GIR Global Investigations Review

The Guide to Cyber and Data Privacy Investigations - Fourth Edition

India: data privacy rules take shape, raising new questions for cross-border investigations

The Guide to Cyber and Data Privacy Investigations - Fourth Edition

Data breaches and similar incidents pose a unique challenge to organisations – those targeted must both respond and investigate in a tightly regulated, timely manner or face significant penalties. Written by leading contributors with broad experience of handling serious data incidents, the *Guide to Cyber and Data Privacy Investigations* is an invaluable resource for businesses around the globe. It identifies the most urgent issues to consider when creating and implementing a response template, and provides both legal and practical advice.

This edition of the Guide also features a new Spotlight section, which takes a deep dive into the cyber and data protection regimes of key jurisdictions around the world.

Generated: August 2, 2026

India: data privacy rules take shape, raising new questions for cross-border investigations

Shivalik Chandan, **Hardik Choudhary**, **Dhruv Singh** and **Arjun Khurana**
G&W Legal

Summary

SCOPE OF DATA PROTECTION LAWS RELEVANT TO CROSS-BORDER INVESTIGATIONS

WHAT LAWS AND REGULATIONS IN YOUR JURISDICTION REGULATE THE COLLECTION AND PROCESSING OF PERSONAL DATA? ARE THERE ANY ASPECTS OF THOSE LAWS THAT HAVE SPECIFIC RELEVANCE TO CROSS-BORDER INVESTIGATIONS?

In 2023, the Indian legislature enacted the country's first comprehensive data privacy legislation – the Digital Personal Data Protection Act 2023 (DPDPA). On 13 November 2025, the DPDPA was officially notified together with the Digital Personal Data Protection Rules 2025 (the DPDP Rules), the delegated legislation framed thereunder. The notifications adopt a phased implementation model: (1) provisions establishing the Data Protection Board of India (DPB), the regulatory authority under the DPDPA, the foundational definitions and the central government's rule-making power came into force with immediate effect from 13 November 2025; (2) provisions relating to the registration and obligations of consent managers will commence on 13 November 2026; and (3) the remaining substantive provisions, including the notice-and-consent regime, obligations of data fiduciaries, cross-border transfer provisions, the data breach reporting framework, the additional obligations of significant data fiduciaries and the rights of data principals, will commence on 13 May 2027. In practical terms, as of the date of this publication, only the DPB establishment framework and the foundational definitions are in force. The substantive data protection obligations do not yet apply.

From 13 May 2027 (when the remaining substantive provisions are expected to take effect), the DPDPA will regulate, among other things, the processing of "digital" personal data in India. ("Processing" itself is defined in a manner similar to the EU General Data Protection Regulation (GDPR) and subsumes the "collection" of personal data.) The DPDPA defines data fiduciaries (entities that determine the purpose and means of processing of personal data – akin to "data controllers" under the GDPR); data processors (entities that process personal data, including those processing on behalf of data fiduciaries); and data principals (individuals to whom the personal data relates – akin to "data subjects" under the GDPR) and outlines their respective obligations, rights and duties.

The DPDPA also empowers the central government to regulate transfers of personal data outside India by maintaining a list of countries to which transfer is restricted. The specific countries, if any, to be placed on that list have not yet been notified, introducing a degree of uncertainty for cross-border investigations that will only be resolved through enforcement practice after that date.

A note on the pre-DPDPA framework: the DPDPA, upon full implementation, is intended to replace the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (the SPDI Rules), framed under the Information Technology Act 2000 (the IT Act). Until the substantive provisions of the DPDPA come into force on 13 May 2027, the SPDI Rules continue to govern the privacy regime in India and will remain relevant to investigations conducted in the interim.

In addition to the above, there are also certain sector-specific laws in fields such as banking, insurance, medicine or healthcare, and telecoms, which also regulate processing of certain types of personal data. These will continue to apply, provided they do not conflict with the DPDPA or are not expressly repealed. Where a sectoral law imposes obligations more stringent than those under the DPDPA, the sectoral obligations will need to be met. Such

sectoral laws may be of independent relevance depending on the nature and scope of a given cross-border investigation.

Apart from legislative mandates, Indian constitutional jurisprudence affords additional safeguards that may extend to personal data. In what is now popularly known as the ***Puttaswamy*** Judgment, the Supreme Court of India for the first time recognised the right to privacy as a fundamental right. While analysing the various facets of privacy and the allied issues it would impact, the ***Puttaswamy*** Judgment engaged with the concept of "informational privacy" and acknowledged an individual's right to "control the dissemination of personal information". The ***Puttaswamy*** Judgment formed the constitutional basis for the enactment of the DPDPA and is also independently significant. Unlike the statutory regime described above, the constitutional right to privacy recognised in the ***Puttaswamy*** Judgment is presently enforceable and has immediate application to any cross-border investigation raising questions of informational privacy.

WHAT OTHER LAWS AND REGULATIONS, BESIDES DATA PROTECTION LAWS, MAY PREVENT DATA SHARING IN THE CONTEXT OF AN INVESTIGATION?

Apart from the DPDPA, various other regulations also impose obligations that could potentially impact data sharing in the context of a cross-border investigation. This might include situations where data subjects involved in an investigation, or the investigation itself, are in the realm of sectors such as banking or fintech, telecoms or digital health, etc.

For instance, in the banking sector, the storage and transfer of financial data are separately regulated. The Reserve Bank of India (RBI), India's central bank and regulator, mandates that data related to payments (such as customer information and identification numbers, account details, passwords or transaction details) be stored on systems within India; for cross-border transactions, a "copy" of the domestic leg of the transaction may be stored overseas, but the mandate of storage in India still applies. In cases where payments are processed overseas, the RBI mandates that data be deleted from foreign systems and "brought back" to India within 24 hours. Also, to protect "card data", the RBI has mandated "tokenisation" of data subjects' credit card and debit card information that would replace saving (collection) actual card details, and also mandates purging of the actual card details.

Other sectoral examples include the Insurance Regulatory and Development Authority of India (Third Party Administrators – Health Services) Regulations 2016 (the IRDAI Regulations), which restrict the sharing of policy and claims-related data and personal information; and cases where government data is involved. The latter is especially relevant where an investigation involves Indian government departments or a third-party storing government data since such data is required to be stored in India under the IRDAI Regulations.

WHAT CONSTITUTES PERSONAL DATA FOR THE PURPOSES OF DATA PROTECTION LAWS?

As the DPDPA's substantive provisions are not yet in force, cross-border investigations conducted prior to 13 May 2027 will continue to be governed by the SPDI Rules where SPDI is involved. The SPDI Rules distinguish between "personal information" and "sensitive personal data or information" and accord a higher emphasis on the protection of the latter. The subject matter covered as SPDI under the SPDI Rules is exhaustive and comprises passwords; financial information (bank account and credit card details); health conditions and medical records; sexual orientation; biometric information; and any other details relating

to the preceding (unless such information is freely available or accessible in the public domain).

From 13 May 2027, under the DPDPA, "personal data" is broadly defined to mean any data about an individual who is identifiable by or in relation to such data. Data is also defined to include, among other things, "representation of information, facts, concepts, opinions or instructions", rendering the overall scope of "personal" data quite wide. Personal data under the DPDPA is, however, restricted to data that relates to natural persons only.

The DPDPA is applicable only to "digital" personal data; while there is no further sub-categorisation of "digital" personal data, the DPDPA delineates the scope of "digital" to include personal data collected in digital form or that collected in non-digital form and subsequently digitised.

There are a few exemptions to the defined scope: personal data that is made or caused to be made available in the public domain by the data principal, or any other person under a legal obligation to do so, would fall outside the scope of "personal data" or applicability of the DPDPA. Personal data processed by an individual for personal or domestic purposes also falls outside the scope of the DPDPA.

WHAT IS THE SCOPE OF APPLICATION OF DATA PROTECTION LAWS IN YOUR JURISDICTION? WHAT ACTIVITIES TRIGGER THE APPLICATION OF DATA PROTECTION LAWS, TO WHOM DO THEY APPLY AND WHAT IS THEIR TERRITORIAL EXTENT?

Currently, the SPDI Rules are the operative framework, applying to "body corporates" that collect or process "sensitive personal data or information" – a defined category covering passwords, financial information, health data, biometric data and similar categories. Unlike the DPDPA, the SPDI Rules do not carry an express extraterritorial provision and are primarily directed at body corporates operating in India. From 13 May 2027, the SPDI Rules will be replaced by the substantive provisions of the DPDPA.

The DPDPA applies only to the processing of "digital" personal data as mentioned previously. The term "processing" has been defined to include all wholly or partly automated operations performed on personal data, including collection, recording, organisation, structuring, storage, use, sharing, disclosure, dissemination, erasure, etc. The application of the DPDPA may be triggered upon any operation performed on personal data that falls within the definition of processing, or upon breach of any provision or compliance in relation to the same. The processing of personal data can be done by the data fiduciary or the data processor (on behalf of the data fiduciary and under a valid contract only).

Non-digital, fully non-automated or offline processing of personal data is not covered by the DPDPA.

In terms of territorial extent, the DPDPA extends not just to the territory of India but may also apply to the processing of digital personal data outside the territory of India if such processing is in connection with any activity of offering goods and services to data principals within the territory of India. Whether and how this extraterritorial limb will be enforced in practice remains to be seen, as the DPB has not yet operationalised its enforcement machinery.

WHAT ARE THE PRINCIPAL REQUIREMENTS UNDER DATA PROTECTION LAWS THAT ARE RELEVANT IN THE CONTEXT OF INVESTIGATIONS?

Currently, the SPDI Rules remain the operative framework. Body corporates handling SPDI in the context of an investigation must obtain prior consent, provide a privacy policy, use SPDI only for the purpose collected, not retain it beyond that purpose and maintain reasonable security practices. Transfers to third parties outside India require either consent or a contractual arrangement ensuring equivalent data protection standards.

Once fully applicable in May 2027, the DPDPA stipulates that processing of personal data can be done for: (1) a lawful purpose (which is defined as any purpose that is not expressly forbidden by law) for which the data principal has given specific consent; or (2) for certain "legitimate uses" (this has been exhaustively defined under the DPDPA – processing of personal data under these grounds does not require consent). Notably, the obligations under the DPDPA are applicable only to data fiduciaries and not to data processors per se. The data fiduciary is in fact obligated to ensure the data processor's compliance with DPDPA provisions – which will need to be done through contractual provisions between the data processor and data fiduciary. The nature/scope ("lawful purpose" or applicability of exemptions – discussed below) of the investigation might be relevant here from the point of cross-border investigations.

There are certain exemptions to the above umbrella provision. Principal requirements may thus vary depending on the nature of the investigations (if the nature or conditions fall under the exemptions). For instance, if the investigation relates to "enforcement of a legal right/claim" or "of any offence or contravention of law", or for ascertaining "financial assets and liabilities" of a defaulter, then the only obligation applicable is to adopt reasonable security safeguards to prevent breach of the personal data processed.

In the same vein, the consent requirement will not be applicable in certain cases where personal data is processed for the purposes of employment or in compliance with court orders (orders passed under foreign law included – if they relate to claims of a contractual or civil nature), etc.

On the opposite side of the spectrum, there are some additional requirements (including obtaining verifiable parental consent and a prohibition on tracking or behavioural monitoring) when the personal data being processed relates to children. The DPDP Rules provide some clarity on the requirements of the verifiable parental consent needed and have granted exemptions to certain categories of institutions and certain purposes from the requirements relating to processing children's personal data.

Other requirements under the DPDPA take the form of obligations imposed on data fiduciaries, including the appointment of a person answerable to data principals on behalf of the data fiduciary; setting up grievance redressal mechanisms (with a response timeline not exceeding 90 days); reporting of personal data breaches (to the DPB and to affected data principals); and maintaining the accuracy of records – all of which are likely to be implicated in investigations. Additional and more stringent obligations, including appointing an India-based data protection officer, conducting annual data protection impact assessments and independent audits, and undertaking algorithmic due diligence, apply where the data fiduciary is designated as a "significant data fiduciary" (SDF) by the central government. The DPDP Rules now provide concrete guidance on what constitutes "reasonable security safeguards" (including access controls, encryption or masking/tokenisation, logging with a minimum one-year retention period and continuity measures) and prescribe a two-stage data breach reporting framework: an immediate notification to the DPB and affected data principals "without delay", followed by a detailed report to the DPB within 72 hours.

The 72-hour DPB timeline operates alongside the continuing obligation under the Indian Computer Emergency Response Team (CERT-In) directions to report cyber incidents within six hours of becoming aware of the incident, creating a dual reporting clock.

Another important consideration for cross-border investigations is the transfer of personal data outside India. The DPDPA, read with Rule 15 of the DPDP Rules, adopts a "negative list" (blacklist) approach: personal data may be transferred outside India unless the central government, by general or special order, restricts such transfer to a specific country or category of recipients. As at the date of writing, no such restrictions have been notified. The DPDP Rules additionally empower the central government to specify requirements for SDFs in respect of the transfer of certain categories of personal data (and traffic data related to its flow) outside India. The cross-border transfer provisions form part of Phase 3 of the DPDPA's implementation and will become operative on 13 May 2027; until then, transfers continue to be governed by the SPDI Rules and applicable sectoral mandates.

With cross-border investigations going remote in the post-pandemic world, transfer obligations become especially relevant, since the initial collation and review of electronically stored information such as emails will invariably involve a transfer of data outside India.

IDENTIFY THE DATA PROTECTION REQUIREMENTS RELEVANT TO A COMPANY CARRYING OUT AN INTERNAL INVESTIGATION AND TO A PARTY ASSISTING WITH AN INVESTIGATION.

As mentioned above, compliance obligations under the DPDPA are on the data fiduciary (and not the data processor). To put it simply, the burden of compliance under the DPDPA will be on the entity that has determined the purpose and means of processing of the personal data (likely the entity commissioning the investigation). The DPDPA also foresees the possibility of joint fiduciaries as well as multiple independent fiduciaries for the same piece of personal data. However, this is not something that it covers in any detail.

The DPDP Rules further clarify the data fiduciary's obligations to take reasonable security measures to protect personal data in its possession or under its control, including in respect of any processing undertaken by it or on its behalf by a data processor. Among other things, the DPDP Rules mandate that any contract between a data fiduciary and a data processor must include appropriate provisions to this effect.

"Assisting" entities will likely all be data processors with no direct obligations under the DPDPA, and data fiduciaries are required to ensure that data processors comply with applicable data protection standards, and this should be reflected in contractual terms (as explained above) – this becomes particularly relevant in the context of cross-border investigations. Until May 2027, however, the position under the currently operative SPDI Rules is different – the SPDI Rules do not draw an equivalent distinction, and any body corporate that collects or handles SPDI in the course of an investigation, including an assisting entity, may independently bear obligations in its own right, regardless of any contractual arrangement with the commissioning entity.

Applicable sectoral laws (such as those governing financial institutions, healthcare or telecoms) may impose direct obligations on data processors as well, depending on the nature of the personal data involved or the specific facts of the investigation. Additionally, if personal data is transferred outside India for investigative purposes, such transfers must comply with any restrictions and conditions prescribed under the DPDPA and the DPDP Rules (as discussed more fully in a later section).

Finally, data fiduciaries must remain mindful of data principals' rights under the DPDPA, including the right to access, correct and erase personal data. Even in the context of investigations, mechanisms should be in place to respond to such requests within prescribed timelines, unless lawful exemptions (such as for legal proceedings or law enforcement) are applicable. Ensuring legal defensibility in withholding data or denying access will be crucial in such cases.

RIGHTS OF INDIVIDUALS

IS THE CONSENT OF THE DATA SUBJECT MANDATORY FOR THE PROCESSING OF PERSONAL DATA AS PART OF AN INVESTIGATION?

Under the currently operative SPDI Rules, consent is required prior to collection of SPDI but the framework is less prescriptive. Under the DPDPA the data principal's or subject's free, specific, informed, unconditional and unambiguous consent, given through a clear affirmative action, is mandatory for the processing of personal data, and for processing as part of an investigation. There are limited exceptions where data can be processed without the subject's prior consent (including that of an employee, for "employment purposes", among other things, which are discussed later in this chapter).

Under the DPDPA, every request for consent made to the data principal shall be accompanied or preceded by a "notice" given by the data fiduciary. Through the notice, the data fiduciary shall inform the data principal of the personal data being processed and the purpose for processing it; the manner in which the data principal may exercise their rights and the manner in which the data principal may make a complaint to the DPB. These provisions will become operative on 13 May 2027.

IF NOT MANDATORY, SHOULD CONSENT STILL BE CONSIDERED WHEN PLANNING AND CARRYING OUT AN INVESTIGATION?

Although the data principal's or subject's consent is mandatory (barring specific exemptions), this does not always mean that consent must be separately sought when planning or carrying out an investigation. The requirement of consent can be fulfilled even if such consent has already been provided through an underlying contract (and meets the above-stated qualifiers for specific consent and notice).

The DPDPA provides that there are exemptions to the mandatory consent requirement, including in the case of processing employee data for the purposes of employment or protecting the employer from certain loss or liability, and implementation of a court order.

IS CONSENT GIVEN BY EMPLOYEES LIKELY TO BE VALID IN AN INVESTIGATION CARRIED OUT BY THEIR EMPLOYER?

As mentioned earlier, the DPDPA does not require consent in the case of processing employee data if done for the purposes of employment or for safeguarding the employer from loss or liability. A few examples in the DPDPA include prevention of corporate espionage, maintenance of confidentiality of trade secrets and intellectual property, or provision of any service or benefit sought by a data principal who is an employee. Additionally, the standard of consent as under the DPDPA is unlikely to be met in the case of an employee providing consent to an employer (as such consent must be "free" and "unconditional").

HOW CAN CONSENT BE GIVEN BY A DATA SUBJECT? IS IT POSSIBLE FOR DATA SUBJECTS TO GIVE THEIR CONSENT TO PROCESSING IN ADVANCE?

The DPDPA requires specific consent to be obtained through clear, affirmative action and that it be free, specific, informed and unambiguous. Further, as clarified by the DPDP Rules, the request for consent must be presented to the data principal in clear and plain language and must be accompanied or preceded by a notice that specifies the nature and purpose of the processing, the type of personal data being collected and the purpose associated with each type of personal data, and the rights available to the data principal, including the right to withdraw consent.

While it is possible for data principals to give specific consent for processing in advance, such consent would only be valid for so long as their personal data is being processed for the specific purpose for which it was collected. As soon as this remit is exceeded, fresh consent would be necessary.

Moreover, data principals retain the right to withdraw their consent at any time, upon which the data fiduciary is obligated to cease processing the data, unless another lawful basis (such as legal obligation) permits continued processing. Therefore, even where advance consent is obtained, organisations must monitor their processing activities to ensure they remain within the boundaries of the original consent and are prepared to re-engage with data principals to seek fresh consent for any material changes in processing purposes.

WHAT RIGHTS DO DATA SUBJECTS HAVE TO ACCESS OR VERIFY THEIR PERSONAL DATA, OR TO INFLUENCE OR RESIST THE PROCESSING OF THEIR PERSONAL DATA, AS PART OF AN INVESTIGATION?

Under the DPDPA, data principals or subjects have the right to access, correct and erase the personal data provided by them. Further, the DPDPA also gives the data principal the option to withdraw their consent; this will apply equally in the context of an investigation, particularly if the investigation concerns "retainers" or "contractual" hires or if the personal data processed is not for employment purposes. The withdrawal of consent does not affect the legality of the processing of personal data prior to the withdrawal of consent; the DPDPA also clarifies that the data principal is liable to bear the consequences of such withdrawal of consent. If consent is withdrawn, the data fiduciary is under an obligation to cease or cause to be ceased (within "reasonable time") processing of personal data for which consent is withdrawn. Once the relevant provisions are operative on 13 May 2027, data fiduciaries will be required to establish dedicated mechanisms for data principals to exercise these rights and respond within timelines prescribed under the DPDP Rules.

EXTRACTION, LEGAL REVIEW AND ANALYSIS BY THIRD PARTIES, INTERNATIONAL TRANSFER

ARE THERE SPECIFIC REQUIREMENTS TO CONSIDER WHERE THIRD PARTIES ARE APPOINTED TO PROCESS PERSONAL DATA IN CONNECTION WITH AN INVESTIGATION?

Under the DPDPA, the obligation to comply with the law and to ensure compliance by a data processor, is solely on the data fiduciary. This means that if a third party is appointed to process personal data during an investigation, the data fiduciary remains fully accountable for ensuring that the data processor adheres to the requirements of the DPDPA, and penalties under the DPDPA will be imposed on the data fiduciary only if there is non-compliance through action or inaction of the data processor.

Broadly, considering that the direct obligation to comply is on the data fiduciary, when contracting with any third party for assistance during an investigation, it is advisable to not just bind the consultant with comprehensive data protection obligations, but to also ensure

that the consultant, in turn, has robust confidentiality obligations and similar provisions in its agreements with its own employees and subcontractors.

Additionally, it is prudent for data fiduciaries to include audit rights in the contract to verify the third party's compliance with data protection requirements, as well as indemnity clauses to mitigate risks arising from any breach or non-compliance by the processor. Appropriate exceptions to limitation of liability clauses must also be made in such contracts as the penalties prescribed under the DPDPA are substantial – up to approximately US$26.5 million.

IS IT PERMITTED TO SHARE PERSONAL DATA WITH LAW FIRMS OR LEGAL PROCESS OUTSOURCING FIRMS FOR THE PURPOSE OF PROVIDING LEGAL ADVICE?

Under current laws, there is no express provision on the kinds of entities personal data should or should not be shared with. As such, data can be shared with law firms or legal process outsourcing firms, provided the data transfer is compliant with the applicable regulations, which currently include the SPDI Rules and any relevant sectoral laws (such as those governing banking, insurance or healthcare). Under the DPDPA and DPDP Rules, however, it is important to note that such sharing with third parties would entail the creation of a fiduciary–processor relationship where the entity sharing the data would be responsible and liable for ensuring compliance with the provisions of the DPDPA on behalf of the data processor (the law firm or legal process outsourcing firm). The DPDP Rules require these obligations to be reflected in contracts entered into with data processors (the law firm or legal process outsourcing firm), including in respect of reasonable security safeguards.

ARE THERE ANY ADDITIONAL REQUIREMENTS, BEYOND THOSE SPECIFIED ABOVE, THAT REGULATE THE DISCLOSURE OF DATA TO THIRD PARTIES WITHIN YOUR JURISDICTION FOR THE PURPOSE OF REVIEWING THE CONTENT OF DOCUMENTS, ETC?

Beyond what has already been mentioned above, there are no additional requirements that regulate the disclosure of data to third parties for purposes such as external document review under the existing laws.

WHAT RULES REGULATE THE TRANSFER OF DATA HELD IN YOUR JURISDICTION TO A THIRD PARTY IN ANOTHER COUNTRY FOR THE PURPOSE OF REVIEWING THE CONTENT OF DOCUMENTS, ETC?

The transfer of personal data outside India (including for the purpose of reviewing the content of documents) is permissible, provided it is not to a country or class of recipients restricted by the central government. As at the date of writing, no such restrictions have been notified, although these provisions become formally operative only on 13 May 2027. Until then, cross-border transfers continue to be governed by the SPDI Rules and applicable sectoral mandates. Additionally, the DPDPA clarifies that any sector-specific regulations with more stringent cross-border data transfer restrictions will prevail over the DPDPA's requirements.

The DPDP Rules additionally empower the central government to specify requirements for SDFs in respect of the transfer of certain categories of personal data (and traffic data related to its flow) outside India, on the recommendation of a notified committee. SDFs may also be required to undertake due diligence to verify that their technical measures do not pose a risk to the rights of data principals. Whether and how these powers will be exercised in practice remains to be seen.

Additionally, sector-specific regulations, which may impose more stringent obligations including data localisation, may apply to such transfers depending on the nature of the documents being sent abroad for review. The DPDPA recognises and upholds higher thresholds prescribed under other laws.

ARE THERE SPECIFIC EXEMPTIONS, DEROGATIONS OR MECHANISMS TO ENABLE INTERNATIONAL TRANSFERS OF PERSONAL DATA IN CONNECTION WITH INVESTIGATIONS?

Apart from what has already been discussed, there are no other exemptions or specific mechanisms that can automatically enable cross-border data flow in the context of internal investigations under the DPDPA. As stated before, depending on the specific scope and nature of the investigation, sectoral laws may provide for separate mechanisms.

TRANSFER TO REGULATORS OR ENFORCEMENT AUTHORITIES

UNDER WHAT CIRCUMSTANCES IS THE TRANSFER OF PERSONAL DATA TO REGULATORS OR ENFORCEMENT AUTHORITIES WITHIN YOUR JURISDICTION PERMISSIBLE?

The DPDPA does not have any specific mandates relating to the transfer or disclosure of personal data to data regulators or enforcement authorities. However, many exemptions throughout the DPDPA apply to processing (including transfer or disclosure) of personal data by the state or its instrumentalities (including government entities, departments and agencies). For instance, the DPDPA permits processing of personal data by the government and its instrumentalities, including regulators and enforcement authorities for fulfilling any obligation under any law subject to certain conditions.

The DPDP Rules specify the purposes for which the central government may seek information from data fiduciaries or intermediaries, and the persons authorised to seek such information. In sensitive cases, prior written permission may be granted to restrict the disclosure of such requests to the affected data principal. Cross-border investigations involving cooperation with Indian regulators will need to be evaluated in light of these provisions once they come into force.

UNDER WHAT CIRCUMSTANCES IS THE TRANSFER OF PERSONAL DATA HELD WITHIN YOUR JURISDICTION TO REGULATORS OR ENFORCEMENT AUTHORITIES IN ANOTHER COUNTRY PERMISSIBLE?

The DPDPA is silent on the explicit permissibility or procedure for the transfer of data to foreign regulators or enforcement authorities. Further, while a data protection authority (the DPB) is being set up under the DPDPA, it is not immediately clear if and what role the board might play in such a transfer. As of the time of writing, there is no formal mechanism within the DPDPA that governs government-to-government data disclosures or private data fiduciary transfers to foreign enforcement bodies. However, a transfer of personal data to a foreign regulator or enforcement authority may be restricted by the provision of the DPDP Rules that allows the central government to restrict cross-border data transfer to entities and instrumentalities of foreign states.

Additionally, there are sector-specific regulations such as those governing payment data (which fall under personal data) where the RBI's approval is required before data is shared with a foreign regulator. Other sectors such as telecoms, banking and healthcare have similar restrictions or data localisation requirements under their respective regulatory frameworks.

WHAT ARE SOME RECOMMENDED STEPS TO TAKE ON RECEIPT OF A REQUEST FROM A REGULATOR FOR DISCLOSURE OF PERSONAL DATA?

The first thing to do here would be to check whether the request is backed by any DPDPA provision or other applicable law, and if so, if it calls for certain requirements such as a court order for disclosure of personal data. Additionally, it might be helpful for the entity receiving the request to assess if it qualifies as an "intermediary" under the IT Act and whether there are any safe harbour provisions or additional compliances that might affect disclosure requirements under applicable laws and regulations. For example, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 mandate that an intermediary shall comply with an order from an authorised government agency – for information for the purposes of identity verification, or for prevention, detection, investigation or prosecution of offences under any law or for cybersecurity incidents – within 72 hours. Once the relevant provisions of the DPDPA come into force on 13 May 2027, the DPDP Rules will provide an additional reference point for assessing the validity and scope of any such request. It is important to evaluate any request from a regulator to verify if the request is intra vires, and to also be aware of how the request – if ultra vires – can be challenged.

ENFORCEMENT AND SANCTIONS

WHAT ARE THE SANCTIONS AND PENALTIES FOR NON-COMPLIANCE WITH DATA PROTECTION LAWS?

Until the enforcement of the DPDPA in May 2027, the sanctions and penalties in relation to personal data are governed by the IT Act, which provides for a penalty of up to approximately US$1,200 as well as compensation to the affected individuals to the tune of approximately US$12,000 where the contravention is committed by a company and approximately US$1,200 where the contravention is committed by an individual.

Under the DPDPA, the penalty provisions have been significantly enhanced and provide for penalties as high as up to approximately US$26.5 million being imposed.

The determination of the penalty would be done by the DPB based on factors such as nature, gravity and duration of breach; the repetitive nature of breach; mitigating actions taken by the contravening entity, etc; and this decision can be challenged in an appellate tribunal.

RELEVANT MATERIALS

Relevant materials that would be helpful in this context are as follows:

- Digital Personal Data Protection Act 2023
- Digital Data Protection Rules 2025
- CERT-In Directions
- *Justice K.S. Puttaswamy & Anr. v Union of India*, Writ Petition (Civil) No. 494 of 2012
- The Information Technology Act 2000
- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021
- RBI Circular on Storage of Payment System Data

- Insurance Regulatory and Development Authority of India (Third Party Administrators – Health Services) Regulations 2016

Shivalik Chandan shivalik@gnwlegal.com
Hardik Choudhary hardik.choudhary@gnwlegal.com
Dhruv Singh dhruv@gnwlegal.com
Arjun Khurana arjun@gnwlegal.com

http://www.gnwlegal.com