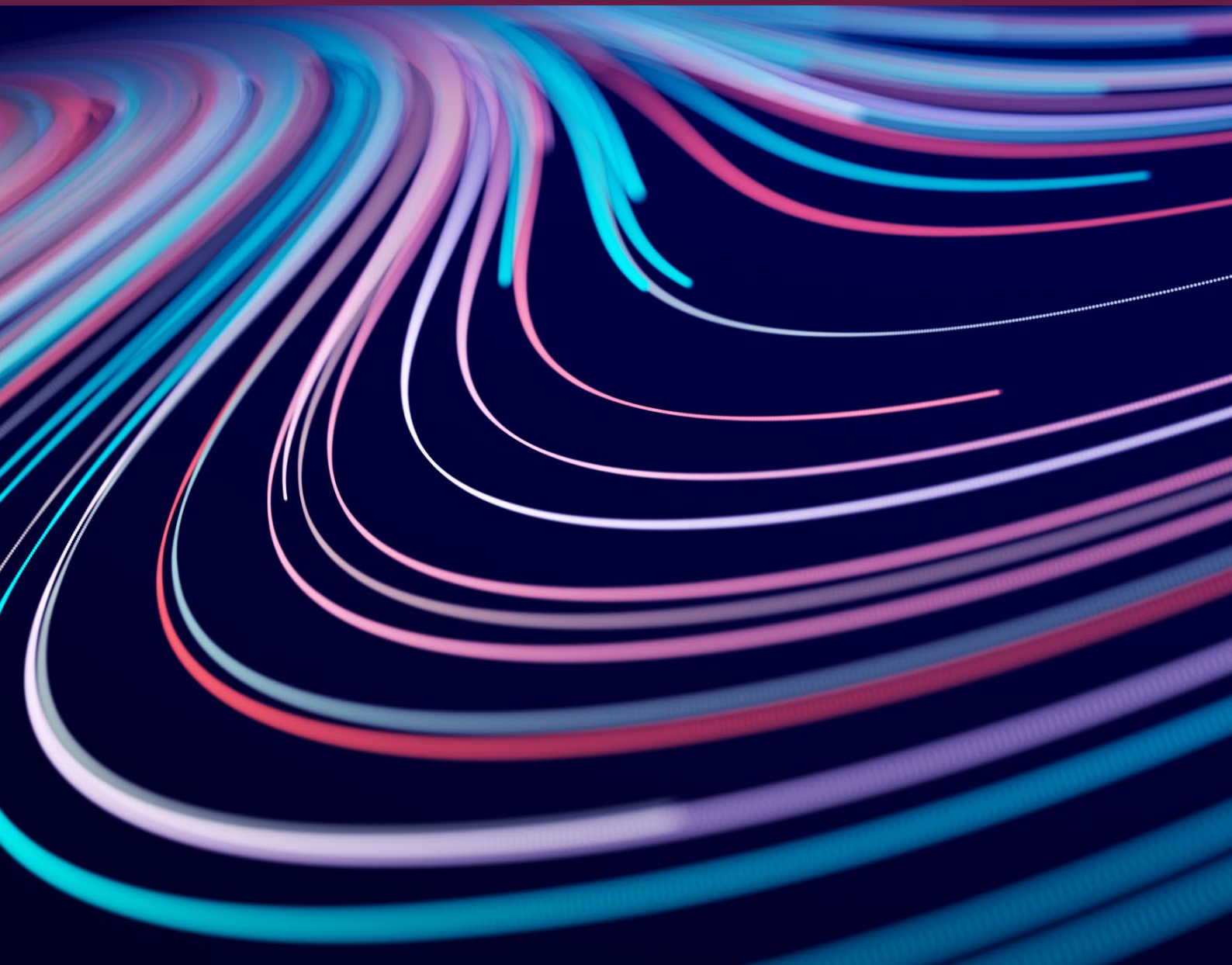
LATHAM&WATKINS

India's Digital Personal Data Protection Act 2023 vs. the GDPR: A Comparison

Organisations doing business in India should note the differences between GDPR and DPDPA requirements, including potential programmes that may need uplift to ensure compliance.

April 2026



The Parliament of India enacted the country's first comprehensive data protection law, the Digital Personal Data Protection Act 2023 (the DPDPA), on 11 August 2023. The DPDPA replaces India's existing patchwork of data protection rules[1] and triggers significant changes in how companies subject to Indian data protection laws process personal data. The DPDPA is an "umbrella" legislation, as it sets out only a high-level framework for India's new data protection regime.

The Digital Personal Data Protection Rules 2025 (the DPDP Rules) — published by the Indian government on 13 November 2025 — provide interpretative guidance on procedural steps and enforcement methodology. While the DPDP Rules aim to finalise the compliance and enforcement framework, any subsequent gaps that have not been addressed in the DPDPA and the DPDP Rules will be clarified by the Ministry of Electronics and Information Technology (MEITY) through a comprehensive set of FAQs, rather than amendments or modifications to the DPDPA or the operational framework.

The procedural provisions of the DPDPA, including the establishment of the Data Protection Board of India (the regulatory authority responsible for supervising compliance and enforcing the DPDPA and the DPDP Rules), entered into force on 13 November 2025. The substantive provisions of the DPDPA and the DPDP Rules, which impose compliance obligations on data fiduciaries and consent managers and establish rights for data principals, will be brought into force in a phased approach over the next 12 to 18 months (i.e., by 12 May 2027).

The DPDPA is triggered when digital personal data is processed within India. The law also has an extraterritorial effect in that it applies to digital personal data processing outside of India if such processing relates to the offering of goods or services to individuals (known as "data principals", which are equivalent to "data subjects" under the EU and UK General Data Protection Regulations (the GDPR)) within India. The DPDPA follows broadly similar principles to those set out in the GDPR and specifies rules for data fiduciaries (equivalent to "controllers" under the GDPR) and data processors, as well as rights for data principals. Penalties for non-compliance under the DPDPA range from INR 500 million to INR 2.5 billion (approximately €4.7 million to €23.5 million). The Data Protection Board is also empowered to impose urgent remedial or mitigation measures in the event of a personal data breach.

As the DPDPA will become fully enforceable on 12 May 2027, enforcement risk remains low in the interim period. Organisations that are located in India or that process personal data of or provide goods and services to individuals in India (i.e., controllers, processors, and consent managers) should use this period to develop transition plans. Specifically, such organisations should align their current data privacy programmes with key requirements under the DPDPA (such as adherence to the duties of controllers, consent processes, and rights of data principals) in order to minimise future compliance risks.

Practical Impact on Existing Privacy Compliance Programmes

The DPDPA signals a major change in the way personal data is processed in India. Organisations operating in or targeting individuals in India should review current privacy compliance programmes against the new framework under the DPDPA and the DPDP Rules and consider steps to bring their privacy compliance in line with the DPDPA. Key elements of the DPDA include:

- **Scope:** The DPDPA regulates the processing of digital personal data, i.e., personal data collected in digital form or collected in non-digital form and subsequently digitised. Whilst the DPDPA's personal data definition is similar to that provided under the GDPR, it excludes from its scope personal data made publicly available by the data principal or by any other person under a legal obligation to make that data publicly available.

- **Legal basis for the processing of personal data:** The DPDPA provides that data fiduciaries may lawfully process personal data only with the consent of the data principals or for certain specified "legitimate uses". Such legitimate uses include: the processing of personal data voluntarily shared by the data principal for a specified purpose (provided that the data principal does not object to such processing); processing to comply with the law or court orders; processing for employment purposes; or processing to respond to medical emergencies, epidemics, or disasters. The DPDPA's consent standard is similar to that of the GDPR, requiring consent to be "free, specific, informed, unconditional and unambiguous with a clear affirmative action".

In contrast to the GDPR, the DPDPA does not recognise the contractual necessity or legitimate interests bases for data processing. Therefore, data fiduciaries processing personal data on the basis of contractual necessity or legitimate interest under the GDPR must identify an alternative legal basis for such processing under the DPDPA, by way of data mapping and periodic audits. If the processing of personal data does not fall under any of the legitimate uses enumerated in the DPDPA, data fiduciaries must obtain consent from the data principal prior to processing their personal data. Organisations should consider implementing layered consent mechanisms, such as separate consent mechanisms for essential and non-essential purposes of processing (and organisations could potentially deny or limit provision of services if a data principal does not consent to data processing that is essential for those services).

- **Data principal rights:** Whilst data principals will have certain rights similar to those under the GDPR for data subjects (i.e., rights of access, correction, and erasure), they will also benefit from a number of new rights which are unique to the DPDPA. These include the right to a readily available and effective means of grievance redressal (e.g., via a grievance redressal officer) and the right to nominate an individual who will be able to exercise the rights of the data principal in the event of death or incapacity of the data principal.

- **Cross-border data transfers:** The DPDPA permits cross-border data transfers to jurisdictions outside of India other than those jurisdictions specifically identified by the Indian government on its list of countries to which data transfers are restricted (to be published). The DPDP Rules specify that such cross-border transfers must meet the conditions set by the government through a general or special order, as may be notified from time to time. No orders to this effect have been passed by the government as of yet.

- **Data breach notification:** Data fiduciaries are required to notify the newly created Data Protection Board and to impacted data principals of personal data breaches involving the compromise of personal data, *regardless* of the magnitude of the data breach or risk of harm. Further, the DPDP Rules prescribe that a breach should be reported to the affected data principals and the Data Protection Board without delay. Additionally, a detailed report of the breach should be submitted to the Data Protection Board within 72 hours of becoming aware of a personal data breach. Currently, there is no interpretative guidance on breach reporting thresholds under the DPDPA; organisations should continue to monitor for further guidance on the Data Protection Board's expectations in practice, including on the feasibility of a risk-based approach to breach reporting.

- **Significant data fiduciaries:** The Indian government will have the power to classify certain data fiduciaries as significant data fiduciaries based on factors such as the sensitivity and volume of data processed; the impact of processing on the rights of data principals; and the impact on the sovereignty, security, and integrity of India. These significant data fiduciaries will have additional obligations, including the appointment of an independent auditor and undertaking yearly data protection impact assessments and audits.

The table below compares the requirements of the GDPR and the DPDPA in further detail, highlighting potential gaps in GDPR-based compliance programmes and outlining possible steps to uplift such programmes for DPDPA compliance purposes. As additional rules to supplement the DPDPA provisions are issued, organisations may need to adjust their compliance approaches accordingly.

The table is colour-coded as below for ease of reference:

Minimal difference: The DPDPA is materially consistent with the GDPR — **no further action required to comply with the DPDPA**

No-action gaps: The DPDPA is generally consistent with the GDPR, but with noticeable differences / the GDPR standard is higher or more comprehensive — **additional compliance actions will not be required to comply with the DPDPA**

Manageable gaps: The DPDPA is generally consistent with the GDPR, but with noticeable differences — **minor additional compliance actions are required to comply with the DPDPA**

Material gaps: The DPDPA is materially different from the GDPR / there are elements under one law that are not found under the other — **significant additional compliance actions are required to comply with the DPDPA**

The DPDPA vs. the GDPR

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Scope of application							
1.	**Personal data**	✓	Any information relating to an identified or identifiable natural person.	✓	Any data about an individual, who is identifiable by, or in relation to, such data. The DPDPA applies only to "digital personal data", which means personal data collected in digital form and personal data collected or stored in a non-digital form that is subsequently digitised. Personal data that is made publicly available by the data principals or pursuant to a legal requirement is out of scope.	**No-action gaps:** The DPDPA applies only to "digital personal data", whereas the GDPR applies to personal data even if that data is non-digital. In addition, personal data that is made publicly available is exempt from DPDPA obligations.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
2.	**Sensitive / special category personal data**	✓	Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.	✗	The DPDPA does not differentiate between personal data and sensitive / special category personal data.	**No-action gaps:** No additional compliance obligations will need to be taken to comply with the DPDPA. GDPR-compliant controllers are likely to meet the requirements under the DPDPA, as a higher degree of protection is offered to "special categories of personal data" under the GDPR.	N/A
3.	**Data subjects**	✓	The identified or identifiable natural person to whom personal data relates.	✓	Data principal (i.e., data subject): The individual to whom the personal data relates. If such individual is a child, the concept includes the parent / lawful guardian of such child. If such individual is a person with a disability, the concept includes the lawful guardian acting on behalf of such an individual.	**Minimal difference**	N/A
4.	**Data controller**	✓	The natural or legal person, public authority, agency, or other body that, alone or jointly with	✓	Data fiduciary (i.e., data controller): Any person/entity who, alone or in conjunction with other persons,	**Minimal difference**	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			others, determines the purposes and means of processing personal data.		determines the purpose and means of processing an individual's personal data.		
5.	**Significant data fiduciary (SDF)**	✗	There is no equivalent concept under the GDPR.	✓	A data fiduciary or class of data fiduciaries designated by the Indian government based on: (i) volume and sensitivity of personal data processed; (ii) risk to the rights of the data principal; (iii) potential impact on the sovereignty and integrity of India; (iv) risk to electoral democracy; (v) security of the State; and (vi) public order. The criteria for who qualifies as a SDF has yet to be defined.	**Material gaps:** The DPDPA identifies a class of data fiduciaries as SDFs based on certain parameters and applies additional obligations to those SDFs. There is no equivalent concept under the GDPR.	If classified as an SDF by the Indian government, additional compliance obligations will apply, such as: • appointing an Indian-resident data protection officer (DPO) who reports to the board of directors; • conducting audits and data protection impact assessments (DPIAs) every 12 months; • deploying risk mitigation measures; • restricting cross-border transfers of certain categories of personal data and related traffic data (categories to be notified and designated by the Indian government) outside India (i.e., a de facto localisation requirement); and • verifying that algorithmic software deployed for processing personal data is

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
							unlikely to pose a risk to the data principal.
6.	**Data processor**	✓	A natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller.	✓	A person who processes personal data on behalf of the data fiduciary.	**Minimal difference**	N/A
7.	**Consent manager**	✗	There is no equivalent concept under the GDPR.	✓	Consent managers act independently of the data fiduciary and are distinct from a local representative or DPO. Entities incorporated in India and registered with the Data Protection Board that provide accessible, transparent, and interoperable platforms through which data principals can review, provide, manage, and withdraw consent for the processing of their personal data. Consent managers are engaged by data fiduciaries to manage consents on behalf of data principals. If multiple consent managers integrate with data fiduciaries, this would	**Material gaps:** There is no equivalent concept under the GDPR.	Organisations applying to be registered as a consent manager must: • be incorporated in India and meet certain capacity, financial, and governance standards;[3] • implement policies to ensure adherence to consent manager obligations; • carry out its operations in the interests of data principals; • maintain independent certification stating that it has implemented (i) an interoperable platform enabling data principals to manage and review their consent; and (ii) appropriate technical and organisational measures in

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
					theoretically provide data principals an option to elect a consent manager of their choice.		place to ensure its platform adheres to relevant standards to be published by the Data Protection Board.
8.	**Processing**	✓	Any operation or set of operations that is performed on personal data or on sets of personal data, whether by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, restriction, erasure, or destruction.	✓	A wholly or partly automated operation or set of operations performed on digital personal data. Includes operations such as collection, recording, organisation, structuring, storage, adaptation, retrieval, use, alignment, combination, indexing, sharing, disclosure by transmission, dissemination, or otherwise making available, restriction, erasure, or destruction.	**Minimal difference**	N/A
9.	**Processing children's data**	✓	The GDPR contains provisions to enhance the protection of children's personal data: • if transparency information is intended to be read by a child, it should be in clear and plain	✓	When processing a child's personal data (person under the age of 18) or that of a person with a disability, "verifiable consent" of the parent or the lawful guardian of such child/person must be obtained.	**Material gaps:** The DPDPA prescribes additional obligations with respect to processing children's data, specifically the requirement to obtain "verifiable consent" of the parent or legal guardian of the child. The relevant age of the child varies under the GDPR / EU Member State law /	Data fiduciaries must not undertake data processing that is detrimental to children or facilitates targeted advertising directed at children. Data fiduciaries must implement verifiable parental consent measures to process children's data, which go beyond

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			language that children can easily comprehend; and • if an information society service is offered to a child, consent should be obtained from a parent/guardian, subject to certain age criteria. The age of majority is not defined under the GDPR, and it varies across EU Member States. However, certain provisions are applicable to children under the age of 16.		With respect to children's personal data, the data fiduciary must not: • undertake processing of personal data that is likely to cause any detrimental effect to the well-being of a child; or • track or engage in behavioural monitoring of children or use targeted advertising directed at children. The DPDP Rules set out certain situation-specific exemptions to the general obligation to obtain verifiable consent, which predominantly exempt healthcare and educational institutions processing children's personal data in a verifiably safe manner. The Indian government may extend the scope of the exemption from the requirement of obtaining verifiable consent under the DPDPA to specific classes of data fiduciaries, which are yet to be notified.	UK law (i.e., 16 years or under) and the DPDPA (18 years).	traditional age gating requirements. Under the DPDPA and DPDP Rules, verifiable consent requires the data fiduciary to: • obtain consent of the parent or lawful guardian of the child; • confirm that the individual identifying as the parent or lawful guardian is an identifiable adult by reference to reliable identify and age details, e.g., government-issued identity documentation (either held by the data fiduciary, voluntarily provided by the individual, or mapped to a virtual token issued by an authorised entity); and • verify the parent/guardian-child relationship, e.g., by the parent/guardian providing the child's passport or PAN Card. In the interim before the DPDPA becomes fully effective on 12 May 2027, companies may continue relying on the following parental consent methods as they begin to transition towards verifiable parental consent:

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
							credit card verification, email verification, and SMS verification.
Transparency							
10.	**Privacy policy disclosures**	✓	Data subjects must be informed of the following at the time of collection of personal data: • name and contact details of the data controller and local representative (if applicable); • contact details of the DPO; • purposes of processing; • lawful basis for processing and legitimate interests for processing (if applicable); • categories of personal data obtained;	✓	A notice must be provided to data principals for obtaining their personal data either at the time of or before seeking consent to data processing. The notice must be in clear and plain language, distinct from other information made available to the data principal, and include: • categories of personal data being collected; • specified purpose of processing, and specific description of the goods or services to be provided / functions to be enabled by such processing; • the mechanisms through which data principals may withdraw their consent and exercise their rights under the DPDPA with	**No-action gaps:** The GDPR provides a more detailed set of requirements regarding notice. Generally, the DPDPA makes it easier for GDPR-compliant controllers to process personal data with notice for consent.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			• recipients of personal data; • details of transfers of personal data to any third countries or international organisations; • retention periods for personal data; • data subject rights; • right to withdraw consent (if applicable); • right to lodge a complaint with a supervisory authority; • source of personal data (if personal data is not obtained from the individual it relates to); • details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is		respect to the personal data; and • the mechanisms through which data principals may make a complaint to the Data Protection Board.		

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			collected from the individual it relates to); and • the details of the existence of automated decision-making, including profiling (if applicable).				
11.	**Language requirements**	✓	Information provided to data subjects must be in clear and plain language (including the native language of the data subject, when required).	✓	Data principals must be provided with an option to access the contents of a consent request in English or in any of the 22 languages specified in the Eighth Schedule of the Constitution of India.	**Manageable gaps:** Both the GDPR and the DPDPA require information provided to data subjects to be in a language they understand.	Whilst the language requirements under the GDPR and the DPDPA are broadly similar, given the potential for a large number of languages (i.e., 22 languages specified in the Indian Constitution), the practical implications of providing many language options could be significant.
Legal basis of processing							
12.	**Consent**	✓	*Consent* Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which they, by a statement or clear affirmative action, signifies agreement to the processing of	✓	Consent given by the data principal must be: • duress-free; • specific; • informed; • unconditional; • unambiguous;	**Minimal difference**	The DPDPA and the DPDP Rules prescribe that prior to obtaining consent, the data principal should be provided with a notice containing the following: • categories of personal data being collected; • specified purpose of processing and description

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			personal data relating to them. *Explicit consent* Undefined, but must be affirmed in a clear statement and needs to refer to the element of the processing that requires explicit consent.		• with a clear affirmative action signifying an agreement to the processing of personal data for the specified purpose; and presented in clear and plain language with the option to accept such requests as per the Language Requirements (see #11).		of the goods or services to be provided / functions to be enabled by such processing; • the mechanisms through which a data principal can (i) withdraw their consent; (ii) exercise their rights under the DPDPA; and (iii) make a complaint to the Data Protection Board; and • contact details of a DPO (if applicable) or any person who can answer questions on behalf of the controller. Consent for each specific purpose of processing can be obtained through ticking a check-box after providing the information set out above to the data principal. Data fiduciaries could provide a single check-box for obtaining consent for the essential/core purpose of any service (without which the service could not be provided) and have separate, purpose-specific check-boxes for secondary/optional purposes of processing.

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
13.	**Contract**	✓	Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.	✗	Processing personal data for the performance of a contract is not recognised as a "legal basis for processing" under the DPDPA, which refers to legitimate uses. These uses include compliance with laws, ensuring the safety of a person, performance of statutory duties/functions, and employment purposes. Certain obligations of the data fiduciary under the DPDPA will not apply if the data subjects are not within the territory of India and their personal data is processed pursuant to a contract entered into with any person outside the territory of India, by any person in India.	**Material gaps:** Processing personal data for the performance of a contract is not a legal basis under the DPDPA. Unless an exemption is granted by the subordinate rules that are yet to be framed, this exclusion differs significantly from the GDPR.	Determine when personal data is processed according to a contract and ensure that steps are taken to comply with a DPDPA statutorily recognised legal basis for processing (i.e., legitimate use or consent). In practice, data fiduciaries that rely on contractual necessity for existing processing — i.e., processing that is essential/ core to the provision of the service to the data principal — could consider relying on consent for such processing. For example, data fiduciaries could require data principals to affirmatively provide their consent to the privacy policy (which details all essential processing), such as by ticking a check-box which states "I consent to the privacy policy" or "I acknowledge the privacy policy". In the event of withdrawal of consent, the data fiduciary is required to cease processing of personal data within a reasonable period of time and may discontinue or limit services to the data principal if such essential consents are withdrawn.

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
14.	**Legal obligation**	✓	Processing is necessary for compliance with a legal obligation to which the controller is subject.	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if the data is required to comply with any judgment, decree, or order issued under Indian law, or any contractual or civil claim-related judgment or order under any law in force outside India.	**Minimal difference**	N/A
15.	**Public health emergency / vital interests**	✓	Processing is necessary to protect the vital interests of the data subject or of another natural person.	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if the data is required for responding to a medical emergency involving a threat to life or an immediate threat to the health of the data principal or any other individual.	**Minimal difference**	N/A
16.	**Medical treatment or health services in an epidemic**	✓	Processing is necessary in order to protect the vital interests of the data subject or of another natural person; or	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if the data is required to provide medical treatment or health services to an individual during an	**No-action gaps:** The DPDPA specifically provides that consent is not required to process personal data to provide medical treatment or health services to individuals during an epidemic. There is no exact equivalent under the GDPR, but the closest legal basis would be for an	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.		epidemic, outbreak of disease, or threat to public health.	individual's vital interests or for public interest purposes.	
17.	**Public interest**	✓	Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if such processing is required to ensure the safety of individuals or provide assistance or services to any person during a disaster or breakdown of public order.	**Minimal difference**	N/A
18.	**Voluntary disclosure**	✗	The GDPR does not have a specific legal basis for voluntary disclosure.	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if the data principal provides their personal data voluntarily to the data fiduciary for a specified purpose and does not object to the processing of such personal data.	**No-action gaps:** The GDPR does not have an equivalent legal basis for processing. However, as this is an additional legal basis (and does not preclude any other GDPR legal basis), no additional compliance steps are needed.	Data fiduciaries can rely on a data principal's voluntary disclosure of personal data if the data principal (i) voluntarily provides their personal data for the specified purposes of the processing, and (ii) does not object or indicate absence of consent. Examples include individuals sharing their phone number or email address in order to receive an electronic receipt of a purchase, or providing their contact and vehicle details to register for an

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
							extended warranty programme for their car. If the data principal subsequently objects to the processing or revokes/ withdraws their consent, or if the specific purpose of the processing comes to an end (e.g., the service being provided to the data principal is completed/terminated/expires), the data fiduciary must cease such processing of personal data.
19.	**Legitimate interests**	✓	Processing is necessary for the purposes of legitimate interests pursued by the controller or by a third party, except when such interests are overridden by the interests or fundamental rights and freedoms of the data subject that requires protection of personal data, in particular if the data subject is a child.	✗	The DPDPA does not have a legitimate interest legal basis (the only available legal bases are "consent" or the "legitimate uses" set out in #14, #15, #16, #17, #18, and #20).	**Material gaps:** The DPDPA does not recognise the equivalent exemption for legitimate interests for processing without consent.	Determine when the personal data processing is conducted under legitimate interest and ensure that steps are taken to process personal data according to an available legal basis for processing personal data under the DPDPA (i.e., legitimate use or consent). In practice, data fiduciaries that rely on legitimate interests for existing processing could consider relying on consent for such processing (if the processing does not constitute a legitimate use under the DPDPA). Data fiduciaries could provide (i) a single check-box for obtaining

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
							consent for any processing that is essential/core for the provision of the service, as set out in the privacy policy (e.g., "I consent to the privacy policy" or "I acknowledge the privacy policy"), and (ii) separate, purpose-specific check-boxes for secondary/optional purposes of processing (e.g., marketing, analytics).
20.	**Employment**	✗	The GDPR does not have a specific legal basis for processing personal data in an employment context (except for special categories of personal data). Instead, potential legal bases that could be relevant for processing non-special category data in an employment context include processing for the performance of a contract, necessity to comply with a legal obligation, or legitimate interests.	✓	Under the DPDPA, a data fiduciary or an SDF is permitted to process personal data without a data principal's explicit consent if the data is needed for employment or related to safeguarding the employer from loss or liability such as of corporate espionage, to maintain confidentiality of trade secrets, intellectual property, classified information, or provision of any service or benefit sought by a data principal who is an employee.	**No-action gaps:** The GDPR does not have the equivalent "employment" legal basis for processing.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Data processing agreements							
21.	**Data processing agreements**	✓	Processors must process personal data in accordance with a contract that requires that the processor: • processes personal data in accordance with agreed purpose(s); • returns or destroys personal data upon termination; • obtains consent prior to contracting with sub-processors; • implements necessary measures to ensure the security of personal data; • submits to audits and inspections; • provides assistance to the controller to fulfil obligations under the GDPR; and • notifies the data controller as soon	✓	The DPDPA requires that if a data fiduciary is to employ a data processor for undertaking any processing activity on its behalf, then such engagement should be through a valid contractual relationship with the data processor. Data fiduciaries are required to ensure that the engaged data processors: • comply with the DPDPA and rules thereunder; • cease processing of and erase personal data once consent is withdrawn; and • take reasonable security safeguards to prevent data breach. According to the DPDP Rules, such reasonable security safeguards include: (a) data security measures such as encryption, masking, or tokenisation;	**Minimal difference**	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			as reasonably possible upon discovering a security breach.		(b) access control measures and access logs (retained for one year); and (c) periodic data backups.		
International data transfers							
22.	**Adequacy decision**	✓	Transfers of personal data from the European Economic Area (the EEA) to white-listed countries[4] subject to an adequacy decision by the European Commission do not have to comply with additional safeguard requirements under the GDPR.	✗	Currently, the DPDPA provides only for the government's ability to provide a list of countries where data transfers are restricted.	**Manageable gaps:** Subject to additional guidance in the form of rules from the Indian central government, the DPDPA does not provide for an adequacy decision.	Do not transfer data to restricted countries (specific restricted countries to be notified by the government).
23.	**Transfer mechanism**	✓	To transfer personal data from the EEA or the UK to a non-white-listed jurisdiction, the controller must: • implement an appropriate transfer mechanism (e.g., standard contractual clauses adopted by the European	✗	The DPDPA allows for transfers of personal data to all countries, unless that country is included on the Indian government's list of countries to which data transfers are restricted. The DPDP Rules specify that such cross-border transfers must meet the conditions specified by the government through a general or special	**Material gaps:** The DPDPA does not provide for specific transfer mechanisms; cross-border transfers must meet conditions to be further specified by the government (through a general or special order).	Do not transfer data to restricted countries (specific restricted countries to be notified by government). Additionally, SDFs may be subject to data localisation requirements in relation to specific categories of personal data and related traffic data (if and when such localisation requirements are notified by the government).

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			Commission or the UK equivalent); • carry out a transfer impact assessment (a TIA); and • depending on the TIA outcome, implement supplementary measures (e.g., encryption of data in transit and at rest).		order, as may be notified from time to time. No orders to this effect have been passed by the Indian government as yet.		
Privacy by design / documentary requirements							
24.	**Inventory / record of processing (ROP)**	✓	The following should be recorded in a ROP: • the name and contact details of the controller, and, if applicable, the joint controller, the controller's representative, and the DPO; • the purposes of the processing; • a description of the categories of data subjects and	✗	Not provided for in the DPDPA.	**No-action gaps:** Not provided for in the DPDPA.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			of the categories of personal data; • the categories of recipients to whom the personal data have been or will be disclosed, including recipients in third countries or international organisations; • if applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation, and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards; • if possible, the envisaged time				

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			limits for the erasure of the different categories of data; and • if possible, a general description of the technical and organisational security measures.				
25.	**Data protection impact assessment (DPIA)**	✓	A DPIA should be conducted when a type of processing (particularly using new technologies, and taking into account the nature, scope, context, and purposes of the processing) is likely to result in a high risk to the rights and freedoms of natural persons.	✓	SDFs are required to conduct annual DPIAs to ensure effective compliance with the DPDPA and manage the risk to data principals' rights.	**Manageable gaps:** The DPDPA only requires SDFs (and not all data fiduciaries) to undertake periodic DPIAs.	SDFs must ensure that the person carrying out the DPIA and the independent audit furnishes a report with significant observations to the Data Protection Board.

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Governance							
26.	**Data protection officer (DPO)**	✓	A controller or processor must appoint a DPO if: • the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; • the core activities of the controller or the processor consist of processing operations that, by virtue of their nature, their scope, and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or • the core activities of the controller or the processor consist of processing data on a large scale, of special categories of data, or personal data relating to criminal convictions and offences.	✓	All data fiduciaries are required to appoint either a DPO or a person able to answer data principals' questions on behalf of the data fiduciary. Data fiduciaries are required to publish the business contact information of such DPOs/appointed persons prominently on their website or app and in every communication with a data principal exercising their DPDPA rights. SDFs have an additional obligation to ensure that the appointed DPO is based in India and is responsible to the board of directors or similar governing body of the organisation and would act as the point of contact for the grievance redressal mechanism under the DPDPA.	**Manageable gaps:** Both the GDPR and the DPDPA require the appointment of a DPO if certain conditions apply; however, SDFs have an additional obligation under the DPDPA to ensure that its appointed DPO is based in India.	If the data fiduciary is classified as an SDF, appoint a DPO based in India who reports to the board of the SDF. Non-SDF data fiduciaries must appoint either a DPO or a person able to respond to questions from data principals on data processing matters. In practice, data fiduciaries with existing DPO functions (whether within or outside India) are likely to fulfil this requirement (provided the DPOs are readily accessible to data principals in India).

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
27.	**Representative**	✓	A controller or processor must appoint a local representative if the controller or processor is not established in the EEA.	✓	All SDFs are required to appoint a representative who is based in India, though a DPO can fulfil this role (see #26 for relevant DPO requirements).	**No-action gaps:** SDFs are required to appoint a local representative based in India, but a DPO based in India can fulfil both roles.	N/A
Data subject rights							
28.	**Right to be informed**	✓	Data subjects have the right to be informed about how and why their data is used (see "Privacy Policy Disclosures" in #10).	✓	The data fiduciary or consent manager (as applicable) must publish on its website and/or app the following information: • the means through which the data principal can exercise their rights; • any form of identification that the data fiduciary / consent manager may require from the data principal to verify their identity when exercising their DPDPA rights; and • its typical "grievance resolution period" under its grievance redressal process (not more than 90 days (see #37). Upon the data principal's request, a data fiduciary or consent manager (as applicable) would need to provide details regarding:	**No-action gap:** The obligations under the GDPR and DPDPA are similar. However, the disclosures provided under the DPDPA need to be made according to and upon the request of the data principal; while under the GDPR, specific information must be disclosed before the collection of personal data or within a specific timeframe in case of indirect data collection. When the data fiduciary relies on consent as its legal basis, relevant transparency information must be provided to the data principal before the collection of their personal data (see #12 for further information on consent as a legal basis).	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
					• the personal data that is being processed; • the processing activities being undertaken; and • the identities of all other data fiduciaries with whom the personal data has been shared, along with the description of the personal data shared.		
29.	**Right of access**	✓	Data subjects have the right to request a copy of their personal data from the controller, as well as other relevant information (subject to certain exceptions).	✓	See #28.	**Minimal difference**	N/A
30.	**Right to rectification**	✓	If personal data is inaccurate or incomplete, data subjects have the right to have their data corrected or completed by the controller, without undue delay (subject to certain exceptions).	✓	Upon receiving a request for the correction, completion, or updating personal data from the data principal, the controller must: • correct the inaccurate or misleading personal data; • complete the inaccurate personal data; and • update the personal data.	**Minimal difference**	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
31.	**Right to erasure**	✓	Data subjects have the right to request that the controller delete their personal data without undue delay (subject to certain exceptions).	✓	Upon receipt of an erasure request, the data fiduciary shall erase the personal data unless retention of the same is necessary for the specified purpose or for compliance with any law for the time being in force.	**Minimal difference**	N/A
32.	**Right to object to and restrict processing**	✓	Data subjects have the right to object to, or request that the controller restricts, processing in certain circumstances.	✗	The DPDPA does not provide specific instances in which data principals may object to, or restrict, the processing of personal data. Data principals have the right to withdraw their consent, which then requires data fiduciaries and processors to cease processing of such personal data (see #35).	**No-action gaps:** Not provided for in the DPDPA.	N/A
33.	**Right to data portability**	✓	Data subjects have the right to request that their personal data be transmitted to another controller (subject to certain exceptions).	✗	The DPDPA does not provide the right to data portability.	**No-action gaps:** Not provided for in the DPDPA.	N/A
34.	**Right not to be subject to automated decision-making**	✓	Data subjects have the right not to be subject to a decision based solely on automated processing (i.e., processing carried out without human intervention that has a legal or similarly	✗	The DPDPA does not provide the right to not be subject to automated decision-making.	**No-action gaps:** Not provided for in the DPDPA.	N/A

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			significant effect on the data subject).				
35.	**Right to withdraw consent**	✓	Data subjects have the right to withdraw their consent to the processing, if such consent is relied on as the legal basis for processing (it must be as easy to withdraw as to give consent).	✓	When consent is the basis for processing personal data, the data principal may withdraw consent at any time, with the ease of doing so being comparable to the ease with which such consent was given. As a result, the data fiduciary must cease processing the personal data.	**Minimal difference**	N/A
36.	**Right to lodge a complaint with the regulator**	✓	Data subjects have a right to lodge a complaint with the relevant data protection authority.	✓	The data principal must exhaust the opportunity for grievance redressal (provided in #37) before approaching the Data Protection Board.	**Manageable gaps:** The right to approach the Data Protection Board is subject to the data principal first approaching the data fiduciary's grievance redressal mechanism.	Ensure that a grievance redressal mechanism is implemented to resolve grievances internally and avoid a situation wherein the data principal invokes their right to approach the Data Protection Board.
37.	**Right to grievance redressal**	✗	There is no specific right to grievance redressal under the GDPR, but if a data subject makes a complaint about a controller, the controller is obliged to attempt to address the data subject's grievances.	✓	Data fiduciaries must provide a readily available and effective means of grievance redressal to data principals and resolve such grievances within 90 days from the date of receipt of the grievance.	**Manageable gaps:** Under the DPDPA, data fiduciaries will need to have in place a grievance redressal mechanism and redress grievances as per the guidelines issued thereunder.	Data fiduciaries should implement a mechanism through which data principals can submit grievances relating to the processing of their personal data or their individual rights under the DPDPA. Data fiduciaries must respond to grievances within a reasonable period of time, not exceeding 90 days from the date of receipt of the

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
							grievance (and must publish on their website and/or app the resolution period (see #28)).
38.	**Right to nominate**	✗	There is no specific "right to nominate" under the GDPR, but data subjects can authorise another person to make data subject requests on their behalf. Controllers must be satisfied that the person making the request is doing so on behalf of the data subject and can request supporting evidence (e.g., a power of attorney).	✓	Data fiduciaries must enable data principals to nominate any other individual who can exercise rights in relation to the data principal's personal data in the event of their death or incapacity.	**Manageable gaps:** There is no specific "right to nominate" under the GDPR. The GDPR applies only to living individuals; there is no ability for data subjects to authorise another person to make data subject requests on their behalf after the data subject's death.	Data fiduciaries should implement mechanisms to allow a data principal to make such nominations. Data fiduciaries must outline the procedure for nominating another person under the DPDPA within its terms of service.
Incident response							
39.	**Notification to regulator**	✓	*Notification content* The notification to relevant data protection authority should include: • nature of data breach; • name and contact details of the DPO;	✓	In the event of a personal data breach, a data fiduciary is required to notify the Data Protection Board as follows: • notification without delay including information on the nature, extent, timing, location, and likely impact of the breach; and	**Material gaps:** Unlike the GDPR, the DPDPA does not contain risk thresholds for the reporting of data breaches, meaning that every data breach is theoretically reportable to the Data Protection Board (and impacted individuals — see #40 below), regardless of the magnitude of the breach or the risk of harm.	Review existing data breach response and notification procedures and amend as necessary to reflect DPDPA mandatory breach reporting requirements. The specific format or manner of reporting will likely be prescribed closer to the DPDPA coming into force in May 2027.

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			• likely consequences of the data breach; and • measures taken or proposed to be taken by the controller to address the data breach, and measures to mitigate its possible adverse effects. *Notification timing* Relevant data protection authorities should be notified without undue delay and not later than 72 hours after becoming aware of the breach, unless the data breach is unlikely to result in a risk to the rights and freedoms of natural persons.		• provision of a detailed report within 72 hours of becoming aware of the breach, including: (a) an updated and more detailed description of the breach; (b) the events, circumstances, and reasons leading to the breach; (c) measures implemented or proposed to mitigate risk; (d) any findings regarding the cause or origin of the breach; (e) remedial measures taken to prevent recurrence of the breach; and (f) a report on the notifications made to affected data principals.		These new breach reporting obligations apply in parallel to the existing requirements on organisations operating in India to report data breaches and certain other cyber incidents to CERT-In (Computer Emergency Response Team — India) if a computer in India is impacted or a computer system from India has caused the data breach.

	Issue	Does the GDPR cover this issue?	Scope	Do the DPDPA or the DPDP Rules cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
40.	**Notification to affected data subjects**	✓	Notification should be made to affected data subjects without undue delay only if a breach is likely to result in a high risk to the rights and freedoms of the affected individuals.	✓	In the event of a personal data breach, a data fiduciary is required to notify affected data principals without delay including: • information on the nature, extent, and timing of the breach; • likely consequences of the breach for the data principal; • measures implemented by the data fiduciary to mitigate the risks; • safety measures recommended to be adopted by the data principal to protect their interests; and • contact information of the person responding to queries on behalf of the data fiduciary.	**Material gaps:** Unlike the GDPR, the DPDPA does not contain risk thresholds for the reporting of data breaches, meaning that every data breach is theoretically reportable to the impacted individuals regardless of the magnitude of the breach of the risk of harm.	Review existing data breach response and notification procedures and expand as necessary to reflect DPDPA mandatory breach reporting requirements. The specific format or manner of reporting will likely be prescribed closer to the DPDPA coming into force in May 2027. These new breach reporting obligations apply in parallel to the existing requirements on organisations operating in India to report data breaches and certain other cyber incidents to CERT-In (Computer Emergency Response Team — India) if a computer in India is impacted or a computer system from India has caused the data breach.

Endnotes

[1] India's data protection rules prior to the DPDPA and the DPDP Rules were made up of Section 43A and 87(2)(ob) of the Information Technology Act 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011.

[2] The gaps identified and steps required to be compliant are subject to the procedural guidance, which may be issued by the Indian government from time to time.

[3] Relevant requirements include: (i) sufficient capacity (including technical, operational, and financial capacity) to carry out consent manager obligations; (ii) corporate good standing and sound financial condition; (iii) adequate capital structure and revenue forecasts; (iv) sound reputation of directors, key managerial personnel, and senior management; and (v) provisions in corporate documentation addressing potential conflicts of interest with data fiduciaries.

[4] The European Commission has so far recognised Andorra, Argentina, Brazil, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, Korea, New Zealand, Switzerland, the United Kingdom, and Uruguay as providing adequate protection, as well as the EU-US Data Privacy Framework for relevant transfers to the US.

Gail E. Crawford
Partner
gail.crawford@lw.com
+44.20.7710.3001
London

Calum Docherty
Partner
calum.docherty@lw.com
+44.20.7710.1079
London

Fiona M. Maclean
Partner
fiona.maclean@lw.com
+44.20.7710.1822
London

Rhys McWhirter
Partner
rhys.mcwhirter@lw.com
+852.2912.2686
Hong Kong

Esther Franks
Counsel
esther.franks@lw.com
+65.6437.5345
Singapore

Danielle van der Merwe
Counsel
danielle.vandermerwe@lw.com
+971.4.704.6351
+44.20.7710.4666
Dubai / London

Bianca H. Lee
Associate
bianca.lee@lw.com
+852.2912.2500
Hong Kong

Amy Smyth
Knowledge Management Counsel
amy.smyth@lw.com
+44.20.7710.4772
London

The authors would like to thank Akash Karmakar, Anshika Gaur, and Kopal Arora at Panag, Babu & Sarangi for their contribution to this report.

This publication relates to legal developments in India, where Latham & Watkins (as a law firm established outside of India) is not licensed to practice. The law firm of Panag, Babu & Sarangi has advised on Indian law elements of the Digital Personal Data Protection Act 2023 and the Digital Personal Data Protection Rules 2025.