GIR KNOW HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

India

Manavi Jain, Hardik Choudhary,
Disha Mohanty and Dhruv Singh
G&W Legal

OCTOBER 2023

GIR

SCOPE OF DATA PROTECTION LAWS RELEVANT TO CROSS-BORDER INVESTIGATIONS

1. 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?

After many versions of a proposed data privacy law were circulated over the last several years, India recently enacted the Digital Personal Data Protection Act 2023 (the DPDPA). Although notified in the Official Gazette as 'law', the DPDPA, as of September 2023, has not been officially implemented. The relevant government department will notify the date of implementation of the DPDPA (different dates may be appointed for different provisions) in due course – likely after the setting up of the Data Protection Board, as many provisions of the DPDPA rely extensively on the setting up of the Board.

Once implemented, the DPDPA will regulate, among other things, the processing of 'digital' personal data in India. ('Processing' itself is defined in a similar fashion as the General Data Protection Regulation (GDPR) and subsumes 'collection' of personal data as well.)

The DPDPA defines data fiduciaries (that is, entities determining the purpose and means of processing of personal data – akin to 'data controllers' under the GDPR); data processors (that is, entities processing personal data, including those on behalf of data fiduciaries) and data principals (that is, individuals to whom the personal data relates to), and outlines their obligations, rights and duties. Further, the DPDPA also provides the Indian government the power to regulate transfers of personal data outside India, which is relevant for cross-border investigations.

A quick note on the pre-DPDPA laws: the DPDPA, upon implementation, seeks to replace the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules), which were framed under the Information Technology Act 2000 (IT Act) and served as the primary data privacy law in India up until now, albeit with very limited scope. Until the implementation of the DPDPA, the SPDI Rules are likely to be applicable at least in some capacity and thus continue to remain currently relevant.

In addition to the above, there also exist 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. There are also subordinate rules and regulations framed under the IT Act (other than SPDI Rules) relating to data protection or privacy in specific scenarios. These will continue to apply, provided they do not conflict with the provision(s) of the DPDPA or are expressly repealed. If a sectoral law provides for higher obligation(s) than the DPDPA, then the obligations under the specific sectoral law may have to be met. These sectoral laws would similarly be relevant depending on the nature and/or scope of a given cross-border investigation.

Apart from legislative mandates, Indian legal jurisprudence also provides additional safeguards that could include personal data within their ambit. 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 became the basis for the enactment of the DPDPA but is also independently significant.

2. 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, telecom 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, which nonetheless means that 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. This can be important in the context of a cross-border investigation because if an overseas regulator is involved in the process, data sharing with that regulator requires RBI approval. Also, towards protecting 'card data', the RBI also issued a circular mandating 'tokenisation' of credit card and debit card information of data subjects that would replace saving (collection) of actual card details and also mandated 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 (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.

3. What constitutes personal data for the purposes of data protection laws?

Under the DPDPA, a broad definition of 'personal data' has been provided to mean any data about an individual who is identifiable by or in relation to such data. Data is also defined – and includes, among other things, 'representation of information, facts, concepts, opinions or instructions', rendering the overall scope of 'personal' data quite wide.

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. As such, non-digital or non-digitised data continues to exist in a state of legislative limbo.

The DPDPA also defines the term 'person' whose definition includes an 'individual' among others, including juristic persons. However, the use of 'individual' over the more generic defined term 'person' in the definition of personal data implies that it is applicable only to natural persons and not to juristic or legal persons.

There are a few exemptions to the defined scope here: 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.

The relatively broad definition of personal data is a major point of difference when compared against the earlier SPDI Rules, which distinguished between 'personal information' and 'sensitive personal data or information (SPDI)' and accorded a higher emphasis on the protection of the latter. The subject matter covered as SPDI under the SPDI Rules was thus exhaustive and comprised 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). If the cross-border investigations of the near future pertain to SPDI, the SPDI Rules might still apply (depending on the date of implementation of the DPDPA).

4. 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?

DPDPA applies 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. It includes collection, recording, organisation, 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 and/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 processing of digital personal data outside the territory of India in some cases, for instance, if such processing is in connection with any activity of offering goods and services to data principals within the territory of India.

5. What are the principal requirements under data protection laws that are relevant in the context of investigations?

As an umbrella provision, the DPDPA stipulates that processing of personal data can be done for (i) 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 (ii) for certain 'legitimate uses' (this has been exhaustively defined under the DPDPA – processing of personal data under these grounds do 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 data processor's compliance with DPDPA provisions. 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 (IS/ISO/IEC 27001 is an approved standard for reasonable security practices and procedure under the SPDI Rules and may also be approved under the DPDPA separately).

In the same vein, the consent requirement will not be applicable in certain cases where personal data is processed for the purposes of employment; 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 a prohibition on tracking or behavioral monitoring) when the personal data being processed relates to children.

Other requirements under the DPDPA are in the form of obligations to be discharged by the data fiduciary and include appointment of a person answerable (to the data principals) on behalf of the data fiduciary, setting up grievance redressal mechanisms, reporting of personal data breaches (including to data principals), maintaining accuracy of records (limited obligation); all of which are possible scenarios in investigations. There could be additional (more stringent) obligations, including appointing an India-based data protection officer and conducting periodic data protection assessments, if the data fiduciary is a 'significant data fiduciary' notified by the government.

Another important consideration for cross-border investigations is the transfer of personal data. There is no restriction on transferring personal data outside of India for the purposes of processing, as long as other umbrella requirements are fulfilled. However, the DPDPA does grant the central government the power to notify countries to which such transfer is prohibited. 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 (ESI) such as emails will invariably involve a transfer of data outside India.

6. 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, primary 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 foresees the possibility of multiple data fiduciaries as well if we go by the definition. The practicalities of discharging obligations with multiple data fiduciaries are yet to be made clear.

On the other hand, 'assisting' entities will likely all be data processors with no direct obligations under the DPDPA; although obligations of data fiduciary under the DPDPA include ensuring compliance by the data processor (which should, as such, be captured within the contract with the data processors – again, something relevant for cross-border investigations). Applicable sectoral laws might differ in this regard in that direct obligations could be incurred by data processors as well – but this will depend on the specific facts or nature of the investigation.

RIGHTS OF INDIVIDUALS

7. Is the consent of the data subject mandatory for the processing of personal data as part of an investigation?

Yes, the data principal 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 – these 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 Data Protection Board.

8. If not mandatory, should consent still be considered when planning and carrying out an investigation?

Although the data subject's consent is mandatory (barring for 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). This might become relevant if the cross-border investigation relates to 'retainers' or 'contractual' hires or the personal data processed is not for employment purposes.

DPDPA provides that the consent requirement is not mandatory in certain cases, including in case of processing employee data for purposes of employment and implementation of a court order.

9. 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.

10. 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 through clear, affirmative action. Further, the request for consent must be presented to the data principal in clear and plain language and should be accompanied or preceded by a notice.

While it is possible for data principals to give specific consent to processing in advance, such consent would only be valid till the time their data is being used for the specific purpose for which it was collected. In theory, a company's standard contract terms could include the possibility of the data principal or subject's personal data being used in the context of audits, investigations, etc, as long as it conforms to the specific consent and notice requirements. As soon as the company's use of a data principal or subject's personal data is exceeding the remit for which consent was initially obtained, fresh consent for the applicable additional purposes would be required.

11. 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, correction and erasure of the personal data provided by them.

Further, the DPDPA also gives the data principal the option to withdraw their consent; and 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 would 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.

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

12. 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 and ensure compliance by a data processor, is solely on the data fiduciary.

Broadly, considering the direct obligation to comply is on the data fiduciary, while 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 make sure that the consultant in turn has robust confidentiality and similar provisions in its agreements with its own employees and subcontractors.

13. 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 shouldn't 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.

14. 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 in the preceding paragraphs, 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.

15. 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?

Under the DPDPA, transfer of data outside India (including for the purpose of reviewing the content of documents) is permissible, provided it is not to a territory blacklisted by the Indian government (which will be notified in due course). Additionally, other sector-specific regulations (which may have a higher protection obligation such as local storage) may apply to such a transfer depending on the nature of documents that are being sent abroad for review – the DPDPA recognises and upholds such higher bar within other laws.

16. 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 dataflow in the context of internal investigations under the DPDPA. As before, depending on the specific scope and nature of the investigation, sectoral laws may provide for separate mechanisms.

TRANSFER TO REGULATORS OR ENFORCEMENT AUTHORITIES

17. 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 'transfer' or 'disclosure'-related mandates in relation to data regulators or enforcement authorities as such. Many exemptions throughout thr DPDPA, however, apply to processing (including transfer or disclosure) of personal data by the state or its instrumentalities. For instance, 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.

Separately, the DPDPA further empowers the central government to exempt the state instrumentalities from its provisions. This provision, which gives the central government the power to direct even the Data Protection Board to furnish information, is being criticised as giving wide reaching powers to the government and may see some change. The provision also expressly exempts the state or its

instrumentalities from the requirement of erasure of personal data, including on request of the data principal.

The DPDPA is silent on the manner in which government agencies can access personal data from data fiduciaries for processing.

18. 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 transfer of data to foreign regulators or enforcement authorities. Further, while a data protection authority (the Data Protection Board of India) is being set up under the DPDPA, it is not immediately clear if and what role the board might play in such a transfer. It is likely that subordinate rules and regulations that follow the DPDPA will shed some clarity on this issue.

Additionally, there are sector-specific regulations such as those governing payment data (which falls under personal data) where the RBI's approval is required before data is shared with a foreign regulator.

19. 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 like 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. The CERT-In Directions also contain certain compliances with respect to data maintenance and its potential disclosure to regulators in a time-bound manner – again, it is important to evaluate any request from a regulator to verify if the request is intra vires, and to also be aware of the ways in which the request – if ultra vires – can be challenged.

ENFORCEMENT AND SANCTIONS

20. What are the sanctions and penalties for non-compliance with data protection laws?

Until now, the sanctions and penalties in relation to personal data were governed by the IT Act, which provided for imprisonment of up to three years and/or a fine of up to 500,000 rupees, depending on the non-compliance.

Under the DPDPA, the penalty provisions have been significantly enhanced and now there is a possibility of fines as high as up to 2.5 billion rupees being imposed in cases of failure to take reasonable security safeguards. The determination of the penalty would be done by the Data Protection Board of India based on factors such as nature, gravity and duration of breach; repetitive nature of breach, and this decision can be challenged.

RELEVANT MATERIALS

21. Provide a list of relevant materials, including any decisions or guidance of the data protection authority in your jurisdiction regarding internal and external investigations, and transfers to regulators or enforcement authorities within and outside your jurisdiction.

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

- Digital Data Protection Act 2023;
- CERT-In Directions;
- Justice K.S Puttaswami & Anr. vs. 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; and
- Insurance Regulatory And Development Authority Of India (Third Party Administrators – Health Services) Regulations, 2016.

Manavi Jain

G&W Legal

Manavi Jain is a managing associate at G&W Legal. She is part of the firm's technology, media and IP practice, with formidable experience in cross-border data protection and privacy issues. She regularly assists clients with issues traversing tech and IP, technology and data transfers, etc, and recently advised a large multinational on regulatory matters surrounding inter-company cross-border sharing of personal data.

Hardik Choudhary

G&W Legal

Hardik is an associate at G&W Legal and is part of the firm's tech, media and IP practice. Outside of his experience working on a broad range of contentious and non-contentious IP matters, Hardik has a strong interest in data protection and privacy. He regularly assists clients on issues involving data transfer, regulatory compliance and reporting obligations.

Disha Mohanty

G&W Legal

Disha Mohanty is a partner at G&W Legal and co-head of the firm's anti-corruption, white-collar and employment law practice.

She has over a decade of experience assisting clients across industries undertake internal investigations, often as part of larger global FCPA audits, as well as advising on money-laundering, fraud and corporate governance issues in India. She also has extensive experience in conducting compliance assessment and training programmes for the Indian subsidiaries of multinationals to ensure compliance with foreign anti-bribery legislation such as the FCPA, UK Bribery Act and Sapin-II Law. Disha's investigations experience includes issues involving employee misconduct, embezzlement, kickbacks and harassment, on behalf of clients across sectors. She also provides guidance to organisations on revamping employment practices, termination procedures and codes of conduct, and often assists with employment-related due diligence.

Representatively, Disha recently conducted an independent investigation into sexual harassment and labour law-related complaints for a multination retail company; has led an investigation into a US entity's Indian affiliate concerning internal financial controls and HR violations; advised one of the world's largest aerospace companies on Indian defence procurement norms and regulations involving intermediaries and government dealings; and represented an international non-profit in an investigation into allegations of bribery for obtaining FCPA registration.

Dhruv Singh

G&W Legal

Dhruv Singh (CIPP/E); counsel - Privacy and Regulatory Affairs, G & W Legal, India

Dhruv is a privacy, tech and media lawyer with over a decade of experience. He deals with novel issues on AIGC's implications under Indian laws on IT, privacy and copyright, as well as intermediary liability for social media platforms. Most recently, he was product counsel for a leading global social media company and dealt with multiple issues on content moderation, intermediary liability, as well as concerns on 'national security' raised by the Indian government. He has an active interest in public policy and has assisted trade associations in comprehending the impact of newly proposed regulations in the area of privacy. Dhruv also has a wealth of experience dealing with issues of freedom of speech and expression and has assisted leading corporations and celebrities deal successfully with well-publicised litigation.

Dhruv greatly enjoys providing his services pro bono to environmental NGOs and animal welfare groups.

G&W Legal

Combining the experience of big law with the expertise of a boutique, G&W Legal is a full-service business law firm that assists its clients at the intersection of law and pragmatism. Our team spans diverse subject matters and industries, using its robust skill set to become greater than the sum of its parts.

As the world grows smaller in the information age, business is no longer limited by borders. We understand this well, and provide our clients with advice and representation on every aspect of expanding into and doing business in India. Our attorneys bring a rich body of knowledge and accomplishment across (often intersecting) areas such as: corporate/commercial; intellectual property, tech and media; privacy and data protection; corporate governance, ethics, compliance and investigations; franchising and distribution; advertising and marketing; product liability and consumer protection; international trade; foreign investment; private equity and venture capital; employment; government contracts; corporate restructuring; antitrust or competition; regulatory affairs; real estate; dispute resolution; and everything in between.

C-9 / 9624,
Vasant Kunj,
New Delhi - 110070
Tel: +91-11-61348306

www.gnwlegal.com

Manavi Jain
manavi.jain@gnwlegal.com

Hardik Choudhary
hardik.choudhary@gnwlegal.com

Disha Mohanty
dishamohanty@gnwlegal.com

Dhruv Singh
dhruv@gnwlegal.com