反	作為／不作為の種類	懲役／罰金／賠償金
70条	第6章に基づくデータ主体の要求に関する不順守	PDPBに基づきデータ主体に権利が与えられている要求にDFが従わない場合	不履行1日につき5000ルピーで、SDFの場合は100万ルピー、それ以外の場合は50万ルピーを限度とする罰金
71条	報告書、申告書、情報等の不提出	DFがDPAIに報告書、申告書または情報を提出しない場合	不履行1日につき1万ルピーで、SDFの場合は200万ルピー、その他の場合は50万ルピーを限度とする
72条	DPAが発行する指示またはその他の命令の不遵守	DFまたはデータ処理者が、DPAIの指示または命令に従わない場合	DFの場合 – 不履行1日につき2万ルピー、最大2000万ルピー データ処理者の場合 – 不履行1日につき5000ルピー、最大500万ルピー
73条	特段の罰金が規定されていない場合の違反	特段の罰金が規定されていないPDPBの条項を誰かが遵守しなかった場合	SDFの場合は1000万ルピー、その他の場合は250万ルピーを限度とする
75条	PDPBに基づく規定違反	DFまたはデータ処理者が本法案のいずれかの条項に違反した結果、データ主体が損害を受けた場合	賠償金
90条	PDPBに反する個人データの取得、移転または売却	単独か共同か、故意か意図的か無謀かを問わず、誰かが 個人データ を取得、開示、移転、売却または売出した場合	最大3年の懲役もしくは最大20万ルピーの罰金、またはその両方
91条	PDPBに反するセンシティブな個人データの取得、移転または売却	単独か共同か、故意か意図的か無謀かを問わず、誰かが センシティブな個人データ を取得、開示、移転、売却または売出した場合	最大5年の懲役もしくは最大30万ルピーの罰金、またはその両方
92条	非識別化された個人データの再識別化および処理	故意か意図的か無謀かを問わず、非識別化された個人データを、誰かが同意を得ることなく再識別化したか、再識別化して処理した場合	最大3年の懲役もしくは最大20万ルピーの罰金、またはその両方
95条	会社による違反	会社が違反を犯した場合	違反が犯された時に責任のあった者全員が違反について有罪とみなされる
96条	中央または州政府省庁による違反	中央もしくは州政府の省庁、または国の機関が犯した違反	省庁または機関の長が違反について有罪とみなされる

2. The Personal Data Protection Bill 2018, Government of India, July 2018

PDPBとGDPRの比較³

内容	PDPB	EU GDPR
用語	データ管理者 (Fiduciary)、データ処理者 (Processor)、データ主体 (Data principal)	データ管理者 (Controller)、データ処理者 (Processor)、データ主体 (Data subject)
データ処理	第4条：公正かつ妥当な処理 データ処理者は、データ主体 (GDPRのData subject) に対し、かかる個人データを公正かつ妥当な方法で処理する義務を負う。	第2章 第5条：個人データの処理に関する原則 データ管理者 (PDPBのData Fiduciary) は、個人データを取得する場合、透明性ある情報をデータ主体に提供しなければならない。
データ侵害の通知	第32条：個人データの侵害 a. データ管理者は、データ管理者が処理する個人データに関する個人データ侵害があった場合、DPAIが指定する期間内にDPAIに通知するものとする。 b. DPAIは、かかる侵害をデータ主体に報告すべきかどうかを決定するものとする。	第4章 第2節 第33条 a. 個人データの侵害については72時間以内に監督機関に通知することが義務づけられている。 b. データ処理者は、最初にデータ違反を知った後、「不当な遅滞なく」顧客と管理者に通知するものとする。
同意	第12条：同意に基づく個人データの処理 a. 個人データは、処理の開始までに与えられたデータ主体の同意により処理できる。 b. 同意が有効であるためには、同意は自由で、情報に基づき、具体的で、明確で、かつ取消可能でなければならない。	第2章 第7条：同意の条件 a. 同意の条件が強化され、同意の要請は理解しやすくアクセスが容易な形式で提示されなければならない。 b. 同意は明確で他の事項と区別ができ、取消可能でなければならない。
開示請求権	第24条：データ主体による開示請求および確認の権利 データ管理者から以下を取得するデータ主体の権利： a. データ管理者が個人データを処理している、または処理したかどうかの確認 b. どのような個人データを処理しているか、または処理したかの概要 c. データ管理者が個人データに関して遂行する処理業務の概要	第2節 第15条：データ主体による開示請求の権利 a. データ主体がデータ管理者から、自身に関する個人データが処理されているか否か、どこでどのような目的で処理されているかについての確認を得る権利 b. 管理者は、個人データのコピーを無料で電子形式により提供するものとする。

3. European Parliament, Council of the European Union, April 2016;
The Personal Data Protection Bill 2018, Government of India, July 2018

内容	PDPB	EU GDPR
忘れられる権利	第27条：忘れられる権利 以下の開示について、データ管理者による個人データの開示継続を制限または禁止するデータ主体の権利： a. 開示が行われた目的のために使用され、必要がなくなった場合 b. 第12条に基づく同意を根拠に開示され、その後かかる同意が取り消された場合 c. PDPBまたはその他の法律の条項に反して開示された場合	第3節 第17条：消去権 a. データ管理者に対し自身の個人データを消去させ、今後のデータ配布を中止させ、第三者によるデータ処理を停止させる権利をデータ主体に与える。 b. 消去の条件は、データが当初の処理の目的に関わりがなくなること、またはデータ主体が同意を取り消すことである。
データポータビリティ	第26条：データポータビリティの権利 データ主体は、構造化され、 一般的に使用される、機械で読み取り可能な形式 により個人データを受け取る権利を有するものとする。	第3章 第3節 第20条：データポータビリティの権利 データ主体は、過去に提供した個人データを 一般的に使用される、機械で読み取り可能な形式 で受け取ることができ、それを別の管理者に送信する権利を有する。
国外での処理に係るルール	第40条：個人データの越境移転に対する制限 a. データ管理者は、個人データのコピーを少なくとも1部、インドにあるサーバーまたはデータセンターに保存する。 b. 中央政府は、インドにあるサーバーまたはデータセンターでのみ処理しなければならない重要個人情報に該当する個人データのカテゴリーを通達する。	第3条：地理的適用範囲 GDPRは、組織の所在国にかかわらず、欧州連合に所在するデータ主体の個人データを処理するすべての組織に適用される。
賠償請求の権利	第75条：賠償請求 a. データ管理者またはデータ処理者の違反により損害を受けたデータ主体は、賠償を求める権利を有する。 b. データ処理者は、以下の場合に責任を負う。 i. 処理に際してデータ管理者の指示以外のもしくは指示に反する行動を取った場合 ii. 不注意な方法で行動した場合 iii. 十分な安全予防措置を講じなかった場合 iv. 明示的に適用される条項に違反した場合	第82条：賠償請求権および賠償責任 a. 物質的または非物質的な損害を負った者は、管理者または処理者から賠償を受ける権利を有する。 b. 処理に関わる管理者は、処理により生じた損害について賠償責任を負う。処理者は、処理者に対し具体的に指示されたGDPRの責務を遵守しなかった場合、または管理者の適法な指示以外のもしくは指示に反する行動を取った場合に限り、処理により生じた損害について賠償責任を負う。

Contact us

KPMGコンサルティング株式会社

T: 03-3548-5111

E: kc@jp.kpmg.com

home.kpmg/jp/kc

KPMGインド

井上ゆかり

アソシエイト・ディレクター

M: 9971356749

E: yukariinoue@kpmg.com

home.kpmg/jp/socialmedia



本冊子は、KPMGインドが2018年に発行したIndian data protection regime – Close to reality?: Personal Data Protection Bill, 2018を翻訳したものです。翻訳と英語原文間に齟齬がある場合には、当該英語原文が優先するものとします。

ここに記載されている情報はあくまで一般的なものであり、特定の個人や組織が置かれている状況に対応するものではありません。私たちは、的確な情報をタイムリーに提供できるよう努めておりますが、情報を受け取られた時点およびそれ以降においての正確さは保証の限りではありません。何らかの行動を取られる場合は、ここにある情報のみを根拠とせず、プロフェッショナルが特定の状況を綿密に調査した上で提案する適切なアドバイスをもとにご判断ください。

© 2019 KPMG, an Indian Registered Partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

© 2019 KPMG Consulting Co., Ltd., a company established under the Japan Company Law and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. 19-1056

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

This document is for e-communication only.