GIR KNOW HOW DATA PRIVACY & TRANSFER IN INVESTIGATIONS

India

Disha Mohanty, Arjun Khurana
and Meghna Arora
G&W Legal

OCTOBER 2021

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?

There is currently no dedicated data protection legislation in India. Data, in general, is governed by the Information Technology Act 2000 (IT Act), which is the umbrella legislation covering several matters relating to IT activities, cybercrimes and security and the like, and under which rules such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) have been framed. The IT Act, among other things, imposes an obligation on entities dealing with sensitive personal data to adopt 'reasonable security practices and procedures', and provides for compensation in cases of harm to data subjects. The SPDI Rules, on the other hand, are the most comprehensive Indian regulation dealing with personal data for the moment. Apart from providing the operating definition of 'sensitive personal data or information' (SPDI), the SPDI Rules regulate the collection, processing, disclosure, transfer and security of SPDI – all of which can be relevant for cross-border investigations. The SPDI Rules will thus, for the most part, be the focus of this chapter.

Certain sector-specific laws in fields such as banking, insurance, medicine/healthcare and telecom (which will be discussed later in this chapter) also impose obligations regarding the confidentiality of personal data and its use for limited, pre-agreed or prescribed purposes. 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 Puttawamy judgment engaged with the concept of 'informational privacy' and acknowledged an individual's right to 'control the dissemination of personal information'.

Dedicated legislation and framework for data protection has long been pending in India, and while a Personal Data Protection Bill (PDP Bill) has been tabled in parliament, it is yet to become law. In its most recent iteration, the PDP Bill, inter alia, seeks to make three broad categories (ie, personal data, sensitive personal data and critical personal data) with gradient obligations applying to each. The PDP Bill has, however, been heavily debated and has rightly come under criticism from various quarters, on issues ranging from protectionism, arbitrariness, governmental overreach and surveillance implications.

2. What other laws and regulations, besides data protection laws, may prevent data sharing in the context of an investigation?

As things stand, there is no blanket prohibition on the transfer of personal data outside India under the SPDI Rules. SPDI may be freely transferred outside India, provided certain conditions are met, which include obtaining the data subject's consent, or having an underlying contract with the data subject that necessitates such a transfer; and the transferee ensuring the same degree of data protection as the transferor.

Apart from the SPDI Rules, which primarily govern personal data, 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.

For instance, in the banking sector, the storage and transfer of financial data are separately regulated. The Reserve Bank of India (RBI), Indian'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.

Other sectoral examples include the Insurance Regulatory and Development Authority of India (Third Party Administrators – Health Services) Regulations 2016, 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.

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

Under the SPDI Rules, 'personal information' is any information that, directly or indirectly, in combination with other information available or likely to be available with a body corporate, can identify a 'natural person'. The explicit reference to 'natural person' in this definition implies that data belonging to legal persons such as companies may not be considered 'personal data' within the regulations. Under the same Rules, SPDI is a subset of personal data that includes 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. Understandably, SPDI is subject to a higher degree of care and protection, and is thus regulated more stringently, than non-personal data or personal information.

The PDP Bill, in its most recent iteration, retains some of the current categorisation but goes a step further. It divides such data into three heads – personal data, sensitive personal data, 'critical personal data'. While both 'personal data' and 'sensitive personal data' are defined within the PDP Bill, 'critical personal data' (which would entail the strictest obligations in terms of data localisation and other factors) is a wildcard category; any personal data may be notified by the Indian government as critical personal data.

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?

Data protection provisions under the IT Act may get triggered in cases such as misuse of personal data, failure to implement reasonable security practices, wrongful disclosure and violation of contractual terms involving personal data. The SPDI Rules, on the other hand, apply to all entities (or their representatives) involved in collecting, storing, processing, transferring, disclosing or dealing with personal information (including SPDI).

Unlike more mature legislation such as the GDPR, the SPDI Rules do not define or delineate data controllers, data processors or data subjects. The two primary distinctions under the SPDI Rules are 'body corporate' (which includes any association of individuals engaged in commercial or professional activities, and effectively covers both controllers and processors) and 'provider' (ie,', the data subject). The PDP Bill proposes to adopt a more nuanced application, with 'data fiduciaries' (similar to data controllers), 'data processors' and 'data principals' (ie, data subject) all separately defined.

In terms of jurisdiction, the IT Act extends not just to the territory of India but also applies to offences committed by any person – regardless of nationality – outside India, so long as the offence was committed using a computer, network or system located within India. The PDP Bill proposes an even broader application and seeks to also include any data fiduciary or processor outside India that handles personal data in connection with a business conducted in India.

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

The SPDI Rules set out certain minimum requirements wherever the collection and processing of personal data is involved, and the IT Act penalises companies for improper disclosures and failure to implement security standards. In the context of cross-border investigations – especially post covid-19, with investigations going almost entirely remote – these 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. Such ESI will often include employees' personal information and, depending on the nature of business a client and/or target are involved in, could also include SPDI or other regulated data belonging to customers.

When dealing with data transfers in the course of an investigation, it is imperative to ensure that both the transferor and the transferee are fulfilling their respective obligations, in addition to the transfer itself being compliant with the SPDI Rules. The transferor, for instance – as the entity that collected or possesses the personal data in the first place – can be subject to a range of obligations that include having a publicly available privacy policy, a dedicated Grievance Officer, and 'reasonable security practices and procedure (the SPDI Rules mention IS/ISO/IEC 27001 as an approved standard). For the collection of data to be above board, it is essential that the data subject be fully aware not just of the fact that data is being collected, but also of the purpose of collection, the intended recipients, and the name and address of the entity collecting and retaining the SPDI.

Assuming that the transferor is compliant with the law, a cross-border data transfer entails two fundamental requirements: (i) that the transferee practices the same level of data protection as the transferor; and (ii) that the consent of the data subject be obtained (blanket consent for lawful transfers are sometimes already included in contracts with employees).

Companies typically have internal policies in place to restrict or minimise the use of office email and computers for personal purposes, since the privacy or protection of personal information stored on office assets cannot always be guaranteed. However, covid-19 and indefinite remote-work arrangements have created new challenges that often make such policies difficult to monitor and implement. Therefore, where the ESI or other data being collected for the purpose of an investigation includes (or could conceivably include) SPDI, organisations can consider having data subjects specifically provide their consent – simple email confirmations can be enough as well. Once the data is transferred, the recipients – this could include a foreign parent company, external counsel, forensic auditors – are also under an obligation to not disclose the data any further.

6. Identify the data protection requirements relevant to a company carrying out an internal investigation and to a party assisting with an investigation.

Although parties assisting with an investigation – such as external law firms, auditors etc. – will always be the transferees in a data transfer, the company carrying out an internal investigation could either be a transferor or transferee depending on the situation. The principal obligations under the SPDI Rules are on the entity that collected data directly from the data subject, as it would be their responsibility to obtain consent and keep the data subject fully informed about the purpose of collection and other particulars in the first instance. In a cross-border investigation, however, the target entity in India will typically be the one that collected and possess the SPDI, while the foreign parent, affiliate or entity will usually be the one commissioning the investigation and will thus be the transferee. Nonetheless, under the SPDI Rules, the transferee is also expected to practice the same degree of data protection as the transferor, so the obligations to that extent will apply. In so far as requirements may apply differently to the transferor (ie, the company carrying out the investigation) and the transferee (foreign entities, external counsel), please refer to the immediately preceding discussion under question 5.

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 subject's consent is mandatory for the collection of SPDI and for processing or transferring data as part of an investigation. There are limited exceptions where data can be disclosed without the subject's prior consent; these are discussed later in this chapter.

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

Although the data subject's consent is mandatory, this does not always mean that consent has to be specifically 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, such as an employment agreement – so long as that contract contains language specifying the purposes to which the data collection extends, such as company audits and internal investigations. That said, given the nature of data involved and to limit the company's risk exposure, obtaining consent explicitly for the purpose of an investigation may be considered as a part of best practices.

9. Is consent given by employees likely to be valid in an investigation carried out by their employer?

Consent must be obtained from the ultimate data subject, and a precondition to that consent is that the subject be made aware of the purpose of collection and the intended recipients of the SPDI. As such, in an investigation commissioned by an employer, the employee's consent will be valid only if it was given for the specific purpose of an investigation – whether at the time of investigation or earlier, through an appropriately worded contract. In other words, an employer cannot assume blanket consent on behalf of an employee.

The PDP Bill, however, proposes to create a more gradient obligation where non-sensitive personal data of an employee may be processed by an employer without obtaining express consent, for specific purposes such as recruitment and termination, performance assessment, 'provision of any service' to an employee. It remains to be seen, if or when India adopts a standalone data protection legislation, whether any of these exclusions are broad enough to include investigations.

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 SPDI Rules require a data subject's consent to be taken in writing (this includes emails) before collecting any sensitive personal information or data, and mandate that the data subject be made aware of the purpose for which their data is being collected. As such, while it is indeed possible for data subjects to consent to processing in advance – for instance, through terms in their contracts with the controller or processor – such consent would only be valid till the time their data is being used for the purpose for which it was collected. In theory, a company's standard contract terms could include the possibility of the data subject's SPDI being used in the context of audits, investigations, etc. That said, data subjects must also be informed about the intended recipients of their data and, in the context of investigations, external parties such as law firms and auditors are rarely decided so far in advance. Therefore, as soon as the company's use of a data subject's SPDI is exceeding the remit for which consent was initially obtained, fresh consent for the applicable additional purposes should be secured.

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 existing framework, data subjects have the right to review, verify and have corrected any personal information or SPDI provided by them. In fact, the SPDI Rules give data subjects the right to not just deny, but to provide and subsequently withdraw (in writing) their consent for collection or processing of SPDI as well – and this will apply equally in the context of an investigation. That said, in cases of denial or withdrawal of consent, a company also has the option of not providing the data subject with the good or services for which their data was sought.

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?

There are certain specific requirements to consider where third parties (for example, accounting firms or auditors) are appointed to process personal data in connection with an investigation. The most important one is consent – disclosure of SPDI to any such third party requires the data subject's prior consent (unless of course there is a lawful exception).

Another important requirement for companies is to make sure that the third parties they're engaging – who will likely be recipients of SPDI belonging to several data subjects – are subject to the same level of data protection that the company itself is practising, and they are maintaining reasonable security practices as mandated under the SPDI Rules. For example, the International Standard (IS/ISO/IEC 27001) is considered an appropriate standard under SPDI Rules, and the Bureau of Indian Standards has recently issued IS 17428.1 for data privacy and assurance as well.

Broadly, 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 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 for the purpose of providing legal advice?

Under current laws, there is no express provision on the kinds of entities SPDI should or shouldn't be shared with. As such, data can be shared with law firms, provided the data transfer is compliant with the applicable regulations.

14. What is the position and status of law firms under data protection laws? Are law firms directly accountable for data processing under data protection laws, or is responsibility for processing by law firms shared between the law firm and the client?

As discussed above, the current SPDI Rules do not delineate data controllers and data processors, with the term 'body corporate' being wide enough to include both functions. While there are no specific provisions on how a law firm will be treated, it may be considered at par with an authorised third party to which a company can transfer data (provided of course that the transfer is for lawful purposes, with the data subject's consent and other applicable conditions under the SPDI Rules are met). To that end, the provisions of the SPDI Rules regarding data transfer may be interpreted to put the onus on the transferor to ensure that data is shared with a transferee (such as a law firm) that practises an equal level of data protection.

Separately, Indian law prohibits attorneys from disclosing to third parties any communication received from or advice given to clients and any documents received in the course of their professional engagement, unless, of course, a client expressly consents to such disclosure. Therefore, any information or documents shared with external law firms during an investigation may additionally be protected by attorney-client privilege, with limited exceptions in cases where privilege does not apply (eg, data shared in furtherance of an illegal purpose).

15. What is the position and status of legal process outsourcing firms under data protection laws?

Similar to question 14, legal process outsourcing firms (LPO) would be considered a third party with whom a company can share data, provided the transfer is compliant with the SPDI Rules. Whether or not the additional protection of privilege will apply to an LPO may depend on the nature and scope of the engagement.

16. 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.

17. 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?

Sharing data subjects' SPDI overseas is permissible, provided that the transferee located outside India is subject to the same levels of data protection as applicable to the disclosing company in India. Such a cross-border flow of data is possible only if the transfer is necessary for the performance of a lawful contract between the disclosing company (or its representative) and the data subject, or in cases where the data subject has expressly consented to such transfer. It is important to note that these obligations are triggered only where SPDI is involved, and do not apply to non-personal data. That said, whether or not any other sector-specific regulations apply to such a transfer may also depend on the nature of documents that are being sent abroad for review.

18. 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.

TRANSFER TO REGULATORS OR ENFORCEMENT AUTHORITIES

19. Under what circumstances is the transfer of personal data to regulators or enforcement authorities within your jurisdiction permissible?

The SPDI Rules do not allow for the disclosure of transfer of personal data without the data subject's consent, except where the disclosure is made to a competent government agency for the purpose

of identity verification, or for the prevention, detection, investigation, prosecution or punishment of offences (including 'cyber incidents'). In such cases, the relevant government agency must make a written request to the entity in possession of the SPDI, stating the purpose of seeking data and agreeing not to publish or disclose it further.

20. Under what circumstances is the transfer of personal data held within your jurisdiction to regulators or enforcement authorities in another country permissible?

While there is no dedicated data protection authority under the current regime, the SPDI Rules as they stand are silent on the transfer of data to foreign regulators or enforcement authorities. That said, there are sector-specific regulations such as those governing payment data (which may include SPDI), where the RBI's approval is required before data is shared with a foreign regulator.

21. What are some recommended steps to take on receipt of a request from a regulator for disclosure of personal data?

Apart from what has already been touched upon in this chapter, it might be helpful for a company to assess if it qualifies as an 'intermediary' 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 cyber security incidents – within 72 hours.

ENFORCEMENT AND SANCTIONS

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

Sanctions for non-compliance with data protection laws are currently governed under the IT Act.

During the stage of data extraction or collation or transfer in an investigation for instance, if the disclosing company fails to implement or maintain reasonable security practices and procedures and in doing so cause wrongful loss or gain to anyone, it will be liable to compensate the affected person.

The IT Act further penalises wrongful disclosure of information (ie, without the consent of the person concerned) in breach of a lawful contract, by providing for imprisonment up to three years and/or a fine up to 500,000 rupees.

RELEVANT MATERIALS

23. 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:

- Justice K.S Puttaswami & Anr v Union of India, Writ Petition (Civil) No. 494 OF 2012 (https://indiankanoon.org/doc/127517806/);
- The Information Technology Act 2000 (https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=);

- Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (https://www.meity.gov.in/writereaddata/files/GSR313E_10511%281%29_0.pdf);
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 (https://www.meity.gov.in/writereaddata/files/Intermediary_Guidelines_and_Digital_Media_Ethics_Code_Rules-2021.pdf);
- RBI Circular on Storage of Payment System Data (https://www.rbi.org.in/commonman/english/scripts/FAQs.aspx?Id=2995);
- Personal Data Protection Bill 2019 (http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf); and
- Insurance Regulatory And Development Authority of India (Third Party Administrators – Health Services) Regulations 2016
- (https://www.irdai.gov.in/ADMINCMS/cms/Uploadedfiles/Regulations/Consolidated/IRDAI%20TPA%20consolidated%20Reg%20may%202020.pdf)

Disha Mohanty

G&W Legal

Disha Mohanty is a principal 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 FCRA registration.

Arjun Khurana

G&W Legal

Arjun Khurana is a principal at G&W Legal. He chairs the firm's technology and dispute resolution practices, with an additional focus on investigations.

Arjun advises clients on complex technology and content licensing transactions; counsels corporations on data protection and privacy issues; conducts internal investigations, with expertise in matters involving misuse and theft of IP, fraud and privacy, and special emphasis on crisis comms and mitigation strategies; and regularly represents multinationals in commercial disputes before Indian courts.

Notably, Arjun acts for a global media network in high-value commercial litigation; recently advised an international non-profit on data sharing issues and transfer of potentially sensitive data outside India as part of a cross-border investigation; led an internal investigation on behalf one of the world's most recognisable brands into issues involving fraud, identity theft and forgery; advised a multinational manufacturing and automation conglomerate regarding the theft and misuse of proprietary and confidential information by ex-employees in India; assisted an international fashion retailer with setting up a tech hub in India; advised global online marketplaces on regulatory compliance and intermediary safe harbours, private label arrangements, privacy policies and terms of use; and has counselled a major developer on creating an e-sports and gaming portal in India.

Meghna Arora

G&W Legal

Meghna Arora is an associate at G&W Legal. She is part of the firm's technology and IP practices, with an interest in data protection and privacy issues. Meghna recently assisted an Asian conglomerate with crafting a privacy policy and allied procedures for their Indian business.

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

Disha Mohanty
dishamohanty@gnwlegal.com

Arjun Khurana
arjun@gnwlegal.com

Meghna Arora
meghnaarora@gnwlegal.com