インド「個人情報保護法案」と EU「一般データ保護規則（GDPR）」の比較

2021 年 8 月 13 日
One Asia Lawyers 南アジアプラクティスチーム

インドでは、個人情報の保護に関し、現行法制よりも格段に厳しい規定が盛り込まれた**「2019 年個人情報保護法案（Personal Data Protection Bill, 2019）」**の動向が注視されています。同法案は、EU 域内における個人情報保護や取扱いを定めた**「一般データ保護規則（General Data Protection Regulation、以下「GDPR」）」**をモデルにしつつ、**インド独自の規制や企業への義務を含みます**。そのため、既に他国で GDPR や類似規制を遵守した事業を行っている企業であっても、インドで個人情報を扱う場合には、インドの新法案に基づく社内体制の整備や情報取扱の運用等、一定の対応が必要となります。本ニュースレターでは、2019 年個人情報保護法案と、GDPR の相違点にフォーカスし、企業に求められる対応について解説します。

なお、2021 年 4 月 9 日付ニュースレターでは、同法案の概要や審議状況、可決された際のインパクトを解説しました。その後、同法案に関する報告書が 2021 年 7 月の雨季国会（Monsoon Session）で提出され、その内容を踏まえた法案の審議が国会で予定されていましたが、報告書の提出が再び延期され、次回 2021 年 11 月～12 月の冬季国会（Winter Session）での提出とされることが決まっています。企業にとっては対策を講じる準備期間が増えたことになりますが、現行法制よりも厳格化することは必須であると考えられるため、今後も注視が必要となります。

1 .2019 年個人情報保護法案の概要

2019 年個人情報保護法案は、個人情報を包括的に保護し，そのためのデータ保護局を設置することを目的としており、成立すれば、個人情報の取扱いを規定するインドでは初めての統一的な法律となります。

同法案の**適用対象**は、以下のとおりであり、インドで個人情報を扱う外国企業も含まれます（同法案 2）。

【2019 年個人情報保護法案の適用対象】

(a) インド国内で取得、開示、共有、またはその他の方法で処理された個人情報の処理[1]
(b) 政府（the State）、インド企業、インド国民、**インドで設立・創設（incorporated or created）された**

[1] 同法案上、「処理」は、個人情報に対し行われる操作を意味し、取得、記録、組織化、構造化、保管、変更、使用、索引付け（indexing）、送信等による開示、制限、消去等の操作を含みます。

個人または団体による個人情報の処理

(c) **インド国外のデータ管理者（data fiduciary）またはデータ処理者（data processor）**[2]による、(i)インド国内の個人（data principal、データ主体）に対する商品・サービス提供を行う組織的活動（systematic activity）または、(ii)インド国内の個人に関するプロファイリングに関連して行う、個人情報の処理

※なお、匿名化されたデータ（anonymised data）は、適用の対象外となります。

したがって、インドに拠点をもつ日系企業はもちろん、オフショアであっても、インド国内で商品・サービス提供を行う企業は、同法案の規定を遵守することが義務付けられます。

データ管理者が遵守すべき主な義務や規定は以下のとおりです。

【主な義務・規定】

- ✓ 個人情報の**取得・処理目的の制限**：本人が同意した目的、必要な範囲内で、プライバシー確保の上で処理するものとする（5 条、6 条）
- ✓ 個人情報の取得に関する**通知**：取得の際には、本人に対し、規定の情報を含む通知を行う（7 条）
- ✓ 個人情報の**保持制限・処理終了時の削除義務**：処理目的に必要な期間を超えて保持せず、処理の終了時には削除する（8 条）
- ✓ 本人の**同意取得**：個人情報の処理の開始時に本人の同意を得る（11 条）
- ✓ **未成年者の年齢確認および保護者の同意取得**：未成年者（18 歳未満）の個人情報は、処理開始前に年齢を確認し、親・保護者の同意を得る（16 条）
- ✓ **データ主体の権利行使要求への対応**：データ主体の権利に基づき、処理状況照会、削除・訂正・開示制限等を求められた場合、所定期間内に応じる（17～21 条）
- ✓ **プライバシーポリシーの策定と公開**：個人情報の管理や処理技術等、規定の内容を含むプライバシーポリシーを策定し、当局の認証を得た上で、自社および当局のウェブサイトに公開する（22 条）
- ✓ **透明性維持**：個人情報処理の透明性を維持するために必要な措置を講じ、規定の情報を公開する（23 条）
- ✓ **セキュリティ保護措置**：非識別化・暗号化の使用、誤用・不正アクセス等の防止措置、等の措置を実施する（24 条）
- ✓ **個人情報侵害の報告**：侵害の状況に応じ、当局に報告する（25 条）
- ✓ **第三者への委託契約締結**：データ処理を委託する際は契約を締結する（31 条）
- ✓ **苦情処理メカニズムの具備および「苦情処理責任者」の設置**：苦情受理から 30 日以内に解決する（32 条）

[2] 同法案上、「データ管理者」は個人情報の処理の目的および手段を決定する者、「データ処理者」はデータ管理者に代わり個人情報を処理する者を指します。

- ✓ **国外転送規制およびデータローカライゼーション**：「重要個人情報」は国外転送禁止。「機密性の高い個人情報」は一定条件下でのみ国外転送可能、ただしデータはインド国内サーバに保管する（33条、34条）

ただし、以下については**一部またはすべての規定の適用が免除**となります（同法案35～39）。

【規定が免除となる対象】

(a) **政府機関（any agency of the Government）**[3]
(b) 犯罪予防・捜査・起訴目的、個人的・家庭内使用目的、報道目的
(c) インド国外の個人（data principals not within the territory of India）の個人情報
(d) 研究・統計目的
(e) 個人情報の処理が自動化（automated）されていない小規模事業体（small entity）

一部の規定の適用が免除となる**「小規模事業体」の定義は、事業体の年間売上高や個人情報の処理量等を踏まえ、今後規則により定められる**こととされていますが、企業が負うべき義務[4]の多くが免除となります。現行の法規制では小規模事業体を免除する規定は設けられていないため、新法案の施行は、小規模事業体にとっては、一部規制の緩和となると言えます。

2.GDPRとの主な相違点

GDPRは、2016年5月に発行し、2018年5月に施行された、EU域内で取得した個人情報を保護するための統一的な規制であり、インドの新法案はGDPRをベースとしているとされています。しかしながら、インド独自の義務が規定されている点や、規制当局であるデータ保護局（Data Protection Authority of India，以下「DPA」）の裁量が大きく多くの下位規則や定義を定める権限を有する点等、GDPRと異なる点も少なからずあります。

実務上、特に重要となる規定について、インドの個人情報保護法案と、GDPRの主な相違点は以下のとおりです。

[3] 政府が関係機関の適用を免除できる規定であるため、こうした権限の付与は悪用につながる危険性があるとの指摘もあります。

[4] 法案では、個人情報取得時の本人への通知義務（7条）、保持制限および処理終了時の削除義務（9条）、プライバシーポリシー策定義務（22条）等、基本的な義務を含む18の条項が免除となるとされています。

（1） 通知義務

2019 年個人情報保護法案では、データ管理者は、個人情報を**取得する際（at the time of collection）**、または取得源が本人からではない場合には可能な限り速やかに、**本人に通知（notice）**することが義務付けられます（同法案７）。

【通知に含むべき情報】

① 個人情報を処理する目的
② 取得する個人情報の性質・分類
③ データ管理者の身元・連絡先詳細（「データ保護責任者」がいる場合はその連絡先を含む）
④ 本人同意を撤回する権利と手続
⑤ （該当する場合は）同意を取得せずに個人情報を処理する根拠等
⑥ 情報取得源（本人からの取得でない場合）
⑦ 共有される（shared）可能性のある個人または事業体（他のデータ管理者・データ処理者を含む）
⑧ 個人情報の国外移転にかかる情報
⑨ 情報保持期間、または未定の場合は保持期間決定の基準
⑩ データ主体の持つ権利と行使手続
⑪ 苦情処理の手続き
⑫ DPA への苦情申立の権利と手続
⑬ データ・トラスト・スコアの評価、等

通知の内容は、GDPR とほぼ同じ（GDPR13 条、14 条）ですが、**取得した個人情報の共有先（⑦）**を示す必要がある点は、**GDPR では規定されておらず、インドにおいては追加で求められる**こととなります。すなわち、個人情報の処理業務を外部にアウトソースする場合には、当該データ処理者の情報も事前に通知に含むといった対応が必要となります。

（2） 個人情報処理時の本人同意取得義務

個人情報の処理を開始する際（at the commencement of processing）には、必ず**本人の同意（consent）**を得る必要があり、同意を取得しない限り、処理を開始することはできません（同法案 11 条）。本人の同意は、以下の要件を満たしていないと無効とされるため、また、GDPR と同様に本人の同意を得たことを証明する責任はデータ管理者側にある（同法案 11 条(5)）ため、同意取得にかかる記録は適切に保管する運用を整える必要があります。

【個人情報の処理における本人同意取得時の要件】

① （インド契約法 14 条に基づき強制や詐欺等の影響にない）自由な（free）意思のもとの同意であること
② （同法案 7 に基づく）通知を受けていること
③ 処理目的に関し本人が同意の範囲（scope of consent）を決められるという観点で具体的（specific）であること
④ 積極的な肯定（affirmative action）により明確に示されていること
⑤ 同意をする時と同じように、同意を容易に撤回ができること

これらに加え、**「機密性の高い個人情報（Sensitive personal data）」**[5]の処理に際しては、さらに**「明示的に（explicitly）」本人同意を得る必要**があります（同 11 条(3)）。

【機密性の高い個人情報の処理における本人同意取得時の要件】

① 著しい損害を与える可能性のある処理の目的または操作であると本人に通知した後に、
② 文脈や行動からの推測ではなく、明確な言葉により（in clear terms）、
③ 目的、操作、使用について、別途同意する選択肢（choice of separately consenting to）を本人に与えた後

ただし、国家機能を遂行する目的（緊急医療対応、災害援助等）や、企業の人事労務目的（雇用、解雇、福利厚生、勤務管理、業績評価等）のために必要な場合には、本人の同意を取得せずに個人情報（機密性の高い個人情報を除く）の処理が認められています（同法案 12 条、13 条）。
また、**「合理的な目的（reasonable purposes）」がある場合にも、本人の同意なしに個人情報の処理ができる**ことがある（同法案 14 条）と規定されており、不正行為防止、内部告発、M&A、債務の回収、公開されている個人情報、検索エンジンの運営等が例示されています。さらに、この本人同意なしで個人情報を扱える**「合理的な目的」は、DPA が定義するもの**と規定されています。
GDPR においても、正当な目的があり適切な保護措置がされる場合には本人の同意なしで処理が認められるものの、その可否判断は管理者の責任とされています（GDPR6 条 4）。
インドの新法案の特徴的な点として、後述する DPA の権限の大きさが挙げられますが、この「合理的な目的」を DPA が規定する項目である点も、DPA の裁量を示していると言えます。

[5] 財務情報、健康に関する情報、公的な識別子、性生活、性的指向、生体情報、遺伝子情報、トランスジェンダーの状態、インターセックスの状態、カーストまたは部族（tribe）、宗教的・政治的な信念や所属（affiliation）、その他当局が追加規定する分類、と定義され（同法案 3 条(36)）、GDPR9 条に定める「特別な種類の個人データ（Special categories of personal data）」や日本法の「要配慮個人情報」と近い概念。

ONE ASIA LAWYERS

（3） データ管理者の分類と追加義務

インドの新法案の主要な特徴として、**「重要データ管理者（significant data fiduciary）」**、**「ソーシャルメディア仲介業者（social media intermediary）[6]」**、**「保護者データ管理者（guardian data fiduciary）」**という分類を導入しており、これに該当するデータ管理者は、**追加義務**を負う点が挙げられます。
いずれも、GDPR には存在せず、インド独自の規制です。

分類	分類の基準・方法	追加義務
重要データ管理者	(a)処理される個人情報の量、(b)処理される個人情報の機密性、(c)データ管理者の売上高、(d)データ管理者の処理による損害のリスク、(e)新技術の使用、(f)　その他、処理により弊害を引き起こす要因がある場合、等の要素を考慮した上で、**DPA が判断し、重要データ管理者として分類する**もの（同法案 26 条(1)）。	1) **DPA への登録**義務 2) **データ保護の影響評価**（data protection impact assessment）の実施と DPA への提出義務（27 条） 3) 取得・移転・消去等の重要処理やデータ保護影響評価等の最新かつ正確な**記録（records）の維持管理**義務（28 条） 4) **独立データ監査人**による**監査**を受ける義務 5) **「データ保護責任者**（data protection officer）」の設置義務
ソーシャルメディア仲介業者	ソーシャルメディア仲介業者のうち、(a)利用者数が規定の閾値以上であり、かつ(b)その活動が民主主義、国家の安全保障、公序良俗等に重大な影響を与えている・与える可能性がある場合、**連邦政府が DPA と協議の上で、「重要データ管理者」であるとの通知がなされる**もの（同法案 26 条(4)）。	1) 重要データ管理者としてのすべての義務 2) ユーザーが自らアカウントを認証できる機能の付与義務 3) 実証可能で目に見える**「認証済みバッジ**（demonstrable and visible mark of verification）」の提供義務
保護者データ管理者	(a)未成年者を対象とした商業用ウェブサイトまたはオンラインサービスを運営するデータ管理者、または(b)大量の(large volumes)未成年者の個人情報を処理するデータ管理者は、**DPA が別途定める規則で「保護者データ管理者」と分類される**もの（同法案 16 条(4)）。	1) 児童のプロファイリング、追跡（tracking）、行動監視、児童を対象としたターゲット広告、および児童に重大な損害を与える可能性のあるその他の個人情報の処理の禁止

[6] 「2 人以上のユーザー間のオンライン交流を可能にし、情報の作成、アップロード、共有、普及、修正、またはアクセスを可能にする仲介者であるが、主に以下は含まれない。(a)商業的取引、(b)インターネットへのアクセスを提供、(c)サーチエンジン、オンライン百科事典、電子メールサービス、オンラインストレージサービスなどの性質を持つもの」（同法案 26 説明）。

このように、**分類の具体的な指標や閾値が不明**であり、DPA により判断・分類されるものであるため、現時点ではデータ管理者が自身で該否を判断することが難しいものの、追加的に追う可能性のある義務については事前に把握しておくことが推奨されます。

（4） 監査の実施義務

監査は、GDPR にはないインド独自の義務であり、特徴の一つと言えます。
「重要データ管理者」に分類されると、プライバシーポリシーおよび個人情報処理の運用に関し、**毎年、独立データ監査人（independent data auditor）による監査**を受ける必要があります。
監査人は、データ管理者の法令遵守状況に関し、通知の明確性・有効性、プライバシーポリシーの有効性、セキュリティ保護措置等の項目により評価します。データ監査の評価に基づき付与される**「データ・トラスト・スコア」**は公開されるスコアとなります。
なお、データ監査人の選任方法は示されていないものの、人材自体は、関連分野における専門知識を有し、独立性や適格性を備えた者を、DPA が登録することとされています。

（5） 担当者設置義務

新法案では、現行法にも規定される**「苦情処理責任者」に加え**、GDPR の規定する概念と類似する**「データ保護責任者」**の設置が義務付けられています。

「苦情処理責任者（an officer designated for this purpose）」
データ管理者は、データ主体による苦情（grievance）の申立てを受ける「苦情処理責任者」を任命する必要があります（同法案 32）。現行法[7]においても苦情処理責任者（Grievance Officer）の設置は義務付けられており、名前と連絡先をウェブサイトで公開することとされています。新法案では、選任における具体的な要件は定められていないものの、「重要データ管理者」については、後述の「データ保護責任者」が兼務するものとされ、その場合はインドに拠点を有するものを任命する必要があります。

「データ保護責任者（Data Protection Officer）」
データ管理者のうち、「重要データ管理者」はさらに、「データ保護責任者」1 名を任命する必要があります（同法案 30）。これは、新法案で新たに導入されたものであり、GDPR（37～39 条）上の「データ保護オフィサー（Data Protection Officer）」の概念を踏襲していると見られ、職務も類似しています。

---

[7] 「2011 年情報技術（安全措置及び手続き並びに機密個人データ・情報）規則（Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules）, 2011」5 条(9)

インドの新法案においては、データ保護責任者は、本法案に関しデータ管理者を代表する者（represent the data fiduciary under this Act）であり、法令に基づく義務の遂行に関し、データ管理者への助言や監視を行うとされ、「苦情処理責任者」も兼務することとなります。
インド独自かつ厳格化された規制として、データ保護責任者は、**インドに拠点を置く（based in India）者**でなければならないと規定されています。そのため、複数国で展開している企業であっても、インド事業に関してはインド居住者をアサインしなければならず、人事配置に影響を及ぼし得る規制強化と言えます。
その他、資格・経験等の要件は規則により定められることとされています。

（6） データローカライゼーション

新法案において、個人情報の国外転送に関する扱いは、個人情報の性質・分類に応じて規定されます。

「重要個人情報（critical personal data）」[8]
重要個人情報（定義は未規定）は、**インド国内でのみ処理**することが認められ、インド国外に転送することは、緊急医療対応等の例外を除き、禁止されます（同法案 33(2)）。
重要個人情報の定義は，連邦政府が通達により別途規定するものとされています。

「機密性の高い個人情報」
機密性の高い個人情報は、**以下の条件を満たす場合にのみインド国外への転送が認められる**ものの、当該個人情報は引き続き**インド国内のサーバに保管（continue to be stored in India）**しなければなりません（同 33(1)，34(1)）。
(a) 別途同意する選択肢を本人に与える等（同 11(3)）、本人からの明示的な同意（explicit consent）を得ていること、かつ、
(b) DPA が承認した契約またはグループ内スキーム（intra-group scheme）に基づく転送、または、
(c) 連邦政府が DPA と協議の上で承認した他国やその国の事業体、または国際組織への転送、または、
(d) その他 DPA が承認した転送

なお、現行法である 2011 年機密個人情報規則においては、「機密性の高い個人情報」を他社（インド国内・国外問わず）等に移転することに関し、移転先がインド法と同等の措置（プライバシーポリシーの公開、本人同意取得、ISO27001 等の適切な安全対策）を講じていることを条件に、可能とされています（同規則 7）。新法案では、重要個人情報については国外転送が原則禁止され、機密性の高い個人情報についても、国外転送の要件をクリアしたとしてもインド国内サーバでのデータ保管が規定（いわゆるデータ

[8] 新法案で導入された、一段高い規律の対象となる個人情報の分類。ただし、重要個人情報の定義は、通達により別途規定されるため、現時点では具体的な要素は定められていません。

ローカライゼーション義務）され、規制が強化されています。
これは、国外転送の要件を満たしていない場合にのみデータローカライゼーションが求められる GDPR の規定よりも厳しいと言えます。

（7） 規制当局の権限

新法案が草案とおり施行されると、個人情報の管理や同法案の執行を担う DPA（データ保護局）が設立されます（同法案 41 条)。DPA は、個人の利益の保護、個人情報の悪用防止、法令遵守の確保等の措置を講じる機能を有する他、規定違反行為の停止・修正要求、立入検査、不正データ等の押収を行う権限を持つとされます（同法案 54 条、55 条等)。その他、多くの条項において DPA が追加の要件や定義を規定することや、下位規則を公布することを認めており、GDPR における各国の DPA が有する権限に比して、インド新法案上の DPA の権限および影響は非常に大きいと言えます。
DPA の委員長および委員は官房長官を含む上級公務員のみで構成され、政府が任命・解任権を有する（42 条）ことから、DPA の独立性についても疑問視されています。

3 .まとめ・企業に求められる対応

インドにおいては、包括的な個人情報保護法は存在せず、現行法における保護規定についても十分に遵守されていないと言われています。そのような状況から、EU 各国に一律に効力をもつ GDPR と同水準の法律が導入されるとなると、企業には負担の増加ともなり得ます。
法案可決時期が不透明ではあるものの、実務上の影響がとりわけ大きい以下に関しては、早期に対策検討を始めることで混乱を回避することが肝要となります。

プライバシーポリシーby デザインの策定（22 条）：

新法案における**「プライバシーポリシー（Privacy by design policy)」**は、GDPR における「データ保護バイデザイン・バイデフォルト（Data protection by design and by default)」に類似する概念と見られます。すなわち、事後的な措置や救済策によるプライバシー保護に優先し、**初期設定としての予防策**という位置付けとなるプライバシー保護策を策定することが求められます。現行法上も、プライバシーポリシー（privacy policy）の策定と公開が義務付けられていますが、規定される項目は、個人情報の取得・利用目的、合理的なセキュリティ対策等であり、必要最低限の内容と言えます。
一方、新法案では、以下を含むことと規定され、GDPR でのポリシー同様、予めデータ主体の権利が保護されるための仕組みを構築するという理念が根底にあると見られます。
事業において既に実装している適切な技術的対策や組織的措置は、プライバシーポリシーに落とし込む

他、個人情報を扱う業務全体のフローをレビューし、各工程でのリスク分析と対策方針を検討しておくとが肝要です。

【プライバシーポリシーに含むべき内容】

①	データ主体への危害を予測、特定、回避するために設計された、経営的・組織的・ビジネス慣行および技術的システム
②	データ管理者の義務
③	個人情報の処理に使用される技術が商業的に認められている、または認定された基準に準拠していること
④	あらゆる革新を含む企業の正当な利益が、プライバシーを損なうことなく達成されること
⑤	個人情報の取得から削除までの、処理全体におけるプライバシーの保護
⑥	透明性のある方法で個人情報を処理すること
⑦	個人情報処理の各段階においてデータ主体の利益を考慮すること

個人情報の分類：

新法案で導入されるいわゆるデータローカライゼーションの規定では、「重要個人情報」はインド国内でのみ処理することができ、「機密性の高い個人情報」は一定の要件を満たす場合にのみインド国外に転送できるが、データはインド国内に保管する必要があります。また、その他の個人情報については、特段の規制は設けられていないため、国外への転送は可能と解されます。
また、個人情報を処理する際の本人の同意取得に関しても、「機密性の高い個人情報」を処理する場合は、追加的要件が規定されます。
このように、個人情報の分類により取るべき措置が異なり、よって運用の見直しや処理システムの改変が必要となる可能性があります。しかしながら、「重要個人情報」の定義は現時点で不明確であり、また、「機密性の高い個人情報」も DPA により対象範囲が追加されることもあり得ます。そのため、まずは自社が扱う個人情報をマッピングし、整理と把握をしておくことで、今後規定される基準値や要件に応じて個人情報の再分類を容易にする対策も考えられます。
その上で、データローカライゼーション義務に備え、複数国の情報を単一の拠点やクラウド上で処理・保管している場合には、「機密性の高い個人情報」や「重要個人情報」（に相当し得る機微な情報）が含まれないことを確認する、またはインドの個人情報に関してはインド国内のサーバ上で管理し、インド国外からのアクセスを制御するなどの対策を検討する必要があります。

以上

〈注記〉
本資料に関し、以下の点ご了解ください。

- 本資料は 2021 年 8 月 13 日時点の情報に基づき作成しています。

- 今後の政府発表や解釈の明確化にともない、本資料は変更となる可能性がございます。
- 本資料の使用によって生じたいかなる損害についても当社は責任を負いません。

「One Asia Lawyers」は、日本および ASEAN 及び南アジア各国の法に関するアドバイスを、シームレスに、一つのワン・ファームとして、ワン・ストップで提供するために設立された日本で最初の ASEAN 及び南アジア法務特化型の法律事務所です。

One Asia Lawyers 南アジアプラクティスにおいては、南アジア各地の弁護士、専門家と協同しながら対応を行っております。コーポレート、労務、倒産、訴訟等、現地に根付いたサービスを提供しております。

本記事やご相談に関するご照会は以下までお願い致します。
info@oneasia.legal

＜著者紹介＞

志村 公義
One Asia Lawyers 南アジアプラクティスチーム代表
外資系法律事務所に 8 年間所属、外資系企業の日本投資案件(「インバウンド」)・コーポレート業務を中心にサポート。その後、日系一部上場企業アジア太平洋 General Counsel、医療機器メーカーのグローバル本部(シンガポール)での法務部長等、企業内法務に約 10 年間従事。2019 年より One Asia Lawyers に参画し、インド及び南アジア周辺国に滞在している。

藪本 雄登
One Asia Lawyers 南アジアプラクティスチーム
One Asia Lawyers の前身となる JBL Mekong グループを 2010 年に設立。メコン地域流域諸国を統括。カンボジア、ラオス、タイ、ミャンマー、ベトナムで 10 年間に渡る駐在・実務経験を有し、タイを中心にカンボジア、ラオス、ミャンマー、ベトナム（CLMV）の各国につき、現地弁護士と協働して各種法律調査や進出日系企業に対する各種法的なサポートを行う。インフラプロジェクトについては、タイ、カンボジア、ミャンマーにおける道路敷設や鉄道、上下水道、高速道路のメンテナンスなどの開発プロジェクト、ラオスでの電力開発案件等を支援。現地におけるプロジェクトや JV のストラクチャーや設立、建設や発電関連規制の調査、発注者やサブコントラクターとの諸所の契約支援、現地で生じる通関や付加価値税の問題等の法的なサポートを実施。

山田 薫
One Asia Lawyers 南アジアプラクティスチーム
インド事務所に所属。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。