LATHAM & WATKINS LLP

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

December 2023

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

The Indian parliament enacted India's first comprehensive data protection law on 11 August 2023, namely the Digital Personal Data Protection Act 2023 (the DPDPA). The DPDPA will replace India's existing patchwork of data protection rules[1] and is expected to trigger significant changes in how companies subject to Indian data protection laws process personal data. However, the law is not yet operational; no effective date has been established and there is no official timeline for the overall implementation. Stakeholders expect the law to come into force in a phased manner in the next six to 12 months, after: (i) an independent agency responsible for enforcing the DPDPA — the Data Protection Board of India (the Data Protection Board) — is established; and (ii) the Indian government has framed the subordinate rules (which are expected to provide interpretative guidance on procedural steps and enforcement methodology). The DPDPA is "umbrella" legislation, as it sets out only a high-level framework for India's new data protection regime, with supplementary rules expected in due course. Though the new law is not yet operational, companies subject to the new law are advised to begin assessing potential practical implications at an early stage.

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, and rights for data principals (equivalent to "data subjects" under the GDPR). Penalties for non-compliance under the DPDPA range from INR500 million (€5.7 million) to INR2.5 billion (€28 million). The Data Protection Board is also empowered to impose urgent remedial or mitigation measures in the event of a personal data breach.

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 consider preemptive steps to bring their privacy compliance in line with the DPDPA, including as regards data collection and consent mapping practices. Key differences between the DPDPA and the GDPR 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 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: processing of personal data voluntarily shared by the data principal for a specified purpose (provided that the data principal does not object); processing to comply with the law or court orders; for employment purposes; or 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" and, unlike the GDPR, it does not permit processing under the lawful bases of contractual necessity or legitimate interests.

- **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, or erasure), they will also benefit from a number of new rights which are unique to the DPDPA, i.e., 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); otherwise, the DPDPA does not require the implementation of a transfer mechanism.

- **Data breach notification:** Data fiduciaries are required to notify personal data breaches to the newly created Data Protection Board and to impacted data subjects, regardless of the magnitude of the breach or risk of harm. Further, the DPDPA does not prescribe specific deadlines for 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 data protection impact assessments.

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 requirement under the DPDPA is materially consistent with the requirement under the GDPR — **no further action required to comply with the DPDPA.**	**No-action gaps:** DPDPA is generally consistent with GDPR, but with noticeable differences / GDPR standard is higher or more comprehensive — **additional compliance actions will not be required to comply with the DPDPA**.	**Manageable gaps:** DPDPA is generally consistent with GDPR, but with noticeable differences — **minor additional compliance actions will need to be taken to comply with the DPDPA**.	**Material gaps:** DPDPA is materially different from GDPR / there are elements under one law that are not found under the other — **significant additional compliance actions will need to be taken to comply with the DPDPA**.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA 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 of the DPDPA.	**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.
2.	**Sensitive / Special Category 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 personal data / special categories of data.	**No-action gaps:** No additional compliance obligations will need to be undertaken 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
3.	**Data Subjects**	✓	The identified or identifiable natural person, to whom personal data relates.	✓	Data Principal: The individual to whom the personal data relates, and, if such individual: (i) is a child, the concept includes the parent / lawful guardian of such child; and (ii) 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 others, determines the purposes and means of processing personal data.	✓	Data Fiduciary (i.e., data controller): Any person/entity who, alone or in conjunction with other persons, determines the purpose and means of processing an individual's personal data.	**Minimal difference**	N/A.
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: (a) volume and sensitivity of personal data processed; (b) risk to the rights of the data principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order.	**Material gaps:** The DPDPA identifies a class of data fiduciaries as SDFs based on the aforesaid 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 a resident data protection officer (DPO) who reports to the board of directors, conducts periodic audits, carries out periodic DPIAs, and deploys risk mitigation measures.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 are entities registered with the Data Protection Board under the DPDPA and act on behalf of data principals to review, provide, manage, and withdraw consent.	**Material gaps:** There is no equivalent concept under the GDPR.	Organisations may be required to either: (i) register as consent managers (subject to additional guidance provided by the rules framed pursuant to the DPDPA), or (ii) give data principals the option (through their user interface) to nominate a registered consent manager on their platform, app, website, etc.
8.	**Processing**	✓	Any operation or set of operations that is performed on personal data or on sets of personal data, whether or not 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 and 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
9.	**Processing Children's Data**	✓	The GDPR contains provisions to enhance the protection of children's personal data: (i) if transparency information is intended to be read by a child, it should be in clear and plain language that is easily comprehensible for the child; and (ii) 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.	✓	When processing a child's personal data (person under the age of 18) or a person with a disability, verifiable consent of the parent or the lawful guardian of such child/person with a disability must be obtained. With respect to children's personal data: (i) do not undertake processing of personal data that is likely to cause any detrimental effect to the well-being of a child; and (ii) do not track or engage in behavioural monitoring of children or use targeted advertising directed at children.	**Material gaps:** The DPDPA prescribes additional obligations with respect to processing children's data. It is also pertinent that the relevant age of the child varies under the GDPR and national EU Member State law and UK law implementations (i.e., 16 years or less) and the DPDPA (18 years).	To ensure compliance with the DPDPA's obligations for processing children's data, no data processing that is detrimental to children, or processing of data that in any manner would aid targeted advertising directed at children should be undertaken. To this end, to prevent inadvertent processing of children's data, methods that involve verifiable parental consent to process children's data (such as age-gating or multi-factor authentication) are recommended.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Transparency							
10.	**Privacy Policy Disclosures**	✓	Data subjects must be informed of the following at the time of collection of personal data: (i) name and contact details of the data controller and local representative (if applicable); (ii) contact details of the Data Protection Officer; (iii) purposes of processing; (iv) lawful basis for processing and legitimate interests for processing (if applicable); (v) categories of personal data obtained; (vi) recipients of personal data; (vii) details of transfers of personal data to any third countries or international organisations; (viii) retention periods for personal data; (ix) data subject rights; (x) right to withdraw consent (if applicable); (xi) right to lodge a complaint with a supervisory authority;	✓	A notice must be provided to data principals for obtaining their personal data either at the time of or before seeking such consent. The notice must include: (i) the personal data and the purpose for which it is being processed; (ii) the manner in which they may exercise their rights under the DPDPA with respect to the personal data; and (iii) the manner in which they may make a complaint to the Data Protection Board established under the DPDPA.	**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	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			(xii) source of personal data (if personal data is not obtained from the individual it relates to); (xiii) details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to); and (xiv) 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Legal Basis of Processing							
12.	**Consent**	✓	*Consent* Any freely given, specific, informed, and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her. *Explicit consent* Undefined, but must be affirmed in a clear statement and needs to specifically refer to the element of the processing that requires explicit consent.	✓	Consent given by the data principal must be: (i) duress-free; (ii) specific; (iii) informed; (iv) unconditional; (v) unambiguous; (vi) with a clear affirmative action signifying an agreement to the processing of personal data for the specified purpose; and (vii) presented in clear and plain language with the option to accept such requests as per Language Requirements (see #11).	**Minimal difference**	N/A.
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	**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).

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
					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.		
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 data principals' 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 data principals' 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 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 data principals' explicit consent if: • the data is required to provide medical treatment or health services to an individual during an epidemic, outbreak of disease, or threat to public health.	**No-action gaps:** The DPDPA specifically provides that consent is not required to process personal data to provide medical treatment/health services to individuals during an epidemic. There is no exact equivalent under the GDPR, but the closest legal basis would be for an individual's vital interests or for public interest purposes.	N/A.
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 data principals' explicit consent if: • the data is required to ensure the safety of persons, or provide assistance or services to any person during any disaster or any breakdown of public order.	**Minimal difference**	N/A.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 data principals' 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 the equivalent legal basis for processing. However, as this is an additional legal basis and therefore GDPR-compliant controllers are better able to process personal data without consent, no additional compliance steps are needed.	N/A.
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, #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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 data principals' 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	Does the DPDPA 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: (i) processes personal data in accordance with agreed purpose(s); (ii) returns or destroys personal data upon termination; (iii) obtains consent prior to contracting with sub-processors; (iv) implements necessary measures to ensure the security of personal data; (v) submits to audits and inspections; (vi) provides assistance to the controller to fulfil obligations under the GDPR; and (vii) notifies the data controller as soon as reasonably possible upon discovering a security breach.	✓	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: (i) comply with the DPDPA and rules thereunder; (ii) cease processing of, and erase personal data once consent is withdrawn; and (iii) take reasonable security safeguards to prevent data breach.	**Minimal difference**	N/A.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
International Data Transfers							
22.	**Adequacy Decision**	✓	Transfers of personal data from the European Economic Area (the EEA) to whitelisted countries[3] 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.	If and when such list of countries are published, transfers to such countries should be restricted.
23.	**Transfer Mechanism**	✓	To transfer personal data from the EEA or the UK to a non-whitelisted jurisdiction, the controller must: (i) implement an appropriate transfer mechanism (e.g., standard contractual clauses adopted by the European Commission or the UK equivalent); (ii) carry out a transfer impact assessment (a TIA); and (iii) depending on the TIA outcome, implement supplementary measures (e.g., encryption of data in transit and at rest).	✗	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.	**Material gaps:** Subject to additional guidance in the form of rules from the Indian government, the DPDPA does not provide for specific transfer mechanisms.	Do not transfer data to restricted countries (specific countries will be confirmed following the publication of the Indian government's list of countries to which data transfers are restricted).

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Privacy-by-Design / Documentary Requirements							
24.	**Inventory / Record of Processing (ROP)**	✓	The following should be recorded in a ROP: (i) the name and contact details of the controller and, if applicable, the joint controller, the controller's representative, and the data protection officer; (ii) the purposes of the processing; (iii) a description of the categories of data subjects and of the categories of personal data; (iv) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; (v) 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	✗	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	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
			the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards; (vi) if possible, the envisaged time limits for the erasure of the different categories of data; and (vii) 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 periodic DPIAs and manage the risk to data principals' rights.	**No-action gaps:** The DPDPA only requires SDFs (and not all data fiduciaries) to undertake periodic DPIAs, however, the rules will prescribe the manner of conducting such DPIAs.	N/A.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA 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: (i) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity; (ii) 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 (iii) 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 DPOs 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. 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA 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 (in this case, a DPO can fulfil this role) who is based in India (see #26 for relevant DPO requirements). All data fiduciaries are required to appoint a person to answer questions raised by data principals or appoint a DPO, however, there is no requirement for such an appointed person to be based in India.	**No-action gaps:** SDFs are required to appoint a local representative based in India, but a DPO based in India can fulfill both roles.	N/A.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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).	✓	Upon the data principal's request, a data fiduciary would need to provide details regarding: (i) summary of the personal data that is being processed; (ii) the processing activities being undertaken; (iii) identities of all other data fiduciaries with whom the personal data has been shared, along with the description of the personal data shared; and (iv) any other information as may be prescribed.	**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	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 correction, completion, or updating personal data from the data principal: (i) correct the inaccurate or misleading personal data; (ii) complete the inaccurate personal data; and (iii) update the personal data.	**Minimal difference**	N/A.
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 controller 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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
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 significant effect on the data subject).	✗	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.
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.	**Minimal difference**	N/A.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
36.	**Right to Lodge a Complaint With the Regulator**	✓	Data subjects have the 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 respond to any grievances within the prescribed period of time.	**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 grievance redressal mechanism and respond to grievances raised by the data principal within the proposed timeframe.
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.

#	Issue	Does the GDPR cover this issue?	Scope	Does the DPDPA cover this issue?	Scope	Key gaps[2]	Potential step(s) for DPDPA compliance
Incident Response							
39.	**Notification to Regulator**	✓	*Notification content* Notification to relevant data protection authority should include: (i) nature of data breach; (ii) name and contact details of the DPO; (iii) likely consequences of the data breach; and (iv) 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.	✓	In the event of a personal data breach, a data fiduciary is required to notify the Data Protection Board under the DPDPA in the form and manner that will be prescribed through rules under the DPDPA.	**Material gaps:** Unlike the GPDR, the DPDPA does not contain risk thresholds for the reporting of data breaches, meaning that every data breach is 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 expand as necessary to reflect DPDPA mandatory breach reporting requirements. 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	Does the DPDPA 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 the data principal as prescribed.	**Material gaps:** Unlike the GPDR, the DPDPA does not contain risk thresholds for the reporting of data breaches, meaning that every data breach is 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. 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] Indian's current data protection rules are 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 and supplementary rules, which will be issued in due course.
[3] The European Commission has so far recognised Andorra, Argentina, 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. Transfers to the US are also subject to the EU-US Data Privacy Framework (not adequacy decision).

Contact us:

Gail Crawford
Partner, Latham & Watkins

London
gail.crawford@lw.com
+44.20.7710.3001

Fiona Maclean
Partner, Latham & Watkins

London
fiona.maclean@lw.com
+44.20.7710.1822

Danielle van der Merwe
Counsel, Latham & Watkins

London
danielle.vandermerwe@lw.com
+44.20.7710.4666

Kate Burrell
Associate, Latham & Watkins

London
kate.burrell@lw.com
+44.20.7866.2702

Bianca H. Lee
Associate, Latham & Watkins

Hong Kong
bianca.lee@lw.com
+852.2912.2781

Alex Park
Associate, Latham & Watkins

Singapore
alex.park@lw.com
+65.6437.5436

Irina Vasile
Associate, Latham & Watkins

London
irina.vasile@lw.com
+44.20.7710.5894

Amy Smyth
Knowledge Management Lawyer, Latham & Watkins

London
amy.smyth@lw.com
+44.20.7710.4772

The authors would like to thank Akash Karmakar and Ridhima Khurana at the Law Offices of Panag & Babu for their contributions to this article.