International
Comparative
Legal Guides

Practical cross-border insights into data protection law

Data Protection 2023

10th Edition

Contributing Editors:
Tim Hickman & Dr. Detlev Gabel
White & Case LLP

ICLG.com

Expert Analysis Chapters

Q&A Chapters

Q&A Chapters Continued

India


Manisha Singh


Swati Mittal

LexOrbis

1 Relevant Legislation and Competent Authorities

1.1 What is the principal data protection legislation?

Presently, India does not have a separate data protection legislation. The Supreme Court of India, in *Justice K.S. Puttaswamy & Anr. v Union of India & Ors. ((2017) 10 SCC 1),* had recognised privacy as a fundamental right in 2017 and highlighted the need to protect online personal data from prying eyes. The Personal Data Protection (PDP) Bill was then proposed in 2019, covering mechanisms for the protection of personal data and proposed the setting up of a Data Protection Board of India and included the Right to Be Forgotten. However, the PDP Bill was later referred to the Joint Parliamentary Committee (JPC) for review to include both personal and non-personal data. The Indian Government recently unveiled a comprehensive draft of the Digital Personal Data Protection (DPDP) Bill on November 18, 2022, which will be tabled in the Monsoon Session of the Parliament in July 2023. Once the DPDP Bill is passed by the Parliament, it would effectively replace the current Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The provisions of the DPDP Bill have also been referred to while answering the questions in this chapter to ensure the reader has complete information for data protection in India.

In the absence of a distinct data protection legislation, the Information Technology Act, 2000 (IT Act) along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules) have been the cornerstone for data protection in India. To tactfully mitigate issues arising from cybercrimes along with the other challenges around data privacy in recent years, there were multiple amendments and various Rules formulated supplementing the IT Act, such as the Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021).

1.2 Is there any other general legislation that impacts data protection?

Please refer to our responses to questions 1.1 and 1.3.

1.3 Is there any sector-specific legislation that impacts data protection?

Certain ancillary and sector-specific regulations that impact data protection based on their jurisdiction and subject matter include:

- Information Technology (the Indian Computer Emergency Response Team and the Manner of Performing Functions and Duties) Rules, 2013.
- The directions imposed by the Indian Computer Emergency Response Team (CERT-In).
- The Consumer Protection Act, 2019.
- The Consumer Protection (E-Commerce) Rules, 2020.
- Rules published by regulatory authorities in India such as the Reserve Bank of India (RBI), the Insurance Regulatory and Development Authority of India, and the Securities Exchange Board of India.

1.4 What authority(ies) are responsible for data protection?

In India, relevant government departments oversee the enforcement of data protection instead of a separate Authority. However, the draft DPDP Bill envisages setting up of a Data Protection Board of India (DPBI) to regulate the entire regime of digital personal data protection in the country.

The DPBI will be entrusted with handling vast amounts of data collected, redressing grievances of Data Principals and imposing penalties on Data Fiduciaries in case of non-compliance. The DPBI will have the power to summon and enforce the attendance of persons, examine such persons under oath and inspect any data, book, document, register, books of account or any other document to conduct an inquiry for determining legislative compliance by Data Fiduciaries.

2 Definitions

2.1 Please provide the key definitions used in the relevant legislation:

- "**Personal Data**"
  According to the SPDI Rules, "Personal information" is described as "any information relating to a natural person that, directly or indirectly, when combined with other

information already available or likely to be available with a body corporate, is capable of identifying such persons".
The DPDP Bill defines "personal data" under Section 2(13) as "any data about an individual who is identifiable by or in relation to such data".

- "**Processing**"
  The term "Processing" is not defined under the IT Act or the SPDI Rules.
  The DPDP Bill, however, defines "processing" in relation to personal data under Section 2(16) as "an automated operation or set of operations performed on digital personal data, and may include operations such as collection, recording, organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, sharing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction".
- "**Controller**"
  Neither the IT Act defines Controller from the data protection aspect, nor do the SPDI Rules contain mention of a Controller. The proposed DPDP, however, mentions "Data Fiduciary", which is similar to a data controller and means "any person who alone or in conjunction with other persons determines the purpose and means of the processing of personal data". The term "person" is separately defined under Section 2(12).
- "**Processor**"
  The IT Act or the SPDI Rules do not define the term "processor". However, the DPDP Bill defines "data processor" under Section 2(7) as "any person who processes personal data on behalf of a Data Fiduciary".
- "**Data Subject**"
  The IT Act and SPDI rules do not define the term "data subject". However, the DPDP Bill defines "Data Principal" much akin to "data subject" under Section 2(5) as "the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child". A "child" means "an individual who has not completed 18 years of age".
- "**Sensitive Personal Data**"
  The SPDI Rules mention "sensitive personal data or information" (SPDI) and define it as "such personal information which consists of information relating to:
  (i) passwords;
  (ii) financial information such as Bank account, credit card, debit card or other payment instrument details;
  (iii) physical, physiological and mental health conditions;
  (iv) sexual orientation;
  (v) medical records and history;
  (vi) biometric information;
  (vii) any detail relating to the above clauses as provided to the body corporate for providing service; and
  (viii) any of the information received under the above clauses by the body corporate for processing, stored or processed under lawful contract or otherwise,
  provided that, any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005, or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these rules".
  The current proposed DPDP Bill has dropped any reference to "sensitive personal data".
- "**Data Breach**"
  The IT Act and the Rules made thereunder do not define the term "data breach". However, there is mention of "cyber security incidents" under the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties Rules, 2013, which define it as "any real or suspected adverse event in relation to cyber security that violates an explicitly or implicitly applicable security policy resulting in unauthorised access, denial of service or disruption, unauthorised use of a computer resource for processing or storage of information or changes to data, information without authorisation".
  The DPDP Bill describes a "personal data breach" as "any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data".
- **Other key definitions**
  The DPDP Bill defines a "Data Protection Officer" (DPO) as an individual appointed as such by a Significant Data Fiduciary (SDF) under the provisions of this Act.
  Further, the DPDP Bill defines "consent" as "any freely given, specific, informed, and unambiguous indication of the Data Principal's wishes by which the Data Principal, by clear affirmative action, signifies agreement to the processing of their personal data for the specified purpose".
  "Specified purpose" means "the purpose mentioned in the notice given by the Data Fiduciary to the Data Principal in accordance with the provisions of this Act".

3 Territorial Scope

3.1 Do the data protection laws apply to businesses established in other jurisdictions? If so, in what circumstances would a business established in another jurisdiction be subject to those laws?

The applicability of the IT Act and SPDI Rules on an entity incorporated outside India is not clearly defined; however, the IT Act applies "to any offence or contravention committed outside India by any person irrespective of his nationality" as long as the act constituting the offence or contravention uses a "computer" or "computer system" in India which effectively has extra-territorial operation.

The SPDI Rules cast obligations on "body corporates" that process SPDI. The definition of "body corporates" under the IT Act does not have a restrictive meaning to include only entities incorporated within India. Hence, the term is left open enough to include an extra-territorial approach in casting obligations on the said body corporates.

The DPDP Bill shall also apply to the processing of digital personal data outside the territory of India if such processing is in connection with any profiling (any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal) of or activity of offering goods or services to Data Principals within the territory of India.

As per the exemptions mentioned under Section 18 of the DPDP Bill, the provisions of Chapter 2 except sub-section (4) of Section 9, Chapter 3 and Section 17 of the Bill shall not apply where personal data of Data Principals not within the territory of India is processed under any contract entered with any person outside the territory of India by any person based in India.

4 Key Principles

4.1 What are the key principles that apply to the processing of personal data?

- **Transparency**
  Under the SPDI Rules, collecting entities must ensure that a provider of SPDI knows: the fact that SPDI is being

collected; the purpose of such collection; the intended recipients of the SPDI; and the name and address of the agency collecting and retaining SPDI. Further, before disclosing the data subject to any third party, the consent of such person must be obtained, unless the data subject has already agreed to such disclosure in the contract under which SPDI was provided, or such disclosure is necessary.
The DPDP Bill explicitly mentions under Section 6 that "on or before requesting a Data Principal for her consent, a Data Fiduciary shall give to the Data Principal an itemised notice in a clear and plain language containing a description of personal data sought to be collected by the Data Fiduciary and the purpose of the processing of such personal data".
Further, it mentions "where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemised notice in a clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for which such personal data has been processed, as soon as it is reasonably practicable".

- **Lawful basis for processing**
  As per the SPDI Rules, consent is required to be obtained for collecting and disclosing SPDI.
  Section 5 of the DPDP Bill provides the "grounds for processing digital personal data" as "a person may process the personal data of a Data Principal only in accordance with the provisions of this Act and Rules made thereunder, for a lawful purpose for which the Data Principal has given or is deemed to have given her consent in accordance with the provisions of this Act".
  Further, it defines "lawful purpose" as "any purpose which is not expressly forbidden by law".
- **Purpose limitation**
  The DPDP Bill provides certain bases which collecting entities can rely upon to process personal data. These include: consent having been given as mentioned under "deemed consent" for responding to a medical emergency; for purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance; and in the public interest and other reasonable purposes giving liberty to the Central Government, as mentioned under "Exemptions" Section 18 of the proposed bill. The DPDP Bill has limited the processing of data for lawful purposes only as explained in the principles above.
- **Data minimisation**
  The principle of data minimisation is that only those items of personal data are required for attending a specific purpose for which it was collected. Here, the SPDI Rules provide that collection of SPDI is permitted only if it is considered necessary for that purpose.
  The DPDP Bill states that personal data should be collected only to the extent that is necessary for processing such personal data which the Data Fiduciary sought to collect from the Data Principal to process such personal data and the same is clear from the language of the bill. It mentions the requirement of "notice" mandating a Data Fiduciary to give the Data Principal an itemised notice on or before requesting a Data Principal for her consent to the processing of her personal data, in a clear and plain language containing a description of personal data sought along to seek so.
- **Proportionality**
  The principle of proportionality requires that the processing of personal information must be relevant to and must not exceed the declared purpose. Please refer to our responses above for "Lawful basis for processing", "Purpose Limitation" and "Data minimisation".
- **Retention**
  The SPDI Rules stipulate that SDPI may not be retained longer than is necessary for the purposes for which it may be lawfully used or is otherwise required by any other law for the time being in force. Under the DPDP Bill, Data Fiduciaries are prohibited from retaining any personal information if a Data Principal withdraws her consent to the processing of personal data, the same must be ceased or caused to be ceased by its Data Processors within a reasonable time.
- **Accountability**
  Though there is no mention of express principle under the IT Act and SPDI Rules, the DPDP Bill is drafted to ensure that the person deciding the purpose and means of the processing of personal data should be accountable for its fair and reasonable processing. According to the DPDP Bill, any processing conducted by a Data Fiduciary on their behalf or for customers must adhere to the provisions of the DPDP Bill and every Data Fiduciary and Data Processor is obligated to protect personal data in its possession or under its control by taking reasonable security safeguards to prevent a personal data breach. In the event of such breach, there is a mandate imposed on the Data Fiduciary or Data Processor to notify the Board and every affected Data Principal (whom any personal data affected by a personal data breach relates to). There are various other general obligations of Data Fiduciaries and additional obligations to process personal data of children, with obligations of SDFs mentioned in the proposed DPDP Bill.

5 Individual Rights

5.1 What are the key rights that individuals have in relation to the processing of their personal data?

- **Right of access to data/copies of data**
  According to the SPDI Rules, the provider of SPDI can seek a review of the SPDI provided by them. Under the DPDP Bill, the Data Fiduciary is mandated to give the Data Principal the option to access such information.
- **Right to rectification of errors**
  Providers of SPDI have a right to get any errors rectified. An analogous right of rectification has been suggested along with the procedures under Section 13 of the DPDP Bill for the erasure/correction of personal data, under the applicable laws and manner as may be prescribed.
- **Right to deletion/right to be forgotten**
  The IT Act or SPDI Rules do not specifically mention this right. However, it is possible to consider the right to delete incomplete or erroneous information as a part of the right to correct or modify the SPDI.
  Under Section 9(6) of the DPDP Bill, the right to be forgotten has been advocated. It states that as soon as it is reasonable to assume that: (a) the purpose for which such personal data was collected is no longer being served by its retention; and (b) retention is no longer necessary for legal or business purposes, it is obligatory for the Data Fiduciary to cease to retain personal data or remove how the data can be associated with particular Data Principals.

- **Right to restrict or object to processing**
  The IT Act or SPDI Rules do not grant any such rights explicitly. However, the proposed DPDP Bill provides Data Principal with an option to withdraw consent to the processing of personal data, thereby causing the processing of the Data Principal's personal data to cease.
- **Right to data portability**
  The IT Act or SPDI Rules do not grant any such rights explicitly. However, a similar type of right has been proposed in the DPDP Bill. Section 9(9) provides that "the Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data only under a valid contract".
- **Right to withdraw consent or object to marketing**
  By submitting written notification in accordance with the SPDI Rules, SPDI providers can revoke the permission they previously granted to a body corporate at any moment while using their services. The body corporate has the choice in certain situations not to provide the products or services for which the information was requested. The DPDP Bill provides Data Principals with an option to withdraw consent to the processing of personal data.
- **Right protecting against solely automated decision-making and profiling**
  The IT Act or SPDI Rules do not grant any such rights explicitly. However, the DPDP Bill specifically provides that the provisions shall apply to the processing of digital personal data outside India if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India. Thus, there is an implicit right protecting against solely automated decision-making and profiling.
- **Right to complain to the relevant data protection authority(ies)**
  The "grievance officers" of the collecting organisations chosen as per the SPDI Rules are the individuals to whom SPDI providers can file complaints to regarding the processing of their data. Also, resentful parties may bring complaints to the adjudicating officials designated by the IT Act over the payment of compensation *in lieu* of failing to safeguard SPDI. It is possible to file further criminal charges for the unauthorised release of SPDI with police authorities. Affected people or companies may also report cyber security events which include unauthorised access to IT systems/data and information breaches to the CERT-In.
  Under the DPDP Bill, a Data Principal can register a grievance with a Data Fiduciary. In case the Data Principal is not satisfied with the response or does not receive a response, a complaint may be registered with the DPBI. Further, the DPDP Bill also provides that SDFs shall appoint a DPO responsible for the grievance redressal mechanism.
- **Right to nominate**
  Section 15 of the DPDP Bill suggests that a Data Principal shall have the right to nominate any other individual, who shall exercise the rights of the Data Principal in accordance with the provisions of the DPDP Bill in the event of death or incapacity, such as inability to exercise the rights of the Data Principal due to unsoundness of mind or body of the Data Principal.

5.2 Please confirm whether data subjects have the right to mandate not-for-profit organisations to seek remedies on their behalf or seek collective redress.

While the IT Act and SPDI Rules do not mention any rights, the DPDP Bill provides for a "representative application" that may be submitted by one or more Data Principals who have been harmed due to a violation by the same Data Fiduciary or data processor to seek compensation for such injury under Sections 20(3) and 22 of the DPDP Bill.

The Consumer Protection Act, 2019 defines "unfair trade practices" and allows "recognised consumer associations" to file complaints on behalf of the consumers against any unfair trade practice as defined under the Act.

6 Children's Personal Data

6.1 What additional obligations apply to the processing of children's personal data?

There are no specific provisions for children's personal data in the IT Act or SPDI Rules. However, individuals under the age of 18 are not permitted to enter into an independent contract under Indian law (specifically, the Indian Contract Act, 1872, read with the Indian Majority Act, 1875). As a result, organisations processing children's SPDI must get the children's parents' or guardians' permission.

The DPDP Bill specifies additional obligations for the processing of personal data of children under Section 10. It requires the Data Fiduciary to take parental consent (including legal guardians) before processing the personal data of the child. Further, it restricts the processing of any data that is likely to cause harm to a child or undertake tracking or behavioural monitoring of children or targeted advertising directed at children.

7 Registration Formalities and Prior Approval

7.1 Is there a legal obligation on businesses to register with or notify the data protection authority (or any other governmental body) in respect of its processing activities?

The IT Act and its implementing rules do not contain such a requirement. Even the DPDP Bill only provides that the Central Government may notify any Data Fiduciary or class of Data Fiduciaries as SDFs based on an assessment of relevant factors, including: the volume and sensitivity of personal data processed; risk of harm to the Data Principal; potential impact on the sovereignty and integrity of India; risk to electoral democracy; the security of the State; public order; and such other factors as it may consider necessary. Further, it provides that the SDF is to appoint a DPO to represent the SDF that is based in India. The DPO will serve as the point of contact for the grievance redressal mechanism. An Independent Data Auditor is also to be appointed, who shall evaluate the compliance of the SDF with the DPDP Bill. The SDF is to also perform periodic audits and undertake a Data Protection Impact Assessment. Such SDF may be required to register with the DPBI in the prescribed manner. All responses from questions 7.2 to 7.12 are answered accordingly.

7.2 If such registration/notification is needed, must it be specific (e.g., listing all processing activities, categories of data, etc.) or can it be general (e.g., providing a broad description of the relevant processing activities)?

The IT Act and its implementing rules do not contain such a requirement. There are no specific guidelines for this aspect as the DPDP Bill has not come into force and the supplementing rules are not yet published. However, the DPDP Bill, under Section 11(1), does mention a Data Fiduciary or class of Data Fiduciaries that may be notified by the Central Government based on an assessment of relevant factors that they are an SDF. These assessment factors are as follows:

(a) the volume and sensitivity of personal data processed;
(b) risk of harm to the Data Principal;
(c) potential impact on the sovereignty and integrity of India;
(d) risk to electoral democracy;
(e) security of the State;
(f) public order; and
(g) such other factors as it may consider necessary.

Furthermore, under Section 20(3), the DPBI may in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach (which may have provided an unwarranted broad description) or mitigate any harm caused to Data Principals.

7.3 On what basis are registrations/notifications made (e.g., per legal entity, per processing purpose, per data category, per system or database)?

See question 7.2.

7.4 Who must register with/notify the data protection authority (e.g., local legal entities, foreign legal entities subject to the relevant data protection legislation, representative or branch offices of foreign legal entities subject to the relevant data protection legislation)?

See questions 7.1 and 7.2.

7.5 What information must be included in the registration/notification (e.g., details of the notifying entity, affected categories of individuals, affected categories of personal data, processing purposes)?

The IT Act and its implementing rules do not contain such a requirement. There are no specific guidelines for this aspect as the DPDP Bill has not come into force and the supplementing rules are not yet published.

7.6 What are the sanctions for failure to register/notify where required?

The DPDP Bill proposes a penalty for non-fulfilment of obligations of the SDF under Section 11, stipulated to be a maximum of INR 150 Crores (Approx. 18,209,518 USD).

7.7 What is the fee per registration/notification (if applicable)?

See question 7.5.

7.8 How frequently must registrations/notifications be renewed (if applicable)?

See question 7.5.

7.9 Is any prior approval required from the data protection regulator?

See question 7.5.

7.10 Can the registration/notification be completed online?

See question 7.5.

7.11 Is there a publicly available list of completed registrations/notifications?

See question 7.5.

7.12 How long does a typical registration/notification process take?

See question 7.5.

8 Appointment of a Data Protection Officer

8.1 Is the appointment of a Data Protection Officer mandatory or optional? If the appointment of a Data Protection Officer is only mandatory in some circumstances, please identify those circumstances.

The appointment of a DPO is not included in the present data protection legislation. The SPDI Rules include the creation of a grievance officer to address the complaints of the SPDI provider over the prompt processing of her SPDI.

According to the proposed DPDP Bill, an SDF is mandated to designate a DPO, and other Data Fiduciaries are to designate a DPO or a person who can answer the Data Principal's questions about the processing of personal data on behalf of the Data Fiduciary.

8.2 What are the sanctions for failing to appoint a Data Protection Officer where required?

The absence of a grievance officer is not specifically punished or sanctioned under the present IT Act and SPDI Rules. If a data provider experiences a "wrongful loss" because of a party's negligence in following acceptable security practices and procedures, such party may be subject to a claim for compensation under the IT Act.

Under the proposed DPDP Bill, if an SDF fails to appoint a DPO, it may face a penalty of up to INR 150 Crores (Approx. 18,209,518 USD) for non-fulfilment of additional obligations imposed on the SDF under Section 11. If another Data Fiduciary fails to appoint a person to be answerable on behalf of the Data Fiduciary, then they may be subject to a penalty of up to INR 50 Crores (Approx. 606,984 USD) for non-compliance with the DPDP Bill.

8.3 Is the Data Protection Officer protected from disciplinary measures, or other employment consequences, in respect of his or her role as a Data Protection Officer?

Both the present legislation and the DPDP Bill do not mention any such specific exemptions.

8.4 Can a business appoint a single Data Protection Officer to cover multiple entities?

There are no limitations on the appointment of a single grievance officer/DPO to cover several entities under either the present legal system or the DPDP Bill.

8.5 Please describe any specific qualifications for the Data Protection Officer required by law.

There are no requirements for the grievance officer specified under the IT Act or SPDI Rules. The appointment of a DPO by the SDF is a mandate by the DPDP Bill, and such DPO must be based in India. There is no provision explicitly stating the qualification required for the appointment of such DPO, and a legal notification is awaited in this regard. Some common qualifications that may be released by the appropriate authority for the appointment of such DPO may include the requirements of expertise in legal, IT security, data compliance or audit; knowledge of data protection laws such as the GDPR and other similar national laws, computer security system knowledge; experience in operational application of Privacy law; relevant working experience of monitoring compliance with regulatory requirements and engaging with regulatory bodies. Such mentioned specific qualifications might be required by law for better appointments in the future.

8.6 What are the responsibilities of the Data Protection Officer as required by law or best practice?

Under the IT Act and SPDI Rules, the grievance officer must swiftly and within a 30-day window resolve complaints from SPDI providers.

According to the DPDP Bill, the DPO has a variety of responsibilities, including to:

a) represent the SDF;
b) answer to the Board of Directors or similar governing body of the SDF;
c) serve as a point of contact for the grievance redressal mechanism;
d) undertake measures including a Data Protection Impact Assessment;
e) undertake periodic audits concerning the objectives laid down in the Act; and
f) monitor processing activities, advise on the creation of internal systems to support Data Principals' rights and maintain a list of the records that SDFs must keep.

8.7 Must the appointment of a Data Protection Officer be registered/notified to the relevant data protection authority(ies)?

Neither the present law nor the proposed bill has such an express requirement. However, the DPDP Bill does require the business contact details of the DPO to be published in such manner as may be prescribed.

8.8 Must the Data Protection Officer be named in a public-facing privacy notice or equivalent document?

The identity regarding the name and contact information of the grievance officer is required to be made public under the SPDI Rules. The DPDP Bill imposes similar requirements for providing the business contact details of a DPO.

9 Appointment of Processors

9.1 If a business appoints a processor to process personal data on its behalf, must the business enter into any form of agreement with that processor?

The IT Act 2000 does not specifically state that a processor needs to enter into any form of agreement. However, it is standard operating procedure for commercial organisations to enter into a Data Processing Agreement (DPA) with a Data Processor. The DPDP Bill mandates a valid enforceable contract between a Data Processor and a Data Fiduciary.

9.2 If it is necessary to enter into an agreement, what are the formalities of that agreement (e.g., in writing, signed, etc.) and what issues must it address (e.g., only processing personal data in accordance with relevant instructions, keeping personal data secure, etc.)?

DPAs are not legally obligated at present. There are no specifications for this as the DPDP Bill has not come into force and the supplementing rules are not yet published.

10 Marketing

10.1 Please describe any legislative restrictions on the sending of electronic direct marketing (e.g., for marketing by email or SMS, is there a requirement to obtain prior opt-in consent of the recipient?).

The IT Act does not cover electronic marketing; although the IT Rules 2021 impose an obligation on significant social media intermediaries to make information identifiable to its users as being advertised, marketed, sponsored, owned or exclusively controlled. The IT Act and Rules do not explicitly restrict electronic direct marketing. However, organisations must provide an "opt-out" option in email marketing. Further, the organisation's privacy policy must address marketing and information collection practices.

The Telecom Commercial Communication Customer Preference Regulations, 2018 (TCCPR) set out by the Telecom Regulatory Authority of India (TRAI) provide regulations regarding marketing. Individuals can register their numbers on a do-not-call registry. The TCCCPR are only applicable to telecommunications including text messages and phone calls, but not e-mails.

In June 2022, the Central Consumer Protection Authority (CCPA) issued Guidelines on Prevention of Misleading Advertisements and Endorsements for Misleading Advertisements, 2022 (the Guidelines). The Guidelines lay down the conditions for non-misleading and valid advertisements, and conditions for bait advertisements. The Guidelines prohibit surrogate advertising and lay down conditions for advertisements targeted at children.

10.2 Are these restrictions only applicable to business-to-consumer marketing, or do they also apply in a business-to-business context?

There is no distinction between business-to-consumer or business-to-business.

10.3 Please describe any legislative restrictions on the sending of marketing via other means (e.g., for marketing by telephone, a national opt-out register must be checked in advance; for marketing by post, there are no consent or opt-out requirements, etc.).

See question 10.1.

10.4 Do the restrictions noted above apply to marketing sent from other jurisdictions?

The TCCCPR govern transactions between Indian telecommunications and reserve the right to frame additional rules for mass foreign marketing. However, there have been no rules framed by the regulator yet.

10.5 Is/are the relevant data protection authority(ies) active in enforcement of breaches of marketing restrictions?

The TRAI in 2021 (while not a data protection body) penalised many senders and telemarketers for failing to comply with the TCCPR. The TRAI also issued a list of defaulting senders and telemarketers on its website. It was also said that the system would reject any commercial communication that did not match the parameters.

In addition, in response to reports of fraudulent banking alerts and calls, the Department of Telecommunications issued a circular in 2021 announcing the setting up of a "Digital Intelligence Unit" platform, the "Telecom Analytics for Fraud Management and Consumer Protection", the "Safe Access of Telecom Resources without Harassment and Infringement (SATHI) system" to detect sceptical telecommunications interactions and illicit activities, and an "Information Sharing Platform". This is expected to lead to a more successful application of this framework in the future.

10.6 Is it lawful to purchase marketing lists from third parties? If so, are there any best practice recommendations on using such lists?

The legality of the purchase of marketing lists from third parties is still ambiguous; yet, such practices are rather frequent. To limit risk and exposure, it is best to get proper guarantees and representations from third parties that offer such lists, saying that the information included in such lists was gathered with the agreement of the individuals affected.

10.7 What are the maximum penalties for sending marketing communications in breach of applicable restrictions?

The TCCPR provides tier-wise financial disincentives, and depending on the gravity of the violation may also impose a usage cap and/or disconnection of telecom services. For violation of the CCPA, a penalty of up to INR 0.1 Crores (approx. 12,192 USD) can be imposed on manufacturers, advertisers and endorsers for any misleading advertisements. For subsequent contraventions, the CCPA may impose a penalty of up to INR 0.5 Crores (approx. 60,796 USD). The Authority can prohibit the endorser of a misleading advertisement from making any endorsement for up to one year and for subsequent contravention, prohibition can extend up to three years.

11 Cookies

11.1 Please describe any legislative restrictions on the use of cookies (or similar technologies).

The IT Act and the supplementing rules do not provide any legislative restrictions on the use of cookies explicitly. However, under the SPDI Rules, the processing of SPDI requires written consent which also applies to cookies used for the collection of SPDI. There are no exceptions to this obligation. Since the SPDI Rules allow denial of services if consent is withheld for the collection of data, it is often used by organisations to restrict access to their websites or platforms if users do not give consent for using necessary cookies.

Under Section 43 of the IT Act, permission from the data owner is required to download, copy or extract any data or information from the computer, which squarely applies to cookies as well. However, there are no specific guidelines or judicial precedents for the same.

Once the DPDP Bill is brought into force, the guidelines for the use of cookies may likely be issued. In any case, organisations are to seek clear, unambiguous and explicit consent for the use of cookies.

11.2 Do the applicable restrictions (if any) distinguish between different types of cookies? If so, what are the relevant factors?

There is no such distinction between different types of cookies.

11.3 To date, has/have the relevant data protection authority(ies) taken any enforcement action in relation to cookies?

None, since there is no specific provision in the IT Act or Rules.

11.4 What are the maximum penalties for breaches of applicable cookie restrictions?

See question 11.3.

12 Restrictions on International Data Transfers

12.1 Please describe any restrictions on the transfer of personal data to other jurisdictions.

The SDPI Rules require consent to be taken from data owners before transferring their SPDI. However, there is no specific provision for cross-border transfer. The RBI has issued guidelines for outsourcing financial services that mandate companies to ensure data safety while outsourcing. There may be sectoral restrictions placed on the transfer of data.

Section 17 of the DPDP Bill provides that the Central Government may, after an assessment of such factors as it may consider

necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer Personal Data as per terms and conditions that may be specified.

12.2 Please describe the mechanisms businesses typically utilise to transfer personal data abroad in compliance with applicable transfer restrictions (e.g., consent of the data subject, performance of a contract with the data subject, approved contractual clauses, compliance with legal obligations, etc.).

Organisations generally use explicit permission forms for data collection to promote the free flow of data and accelerate the rise of the data economy and global economic order. Organisations utilise numerous pop-up windows asking for authorisation before activating cookies on specific websites or subscribing to the terms and conditions of a platform on the internet to acquire agreement from users.

12.3 Do transfers of personal data to other jurisdictions require registration/notification or prior approval from the relevant data protection authority(ies)? Please describe which types of transfers require approval or notification, what those steps involve, and how long they typically take.

See question 12.1.

12.4 What guidance (if any) has/have the data protection authority(ies) issued following the decision of the Court of Justice of the EU in Schrems II (Case C-311/18)?

There is no data protection authority in India presently, so there are no specific guidelines.

12.5 What guidance (if any) has/have the data protection authority(ies) issued in relation to the European Commission's revised Standard Contractual Clauses published on 4 June 2021?

See question 12.4.

13 Whistle-blower Hotlines

13.1 What is the permitted scope of corporate whistle-blower hotlines (e.g., restrictions on the types of issues that may be reported, the persons who may submit a report, the persons whom a report may concern, etc.)?

The Whistleblowers Protection Act, 2014, relates to a vigil mechanism for the security of an individual reporting unethical, immoral and illegal acts such as malpractice and fraud in public-sector organisations. A complainant can be any person who makes a complaint relating to disclosure under the Act. Under the Act, any complaint by a whistleblower must be submitted to the Competent Authority as defined under the Act. The Competent Authority differs with persons against whom any complaint is being made. However, the Competent Authority under the Act is usually the senior official in the same hierarchy as the person against whom a complaint is being made. This negates the neutrality of the investigation and the findings reached are usually biased.

The legal framework concerning the whistleblower or vigil mechanisms is also governed by: the provisions of The Companies Act, 2013; the Companies (Meeting of Board and its Powers) Rules, 2014; and the Securities and Exchanges Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015.

13.2 Is anonymous reporting prohibited, strongly discouraged, or generally permitted? If it is prohibited or discouraged, how do businesses typically address this issue?

According to the Whistleblower Protection Act, an authorised body can only act on an allegation if the whistleblower reveals their identity in the claim. Whistleblowers that provide counterfeit aliases or make complaints anonymously are not acknowledged. Nonetheless, there is no bar in the Companies Act regarding confidential disclosure of company activity.

The Audit Committee or the Board of Directors may independently evaluate the substance of the unidentified accusation and take appropriate action, or they may seek to contact the whistleblower for additional material and assistance. Leading business organisations in India accept complaints anonymously and have put in place procedures to protect whistleblowers' identities and the secrecy of the investigation procedure.

14 CCTV

14.1 Does the use of CCTV require separate registration/notification or prior approval from the relevant data protection authority(ies), and/or any specific form of public notice (e.g., a high-visibility sign)?

The IT Act, SPDI Rules and DPDP Bill can be invoked for the use of CCTV for surveillance. However, there are no provisions or regulatory requirements for the same. The IT Act provides that if a camera captures or transmits photos of a person's private parts, male or female, without consent, the criminal can be charged under Section 66E. This, nevertheless, has several exemptions. For example, the use of CCTV cameras at public locations without the approval of individuals is permitted, if the cameras are not pointed at locations where individuals are entitled to a reasonable right of privacy, such as restrooms or changing facilities. Furthermore, CCTV cameras may be used to preserve the welfare and protection of individuals and possessions, as well as to hinder, identify and investigate crime. In such circumstances, the video footage gathered can be shared with law enforcement agencies as required by the law.

14.2 Are there limits on the purposes for which CCTV data may be used?

See question 14.1.

15 Employee Monitoring

15.1 What types of employee monitoring are permitted (if any), and in what circumstances?

There are no specific provisions for employee monitoring under the legislature. However, the IT Act and the Telegraph Act, 1885, permit the "interception, inspection or deciphering of any data transferred, obtained or retained on an organisation's device". This is particularly relevant if the monitoring has a genuine and reasonable business objective and does not infringe on the personnel's personal space and privacy. Most

organisations collect employee data for background verification or standard business purposes such as payroll and insurance.

15.2 Is consent or notice required? Describe how employers typically obtain consent or provide notice.

All employers that collect and process the personal data of their employees are to follow the obligations under the SPDI Rules that require written consent to be taken from the data subject. The proposed DPDP Bill also requires consent to be taken from the Data Principal for the collection and processing of personal data. Through judicial precedents, it is established that monitoring, especially audio monitoring, must be done only after obtaining such consent.

15.3 To what extent do works councils/trade unions/employee representatives need to be notified or consulted?

There are no specific provisions under present legislation or the proposed DPDP Bill.

15.4 Are employers entitled to process information on an employee's COVID-19 vaccination status?

Yes, an organisation may require its employees to provide documentation of vaccination. Any relevant vaccination-related data will be classified as "sensitive personal data or information" under the SPDI Rules and any employer that collects, stores or processes this data will be obligated to comply with all applicable data protection obligations.

16 Data Security and Data Breach

16.1 Is there a general obligation to ensure the security of personal data? If so, which entities are responsible for ensuring that data are kept secure (e.g., controllers, processors, etc.)?

The SPDI Rules mandate data protection obligations on every organisation dealing with SPDI to implement and maintain acceptable security practices and procedures. It includes measures that govern Personal Data/Information processing and/or SPDI processing and security practices and procedures for handling Personal Data/Information and/or SPDI.

The proposed DPDP Bill requires every Data Fiduciary and Data Processor to protect personal data in its possession or under its control by taking reasonable security safeguards to prevent personal data breaches.

16.2 Is there a legal requirement to report data breaches to the relevant data protection authority(ies)? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

The IT Act and Rules do not provide any mandatory requirement to report data breaches.

On April 28, 2022, the Indian Government issued a new directive regarding Cybersecurity Incident Reporting that will force organisations across India to report cyber incidents, infosec and data breaches to CERT-In within a mere six-hour deadline of "noticing such incidents". CERT-In has issued a list of cyber incidents (PDF) that all service providers, intermediaries, data centre operators, companies and government organisations must report within CERT-In's designated six-hour window. This tightened cybersecurity guidance follows the introduction of new rules and regulations by CERT-In. Additionally, the entities and organisations covered by the rules must securely maintain IT and communications logs of all ICT systems for six months (180 days). The new directive has been integrated into Section 70B of the IT Act relating to information security practices, procedures, prevention, response and reporting of cyber incidents for Safe & Trusted Internet.

The proposed DPDP Bill requires the Data Fiduciary to inform the DPBI of all data breaches. The Data Fiduciary is to convey the same to affected Data Principals. Further, it provides that the DPBI may accept a voluntary undertaking in respect of any matter related to compliance at any stage.

16.3 Is there a legal requirement to report data breaches to affected data subjects? If so, describe what details must be reported, to whom, and within what timeframe. If no legal requirement exists, describe under what circumstances the relevant data protection authority(ies) expect(s) voluntary breach reporting.

See question 16.2.

16.4 What are the maximum penalties for data security breaches?

When personal information is disclosed in violation of a legitimate contract or without authorisation, Section 72-A of the IT Act provides for a fine of up to INR 0.05 Crores (approx. 6,070 USD) or imprisonment for three years, or both. The proposed DPDP Bill provides that a financial penalty not exceeding INR 500 Crores (approx. 60,698,320 USD) can be imposed for non-compliance related to a data breach.

For failing to disclose information to the CERT-In or comply with CERT-In's directives, a body corporate or its officers risk imprisonment for up to one year, a fine of INR 0.01 Crores (approx. 1,214 USD), or both.

17 Enforcement and Sanctions

17.1 Describe the enforcement powers of the data protection authority(ies).

(a) **Investigative Powers:** At present, only police officers holding the rank of inspector or higher can investigate under the IT Act. However, the proposed DPDP Bill provides that the DPBI may conduct inquiries after being satisfied that there are sufficient grounds to proceed with an inquiry on receipt of a complaint.

(b) **Corrective Powers:** Claims for compensation of less than INR 5 Crores (Approx. 606,983 USD) filed under Section 43A of the IT Act are decided by an adjudicating officer designated by the Central Government. Claims over the aforesaid amount are adjudicated by competent courts according to Section 46 of the IT Act.

(c) **Authorisation and Advisory Powers:** There is no official state regulator in India for data protection and privacy. The Ministry of Electronics and Information Technology (MeitY) enforces the provisions of the IT Act and Rules.

(d) **Imposition of administrative fines for infringements of specified GDPR provisions:** Infringement of the IT Act and Rules may result in the following consequences:
- Compensation to an impacted person for a body corporate's failure to develop and maintain "reasonable security practices and procedures" to secure SPDI or personal information.
- Damages are not limited and can vary from instance to case.
- Imprisonment for up to three years or a fine of INR 0.05 Crores (Approx. 6,070 USD), or both, for releasing personal information in violation of a legitimate contract or without the consent of the data subject.
- For failing to disclose information to the CERT-In or comply with CERT-In's directives, a body corporate or its officers risk imprisonment for no more than one year, a fine of INR 0.01 Crores (Approx. 1,214 USD), or both.

The proposed DPDP Bill provides that a financial penalty not exceeding INR 500 Crores (Approx. 60,698,320 USD) can be imposed for non-compliance.

(e) **Non-compliance with a data protection authority:** See question 17.1 (d) above.

17.2 Does the data protection authority have the power to issue a ban on a particular processing activity? If so, does such a ban require a court order?

Section 69A of the IT Act, read along with the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 (the "Blocking Rules") provides for certain powers of the Central Government to issue orders to any relevant authority to block access by the public to certain sensitive information that pertains to the Sovereignty, integrity, defence and security of the state. The same also finds its basis in the Official Secrets Act, 1923, and the Right to Information Act, 2005.

17.3 Describe the data protection authority's approach to exercising those powers, with examples of recent cases.

The aforesaid provisions described in question 17.2 authorise the Central Government or an authorised officer to issue a reasoned order directing any government agency or intermediary to block online content in the interest of the sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognisable offence relating to above. Under Section 69A(3) of the IT Act, intermediaries are bound to comply with blocking directions or face criminal sanctions.

The last two years have witnessed a sudden surge in the number of YouTube videos and Mobile applications such as TikTok being blocked. Parliamentary questions reveal that 78 YouTube news channels and 560 YouTube URLs were blocked in 2021 and 2022. Additionally, 2021 mobile apps were blocked in 2022. The MeitY recently issued orders to block 138 online betting platforms and 94 money lending apps on an "urgent" and "emergency" basis under Section 69(A) of the IT Act.

17.4 Does the data protection authority ever exercise its powers against businesses established in other jurisdictions? If so, how is this enforced?

According to Section 75 of the IT Act, the jurisdiction of the legislation is expanded to foreign jurisdictions subject to the provisions of subsection (2) stating that the offence or the act under investigation must involve a computer, computer system and computer network located in India. The ban on mobile applications that may have been from foreign jurisdictions is an example of the exercise of powers against businesses established in other jurisdictions.

The enforcement is done through the concerned government agency or intermediary. On receiving a blocking request, the Designated Officer as per the IT Act and Blocking Rules is required to make "all reasonable efforts" to identify the person or the intermediary who has hosted the impugned information online, issue a notice to them to appear before the Committee and present their case opposing the proposed blocking. Thus, under Rule 8(1), prior notice to the originator of content or the intermediary is a necessity. The Committee must then examine the blocking request to determine whether it falls within the parameters of Section 69A(1) of the IT Act. The Designated Officer then sends the Committee's recommendations to the Secretary of the Department of Information Technology, who takes the final decision regarding blocking. Upon approval, the Designated Officer directs the concerned government agency or intermediary to block the offending content. Rule 9 deals with blocking content in cases of an emergency, in which case no prior notice is required to be given to the originator of the content. However, such an action must be confirmed within 48 hours.

18 E-discovery / Disclosure to Foreign Law Enforcement Agencies

18.1 How do businesses typically respond to foreign e-discovery requests, or requests for disclosure from foreign law enforcement agencies?

India ratified the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (the "Hague Convention") in 2007. However, no domestic law has been passed by the Parliament of India to give effect to the Hague Convention. The closest provisions in Indian law that allow requests for disclosure or e-discovery in the form of "letters of request issued by foreign courts" are under Section 78 and Order 26, Rules 19 to 22 of the Code of Civil Procedure (CPC). Section 78 read with Rule 19 of Order 26 of the CPC provides for conditions that are required to be satisfied for the execution of letters of request from foreign courts:
- a foreign court should wish to obtain evidence of a witness in any proceeding of civil nature before it; and
- the witness should be residing within the appellate jurisdiction of the High Court before which the request is placed.

After India ratified the Hague Convention, the High Courts of Andhra Pradesh and Delhi entertained the letters of request presented to them and appointed commissioners for the execution of the letters of requests under Order 26 of the CPC, dehors the application of the Hague Convention.

The Indian Government has, in response to a questionnaire relating to the Hague Convention (published in May 2009), taken the position that the domestic implementation of the convention in India would be through Section 78 and Order 26, Rules 19 to 22 of the CPC. Thus, Indian entities are not legally obligated to comply with any requests for e-discovery unless a specific request has been made in that regard as per law.

18.2 What guidance has/have the data protection authority(ies) issued?

As India does not have a specific data protection authority, there have been no guidelines that were issued specifically for this subject.

19 Trends and Developments

19.1 What enforcement trends have emerged during the previous 12 months? Describe any relevant case law or recent enforcement actions.

Forty-seven incidents of data leaks and 142 incidents of data breaches have been reported during the last five calendar years as per the MeitY response to a question raised in Parliamentary proceedings.

Recently, the servers of the All-India Institute of Medical Sciences (AIIMS) were ravaged by a ransomware attack, which affected over 40 million records and encrypted the data, due to which the servers went offline for about two weeks. Following the ransomware assault at the AIIMS in November 2022, the Indian Government formed the National Counter Ransomware Taskforce to avoid such attacks in the future.

Refer to the response to question 17.3 above for recent examples of enforcement actions.

19.2 What "hot topics" are currently a focus for the data protection regulator?

Currently, India does not have a Data Protection Regulator. However, if the DPBI is established as a part of the DPDP Bill, certain areas will attract concerns and require focus:

- Greater emphasis on privacy by design i.e., proactively embedding privacy into the design and operation of IT systems, networked infrastructure and business practices.
- Service providers may move to privacy-focused technology such as secure messaging apps and browsers; virtual private networks and encrypted email services.
- Alternatives to cookies will invoke newer technologies and methods to track and target users. For example, using browser fingerprints that can be used to track a user without using cookies.
- Edge computing that allows data processing near the source of data rather than in a centralised data centre.
- Artificial Intelligence-enabled cyber security.
- Data Automation.
- Synthetic data generation that does not contain any data from real persons, but still has the statistical features that are characteristic of real-life data.
- Confidential computing using hardware-based trusted execution environments such as processors that guarantee certain security features for the memory or parts of the memory.

Manisha Singh is the founder and managing partner of LexOrbis. She oversees and supervises all practice groups at the firm. Manisha is known and respected for her expertise in the prosecution and enforcement of all forms of IP rights and for strategising and managing the global patents, trademarks and designs portfolios of large multinationals and domestic companies. She is also known for her sharp litigation and negotiation skills for both IP and non-IP litigations and dispute resolution. She has represented companies in many IP litigations with a focus on patent litigation covering all technical fields, but particularly pharmaceuticals, telecommunications and mechanics.

LexOrbis
709/710, Tolstoy House, 15–17, Tolstoy Marg
New Delhi – 110 001
India

Tel: +91 11 2371 6565
Email: manisha@lexorbis.com
URL: www.lexorbis.com

Swati Mittal is an attorney-at-law and holds an LL.M in IP & Technology Law, an M. Tech in Biotechnology and a PG Diploma in Patents Laws in India, the US & EP. She has diverse knowledge and expertise of handling patents, designs, trademarks, copyrights and other civil and commercial litigations. She regularly appears in litigation, revocation and opposition cases before the Delhi High Court, Bombay High Court, Calcutta High Court, Supreme Court of India, District courts of Delhi and other judicial forums and tribunals. She has a thorough understanding of the IP, Technology and Privacy Laws and has been involved in strategising commercial disputes relating to infringement of IP Rights pertaining to patents, trademarks, designs, copyrights and passing off.

LexOrbis
709/710, Tolstoy House, 15–17, Tolstoy Marg
New Delhi – 110 001
India

Tel: +91 11 2371 6565
Email: swati.mittal@lexorbis.com
URL: www.lexorbis.com

LexOrbis is a premier full-service IP law firm with over 260 personnel including 150+ attorneys at its four Indian offices in New Delhi, Bengaluru, Mumbai and Chennai. The firm provides client-oriented and cost-effective solutions for the protection, enforcement, transaction and commercialisation of all forms of IP in India and globally. The firm has been consistently ranked amongst the Top 5 IP firms in India over the past decade and is well-known for managing global patent, designs and trademark portfolios of many technology companies and brand owners. The firm has dedicated teams to cater to the IP lifecycle including attorneys, engineers, scientists and specialists to deal with patent, trademark and copyright filing, research, portfolio building and management, enforcement, protection, spotting, transacting, procurement and consultation.

The trademark practice group at the firm has over 30 attorneys experienced in partnering with brand owners and advising on the entire IP lifecycle from selection to enforcement. The firm's patent practice group has over 100 patent attorneys with domain expertise in information and communication technologies, computer sciences and software including Artificial Intelligence/Machine Learning, Internet of Things, blockchain, big data, mechanical, electrical & electronics, chemical and pharmaceutical, biotechnology, energy management, etc.

www.lexorbis.com

LexOrbis INTELLECTUAL PROPERTY ATTORNEYS

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Environmental, Social & Governance Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Technology Sourcing
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

The International Comparative Legal Guides are published by: global legal group