Chambers AND PARTNERS

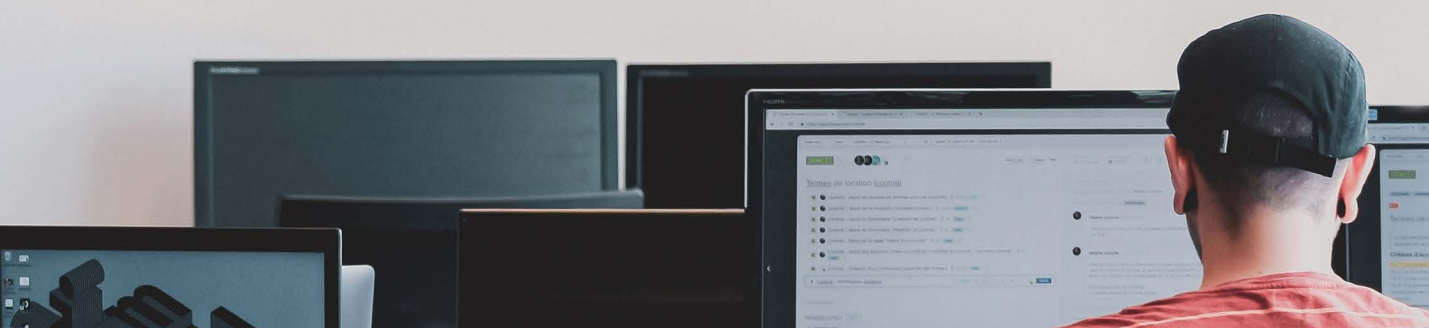
CHAMBERS GLOBAL PRACTICE GUIDES

Technology & Outsourcing 2023

Definitive global law guides offering comparative analysis from top-ranked lawyers

India: Law & Practice and Trends & Developments

Anoop Narayanan
ANA Law Group



INDIA

Law and Practice

Contributed by:
Anoop Narayanan
ANA Law Group

Contents

1. Market Conditions p.4
1.1 IT Outsourcing p.4
1.2 Business Process Outsourcing (BPO) p.4
1.3 New Technology p.4
1.4 Outsourced Services p.5

2. Regulatory Environment p.5
2.1 Restrictions on Technology Transactions or Outsourcing p.5
2.2 Industry-Specific Restrictions p.5
2.3 Restrictions on Data Processing or Data Security p.6

3. Model Outsourcing Contracts p.7
3.1 Standard Contract Model p.7
3.2 Alternative Contract Models p.7
3.3 Digital Transformation p.8

4. Contract Terms p.8
4.1 Customer Protections p.8
4.2 Termination p.12
4.3 Liability p.12
4.4 Implied Terms p.13
4.5 Data Protection and Cybersecurity p.13
4.6 Performance Measurement and Management p.13
4.7 Digital Transformation p.14

5. Employment Matters p.14
5.1 Employee Transfers p.14
5.2 Role of Trade Unions or Workers Councils p.14
5.3 Offshore, Nearshore and Onshore p.15
5.4 Remote Working p.15

ANA Law Group is a full-service Mumbai-based law firm, with a team of experienced and committed professionals who have broad industry knowledge and specialise in a wide spectrum of laws. With prominent cross-border exposure and a solution-oriented approach, the firm provides significant value to clients internationally, as each client receives the attention required to achieve practical legal solutions. Some of the firm's key practice areas include commercial contracts, IT and outsourcing transactions, employment law, data privacy, IP, and digital media.

Author

Anoop Narayanan is the founder of ANA Law Group and has been in practice for nearly 30 years. Anoop is a distinguished commercial, TMT, IP and employment law expert, with significant experience in the field of outsourcing to India. He has worked on projects rolling out some large multinational technology companies in India, as well as on several India-bound outsourcing transactions with major Indian IT companies. Anoop also assisted many multinational companies in setting up their data centres in India and provided related regulatory advice. He regularly advises many multinational banks on Indian data protection law and related matters in connection with outsourcing transactions.

ANA Law Group

7th Floor
Keshava
Bandra Kurla Complex
Bandra East
Mumbai 400 051
India

Tel: +91 22 6112 8484
Email: mailbox@anaassociates.com
Web: www.anaassociates.com

ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES

1. Market Conditions

1.1 IT Outsourcing

India's IT outsourcing industry is still considered one of the largest exporters of IT and business process outsourcing services – something that has been on an increasing growth curve throughout the past several decades. Information technology and business process outsourcing services reportedly constitute approximately 60% of India's service exports and are estimated to be the largest component of India's service exports.

While the early days may have been focused on catering to businesses that reached out to India for cost reduction or to address manpower concerns, the current scenario is significantly different from how it started. IT outsourcing to India currently encompasses anything that one can relate to any kind of advanced technology development. The world reaches out to India for its outsourcing industry's advanced skills and capabilities for support across the globe. Today, Indian captive subsidiaries and third-party vendors support most of the emerging and advanced technology for multinational corporations in the areas of AI, cloud computing, and blockchain.

1.2 Business Process Outsourcing (BPO)

Although the COVID-19 situation created confusion among businesses globally as well as the Indian information technology services industry and workforce in the early days, it surprisingly worked to the advantage of the Indian IT industry. India's domestic consumption for IT services experienced an unprecedented growth, starting from the remote working platforms and spreading to e-commerce, followed by the increased demand for outsourced support of various kinds to global businesses. Many large industries had no choice other than to adopt more and more digital solutions during the pandemic.

One of the key factors behind this development is the high-quality technical skills that today's Indian IT industry offers in the fields of AI, medical devices and pharmaceuticals, gaming, movies, robotics, etc. Another positive trend is that many large global corporations now consider India the preferred location in which to set up their global capabilities centres to support cloud management, data analytics and other high-tech services (as well as traditional services such as software development testing and support).

Further, the remote working that began during the pandemic – followed by the hybrid working model – became very common practice globally and is expected to continue as a preferred working model for employees as well as employers. This has resulted in the demand for technological solutions to support such efficient hybrid work models. Post-pandemic, therefore, two of COVID-19's major contributions (the work-from-home/hybrid work models) have kept the Indian IT outsourcing companies busy developing solutions and support for a variety of businesses across the globe.

1.3 New Technology

New technologies have had a very positive impact on the outsourcing industry. While some of these technologies are intended to reduce human interface and operate as an internal solution for various business functions, the development in the new technology sector has been exponential and continues as an ever-expanding ecosystem. This has opened up new opportunities for research, development, support and maintenance of the new technologies.

The large and highly qualified talent pool available in India is capable of handling all kinds of requirements in the field of new technology and has positioned India as the most preferred jurisdiction for the global clients. Additionally, the language skills, time zone advantage, a well-established common-law-based legal system and geopolitical acceptance also work to India's advantage in attracting global companies. The Indian IT outsourcing industry also supports some of the large Indian corporations –s ome of which are globally appreciated innovators as well as being leading businesses in their respective sectors.

However, the ability to deploy insourced AI and automation for a variety of technology solutions results in companies assessing whether certain kinds of IT services should be outsourced to a third-party service provider or not. Notwithstanding, the scale and coverage of new technologies is likely to keep the Indian service providers engaged.

Further, there has been a lot of interest in the field of cloud-based outsourcing services as businesses have been looking for cost-effective options, along with a need-based increase in capacity. The AI-based technologies have had an impact all across the IT and outsourcing industry. On the one hand, the industry is involved in developing AI technologies for Indian as well as international corporations. At the same time, sectors such as data analytics benefit significantly from the use of AI and the outsourced service providers are engaged in licensing such technologies from established providers as well as developing solutions to increase their overall efficiency.

1.4 Outsourced Services

IT outsourcing to India progressed a lot from its origins as a cost-saving alternative. Currently, all kinds of industries (including IT and manufacturing) and professional service providers such as accounting firms and law firms avail the services of the Indian outsourcing industry. The nature of services outsourced varies from support services to high-end search and product development. The services outsourced to India include traditional software development and testing, cloud services, blockchain, analytics, digital transformation, call centre services, legal and accounting process outsourcing, back-office support, digital marketing, and more.

2. Regulatory Environment

2.1 Restrictions on Technology Transactions or Outsourcing

There are no general regulatory restrictions in respect of technology transactions or outsourcing in India. However, when it comes to outsourcing in Indian banking or the financial sector, India's central bank (the Reserve Bank of India)'s regulations mandate certain compliances concerning the functions that can be outsourced (eg, outsourcing of core functions) and security measures will apply for the appropriate use of contracts and technology. India's insurance regulator and the capital markets regulator also have similar regulations applicable to outsourcing in their respective sectors.

2.2 Industry-Specific Restrictions

A major industry-specific regulation in the financial sector is the Reserve Bank of India's Master Direction on Outsourcing of Information Technology Services 2023 (the "RBI Outsourcing Directions"). These guidelines apply to the outsourcing of IT services by banks and financial

institutions, subject to certain exceptions. These guidelines have been introduced to ensure protection of customer interests as well as regulatory compliance. The major compliance requirements are:

- to carry out due diligence on the outsourced service providers;
- adequate governance in the performance of the outsourced activity (for which the institution's key management must be responsible);
- a proper grievance redressal mechanism in case of deficiencies in the outsourced service;
- a comprehensive outsourcing agreement with the service provider or the financial institution to exercise control over the outsourced activities, if required.

The banks also have certain reporting obligations with regard to the outsourcing of some functions. There are similar compliance requirements for cross-border outsourcing as well.

Similarly, the Securities and Exchange Board India (SEBI) and the Insurance Regulatory and Development Authority of India (IRDAI) had also issued sector-specific guidelines in respect of IT outsourcing to ensure confidentiality, data safety and security. These regulations also restrict the outsourcing of core functions.

2.3 Restrictions on Data Processing or Data Security

India recently enacted its data privacy legislation, the Digital Personal Data Protection Act 2023 (DPDPA). It is anticipated that various provisions of the DPDPA will be enforced in a phased manner and that the legislation seeks compliance by large technology companies in the initial stages. Although there no specific timelines have been prescribed as yet, the smaller companies are likely to receive some more time for total compliance. This law will apply to almost all kinds of data processing in India.

The statute mandates a data subject's specific and express compliance (except in the case of excluded legitimate-use categories). Further, a data controller will be responsible for ensuring reasonable technical and security measures so as to prevent data breaches. Additionally, the data controllers must report any kind of data breaches or cyber-incidents to a government authority – namely, the Indian computer emergency response team (CERT-In). The timelines prescribed for reporting cyber-incidents are sector-specific as well – for example, a shorter timeline is precribed for the banking and financial sector. Other businesses also find the reporting timelines to be very short and find it difficult to determine what kind of incidents should be mandatorily reported. Given that almost all businesses in India can be exposed to cybersecurity or other kinds of cyber-incidents on a daily basis, businesses are adopting a case-to-case-based approach to deciding about such reporting.

Although the transfer of personal data out of India is permitted subject to the prescribed compliances, the government can restrict such data transfers to specific (blacklisted) countries under the DPDPA. However, the government has not as yet prepared such a list of countries.

As regards the data of children, parental consent is mandatory, irrespective of whether the data controller is engaged in a business or activity specifically targeting children.

The foregoing provisions of the DPDPA will apply to international businesses operating in India or through their outsourced providers when processing Indian personal data. In terms of com-

pliance, given that all the major corporations (as well as the large Indian outsourced service providers) already implemented GDPR compliance measures several years ago, a comparative analysis of compliance requirements may be appropriate from the DPDPA perspective.

3. Model Outsourcing Contracts

3.1 Standard Contract Model

The standard contract models followed either a third-party service provider outsourcing, a captive unit, or a Build-Operate-Transfer (BOT) model. Many international businesses commence their initial outsourcing to India through third-party service providers.

A captive unit is normally established by setting up a wholly owned subsidiary in India. Although setting up a captive unit and the associated compliances involve more effort for a customer, the customer can ultimately be in charge of the complete operations of its India captive outsourcing centre. This model provides more transparency, protection of confidential information and IP, and also the ability to implement a customer's own protocols within its captive Indian outsourcing centre.

Another preferred outsourcing model in India is the BOT model, which chosen more for the outsourcing of a company's core functions. A BOT model is suitable for companies that are unsure of their outsourcing plans in the long term. In such cases, the BOT model helps them to have a facility developed in India according to their specifications, as well as the flexibility to either acquire it at a specified date or exit. However, this model has its associated issues as well. For example, the cost of operations can be higher than in a third-party outsourcing and comparable to that of a captive centre. At the point of transfer of the BOT centre to the customer, the customer will thereafter have to comply with various Indian real estate, taxation, employment and other similar legislations applicable to the transfer.

Additionally, as opposed to the initial perception that the IT outsourcing industry involves projects outsourced from overseas jurisdictions, domestic outsourcing is also significant part of the IT outsourcing industry today. Domestic companies across all industry sectors contribute to a large amount of the onshore outsourcing projects in India.

Similarly, many international companies (as well as Indian companies) frequently adopt the staff augmentation model whenever there is need for additional resources. Companies consider this a more cost-effective and easy-to-manage model than a dedicated team-based outsourcing, unless their products are of a long-term nature.

Project-based outsourcing models are also very popular in India. A clear, well-drafted contract that clearly identifies the terms and conditions, remedies in case of default or delays, audit rights, and a reputable outsourcing partner can make the project-based models easy and effective.

3.2 Alternative Contract Models

A joint venture between a customer and the service provider establishes an outsourcing service centre, yet can provide equal participation and control to a customer. However, this is not a very commonly used model for outsourcing to India as the purpose of most India-bound outsourcing transactions is to procure services for a customer's own consumption. This model may be more appropriate if the customer and service

provider want to operate jointly and sell their services to outside entities, in addition to their own consumption.

Multi-sourcing models may be appropriate in certain cases if the kind of services outsourced can be procured from different vendors and without the need of synchronised outputs by the vendors. Although this model has the ability to procure services from multiple vendors, co-ordination between the vendors and management of projects and timelines can be cumbersome. Given that the other existing outsourcing models have been tested and well established over several years, multi-sourcing does not appear to be a commonly used model.

3.3 Digital Transformation

Digital transformation, including the adoption of cloud computing, software as a service (SaaS), and infrastructure as a service (IaaS), had a significant impact on outsourcing contract models in India.

The introduction of these platforms has persuaded businesses to adopt service-based models as opposed to traditional labor-based models. Businesses appear to be more comfortable with pay-per-use arrangements, as opposed to outsourcing based on full-time resources. Similarly, businesses are adopting pay-per-use pricing models in outsourcing contracts, where clients pay only for the resources they use, thereby creating cost-effective outsourcing models in India.

Digital transformation has necessitated more flexible and industry-responsive outsourcing contract models in India. These new and evolving models focus more on services, data security, and adaptability to meet the changing needs of the business landscape. The international customers outsourcing to India, as well as the Indian companies adopting the digital transformation, may have to focus more on their contract negotiations in order to benefit from the digital transformation.

In the past few years, the Indian outsourcing industry has witnessed significant growth in development and support of digital solutions. This is mainly because of the businesses' demand for digital transformation in order to reach out to the consumers in a more attractive cost-effective and interactive manner. Social media content creation and management, app developments, data analytics, etc, contribute as a sizeable complement of the digital transformation initiatives.

The businesses prefer outsourcing models for digital transformation because the key resources within an organisation need not be fully involved in management of such projects. Therefore, while an organisation's human resources focus on their core competencies, an expert outsourced service provider can add a lot more value to a business's requirements in the field of digital transformation – often at a much lower cost and with a faster turnaround as well.

4. Contract Terms

4.1 Customer Protections

At the outset, customer protections can be ensured through a well-drafted contract of international standards. The remedies can be availed through contractual, statutory and common law provisions.

The key contractual provisions are representations and warranties from the vendor, confirming its:

- authority to contract and perform the obligations under the contract;
- principal-to-principal contract arrangement;
- knowledge and skill to render the services;
- obligation not to breach various provisions of the contract;
- responsibility to manage its own business and employees;
- protection of the customer's IP rights and confidential information; and
- provision of services with the agreed quality and timelines.

Further, the following provisions form part of an outsourcing contract to ensure the protection of a customer's rights:

- maintenance of quality;
- audit rights;
- remedies in case of breach;
- indemnity;
- damages as well as liquidated damages;
- assurance of service levels and performance;
- service-level credits;
- business continuity;
- provisions for adequate insurance to be obtained by the service provider;
- provisions for termination and consequences of termination;
- non-compete and non-solicitation provisions;
- dispute resolution provisions;
- choice of forum and choice of the governing law; and
- a well-drafted force majeure clause that excludes events arising from the service provider's defaults or non-compliances.

The customer should be careful to maintain the relationship with the service provider on an arm's length basis by structuring the outsourcing contract on a principal-to-principal basis. Adequate provisions must also be included to ensure the service provider's employees do not get treated in such a manner that they will be able to claim an employment relationship with the customer.

It may also be prudent for a customer to insist that the service provider should not further subcontract the services or should not do so without the customer's prior written approval. While India has a large talent pool of resources working in the IT outsourcing industry, there is significant attrition as well. This results in vendors trying to subcontract their projects to other service providers, which may not always work in the best interests of a customer.

As India has been a favourite destination for global companies for IT activities, research and development, resulting in a variety of IP development, it is imperative that the companies understand the legal and practical aspects to ensure effective ownership of IP developed in India.

In a typical project, the overseas customers ("customers") execute agreements ("development agreements") with their Indian service providers ("service providers") prior to commencement of the projects. In most of these agreements, the service providers confirm that they have assigned and/or agree to assign all service provider-developed IP rights.

However, based on the applicable Indian law and also the practices followed in India, development agreements alone may not ensure the customer's ownership of India-developed IP rights. Therefore, an outsourcing contract must address some practical concerns such as:

- who owns the India-developed works' IP rights;
- how to ensure that the customer owns the IP developed by the service provider;

- the stages of IP development and related ownership; and
- the documents required and the explanation of such documents' necessity.

The IP ownership in India varies under different IP laws - for instance, in the case of an employee-developed copyright, the employer will be the first owner of the copyright. Therefore, the service provider will own its employee-developed copyright. However, this will not apply in case of an independent contractor-developed copyright. As regards patents, the inventor will be the first owner, irrespective of whether they are an employee or a contractor.

In most cases, the standard templates of development agreements normally provide that:

- all the IP developed by the service provider's employees and contractors under the agreement will be assigned to and owned by the customer; or
- the service provider "hereby assigns" (and, in some cases, agrees to assign) the IP developed under the development agreement to the customer.

Nonetheless, the development agreement may not provide for any specific deeds of assignment or other documentation to effect the transfer of IP from the service provider to the customer – although the development agreement may contain an undertaking in that regard.

However, the important legal and practical concern in cases where the service provider promises that its employees and contractors will assign the IP rights to the customer is whether it is advisable to make such assignments directly with the customer and create such contractual relationships between the customer and the service provider's employees and contractors. Further, in cases where the service provider itself promises to assign the IP rights to the customer, the concern is whether the service provider owns all the IP rights in the work product developed by its employees and contractors.

Unless extremely necessary and supported by detailed agreements and documentation, it is better for a customer to avoid direct IP assignment and creation of contract relationships with the service provider's employees and contractors. Therefore, a better option is for the service provider to assign the IP rights to the customer under a two-level IP assignment process. The first level will be between the service provider and its employees and contractors to ensure that the service provider owns the IP in the work product developed. The second level will be between the service provider and the customer under which the service provider will assign the IP rights obtained from its employees and contractors.

Further, the customer and the service provider must agree in the development agreement to execute specific deeds of assignment to assign all the IP rights. A format of the deed of assignment must be agreed upon and preferably a draft should be annexed to the development agreement, broadly identifying the development work to be carried out by the service provider. This will act as prima facie proof of the kind of IP rights that may be developed and that the parties have validly agreed that the customer will own such service provider's developed IP.

The customer, after ensuring that the service provider owns the IP rights developed by its employees and contractors, must ensure that the service provider executes the deeds of assignment in the customer's favour to assign

any copyright, invention, patent, design rights and all other IP that is developed. In order to achieve this, the development agreement between the customer and the service provider should clearly make the service provider liable to ensure that the service provider's contracts with its employees have the above-mentioned provisions for IP protection.

Additionally, under the development agreement, the Indian vendor should provide a power of attorney to the Customer, authorizing the Customer to adopt steps to own the IP rights developed and agreed to be assigned by the Indian vendor in the event the Indian vndor is not available to do so. Similarly, the vendor should also obtain a similar power of attorney from its employees.

The absence of a deed of assignment from the employees and independent contractors to the vendor can cause greater challenges if the vendor's personnel leave the employment in the middle of a partly developed project. This is why there must be a deed of assignment at the beginning of the project, which will broadly identify the nature of work handled by the employees and their agreement to assign this. Thereafter, when the work product/project is complete, the key employees involved in the project must execute another deed of assignment assigning all the IP rights in such work product to the vendor.

Further, in the case of breach of IP or confidentiality obligations by the service provider personnel, the general dispute resolution provisions of the outsourcing contract may not suffice. The customer should obtain specific assurances from the service provider with regard to initiating legal actions against the service provider personnel and also providing adequate information and support in case the customer decides to take charge of such proceedings.

Performance and service levels provisions must be approached seriously. The service provider must agree that the performance of the services will meet or exceed each of the service levels, as may be applicable. Further, service-level credits must be defined as separate from the liquidated damages or penalties - although they can be finally offset against any damages if the customer initiates any proceedings and damages awarded.

Business Continuity and Disaster Recovery

As part of the outsourcing agreement, the service provider must prepare and provide a detailed disaster recovery plan for crisis management and business continuity. The disaster recovery plan must be based on industry practices and include remote performance capabilities for provision of the services in case of a disaster. The parties may also agree to mock disaster recovery exercises once every year.

As data breach can cause irreparable harm to a customer and it may be difficult to estimate the damages in monetary terms, the customer should have the right to seek injunctive relief - irrespective of the arbitration or other dispute resolution mechanism in the agreement. If the service provider personnel breach or threaten to commit a breach of any of the terms and conditions of the outsourcing agreement, the customer shall have the right to seek injunctions against and prosecute such service provider personnel for the breach, in addition to the service provider's right to prosecute them. The service provider must agree to provide all the required assistance to the customer in this regard.

The service provider must agree that any deliverable materials or other softwar/hardware provided as part of the services will not infringe the IP rights of any third party.

The service provider must agree that it will not directly or indirectly participate in any act that constitutes a violation of the United States Foreign Corrupt Practices Act (FCPA), Mexican local laws regarding anti-corruption (eg, the *Ley Federal Anticorrupcion en Contractataciones Publicas*), the UK Bribery Act and all other applicable national and local laws and regulations relating to the subject matter thereof, including both the anti-bribery and accounting provisions of the FCPA.

It is critical to get an agreement from the service provider regarding its key personnel. The parties normally designate a group of service provider employees as critical to the services under an agreement and also ensure such key personnel's consistent quality and availability in providing the services as a material provision.

The customer should carry out detailed background investigations on service provider personnel engaged to provide the services, to the extent permitted by applicable law. Practically, this can be carried out through the service provider, based on a detailed policy and a reputed vendor. The agreement should have detailed provisions confirming that the service provider employees will not be considered as the customer's employees, under any circumstances.

Further, the agreement should also specify that the service provider will be responsible for the payment of compensation (including employment related taxes, federal, state and local income taxes, and workers' compensation) associated with the employment of their employees.

4.2 Termination

One of the major grounds for termination is the material breach of contract. There are practical limitations on comprehensively defining what constitutes material breaches and, as a result, termination on the ground of certain material breaches end up in long discussions. Depending on the nature and scale of the contract, some of them do provide for termination for convenience with a reasonable notice.

Other standard grounds for termination include bankruptcy, a force majeure event, change of control, change of any applicable laws that may impact the rendition of services under the agreement, any adverse regulatory actions against the service provider, and service-level defaults.

The outsourcing agreements normally provide exhaustive post-termination provisions such as transitioning of services to a new service provider. In case the services have to be transitioned because of the service provider's default, many customers do succeed in obtaining an agreement from the service provider to bear the costs for such transitioning. Other provisions include return of customer materials and information.

4.3 Liability

In case of a service provider's breach of the contract, the customer can seek and obtain damages for any direct losses caused as a result of such breach. However, the customer will not be able to succeed in a claim for indirect or consequential damages or loss of profits. Notwithstanding, the parties are free to agree on a quantum of liquidated damages in respect of various breaches or consequences anticipated under the contract. Liquidated damages are a

more practical and preferred option and can be obtained, irrespective of whether the party proves that it has suffered actual damage or loss. In many cases, the liquidated damages are quantified based on the fees paid to the service provider or the value of a certain kind of project.

4.4 Implied Terms

In India, there are no implied terms that are relevant to technology outsourcing transactions.

4.5 Data Protection and Cybersecurity

Please refer to **2.3 Restrictions on Data Processing or Data Security**. Additionally, depending on the nature and size of the outsourced operations, customers demand a variety of cybersecurity and data protection safeguards from the service providers. The services agreements normally include extensive provisions mandating the service provider's obligations to ensure that the customer's confidential information, trade secrets, business plans, and information regarding IP are handled with utmost care and only in the manner and as required for the provision of services as specified in the services agreement. Customers also require that the service provider's personnel must execute non-disclosure agreements to confirm their compliance with the service provider's confidentiality and security obligations under the services agreement.

As regards business continuity in case of cyber-incidents, any service providers who have alternate arrangements and locations to maintain unrestricted provision of services. This has almost become a standard requirement in large-scale outsourcing contracts.

Further, the majority of the Indian outsourcing service providers' customers include any subsidiaries of multinational companies as well as large Indian corporations. These businesses include e-commerce, healthcare companies, financial institutions and technology solution providers, as well as social media platforms. All these businesses will be involved in processing personal data of Indian customers and, therefore, the outsourcing companies will also have to comply with the various requirements of the DPDPA.

As regards data localisation requirements, even though the new legislation reverses the requirement of data localisation, the government has the power to restrict the transfers to certain countries. Additionally, the new legislation does not want to interfere with sector-specific localisation requirements, such as the ones introduced by India's central bank.

4.6 Performance Measurement and Management

Benchmarking, a comprehensive SLA, periodic audits, remedies for deficiency in quality of services or performance timelines, and disaster recovery and business continuity options are the most common contractual clauses that help the customer manage and measure the supplier's performance in technology transactions and outsourcing.

Although a customer can draft a comprehensive outsourcing contract and have it executed by the service provider, the customer's ultimate remedy in the case of the service provider's poor performance or breach of agreement will be to initiate legal actions, which is not an easy solution. Therefore, apart from a good contract, the customer should also approach the outsourcing relationship in a practical manner.

Performance management and measurement is a process that must commence from the initial

stages of an outsourcing engagement. The customer must carry out a thorough due diligence and capability assessment on the service provider. Thereafter, the customer must carry out periodic audits of the services, structured in such manner that it does not create a permanent establishment or employment claims from the service provider personnel against the customer. It is advisable that the outsourcing agreement includes provisions enabling the customer to seek removal of certain service provider personnel in case of non-performance and under performance, contrary to the agreement.

4.7 Digital Transformation

There are no major differences if the outsourcing is cloud-based. However, customers generally tend to exercise more caution to include provisions to address breaches of confidentiality, data privacy, and remedies including liquidated damages for such breaches. In many cases, customers insist that – unless the customer expressly consents – the service provider will not provide the services from, within or through the use of a public, community or hybrid "cloud" or on virtual servers not directly owned or leased and controlled by service provider.

5. Employment Matters

5.1 Employee Transfers

Indian labour laws do not permit automatic transfer of employees from one entity to another unless such transfer arises from a transfer of ownership to another entity. Further, from a practical perspective, most companies do obtain employee consent for the transfer to a new entity, in order to avoid the possibilities of future conflicts.

In case of lack of transparency concerning how the service provider has managed the employee-related compliances, it is advisable for a customer to hire such employees after they formally terminate their relationship with the service provider and the service provider gives appropriate warranties and indemnities to protect the customer from any past claims initiated by the employees. Additionally, in terms of social security benefits such as gratuity and provident funds managed through the government organisations, the transferee may have to continue maintaining those benefits by making contributions from the date of on-boarding such transferred employees.

5.2 Role of Trade Unions or Workers Councils

Historically, trade union activities in India have been limited to the traditional sectors. The unions primarily focused on wage and benefits issues. However, as part of the development of the economy and diversity in employment roles, the trade unions have also been focusing on more areas to ensure the workforce's overall welfare.

Further, the trade unions have become active in the IT/BPO sectors as well during the past few years. Although there have not been any major negative impacts, trade unions in the key cities such as Bangalore, Pune and Kolkatta have been very active participants in the IT industry.

As regards other sectors, workers council consultation can be based on the nature of changes introduced by outsourcing. By way of example, if the outsourcing alters the job conditions or causes loss of employment, the employers will have to consult the workers council.

5.3 Offshore, Nearshore and Onshore

There have not been any organised approaches in this respect. The customer preference in respect of onshore, offshore or nearshore outsourcing can be regarded as more of a needs-based choice. Further, outsourcing activities in India are currently not just limited to data processing or call centre activities. Therefore, the structuring of transactions in this respect is normally based on the assessment of the most beneficial location or model.

5.4 Remote Working

India does not have any specific laws governing remote working. However, certain legislations such as workers' compensation laws may be interpreted to apply to remote working employees, requiring the company to compensate for any injury caused during such a remote work. In some Indian states, the place of remote work can be considered as a commercial establishment even if it is not one.

Trends and Developments

Contributed by:
Anoop Narayanan
ANA Law Group

ANA Law Group is a full-service Mumbai-based law firm, with a team of experienced and committed professionals who have broad industry knowledge and specialise in a wide spectrum of laws. With prominent cross-border exposure and a solution-oriented approach, the firm provides significant value to clients internationally, as each client receives the attention required to achieve practical legal solutions. Some of the firm's key practice areas include commercial contracts, IT and outsourcing transactions, employment law, data privacy, IP, and digital media.

Author

Anoop Narayanan is the founder of ANA Law Group and has been in practice for nearly 30 years. Anoop is a distinguished commercial, TMT, IP and employment law expert, with significant experience in the field of outsourcing to India. He has worked on projects rolling out some large multinational technology companies in India, as well as on several India-bound outsourcing transactions with major Indian IT companies. Anoop also assisted many multinational companies in setting up their data centres in India and provided related regulatory advice. He regularly advises many multinational banks on Indian data protection law and related matters in connection with outsourcing transactions.

ANA Law Group

7th Floor
Keshava
Bandra Kurla Complex
Bandra East
Mumbai 400 051
India

Tel: +91 22 6112 8484
Email: mailbox@anaassociates.com
Web: www.anaassociates.com

ANA LAW GROUP
ANOOP NARAYANAN & ASSOCIATES

Contributed by: Anoop Narayanan, **ANA Law Group**

Introduction

The Indian IT outsourcing industry has been on a growth curve for the past few years. However, the COVID-19 pandemic situation prevented further growth, developments and dimensions in the outsourcing industry. While the demand has been increasing, the industry has been facing its own challenges as well.

One of the recent challenges has been attrition, as the workforce has been switching to jobs with significantly higher compensation (ie, beyond the existing industry average). The Indian vendors were finding it difficult to lose experienced human resources because finding a replacement for comparable compensation was not an easy task. However, the Indian vendors were quick to respond to the situation by taking advantage of India's demographic spread, as well the ability to expand beyond the major long-established capitals of IT outsourcing industry. As a result, companies are reaching out to smaller towns and setting up more and more centres in Tier 2-3 cities, which helps them attract a large talent pool in a cost-effective manner.

As the industry's needs continue to evolve, the outsourcing industry is also currently working with AI assistance to provide a variety of tools, machine-learning programmes and other virtual support systems. Further, the diversification of the IT outsourcing industry has been increasing rapidly, too. The services provided in addition to the traditional software development, support services or call centres include:

- digitisation;
- remote management of clients' core functions (using a project-based model or otherwise); and
- a variety of support functions in the banking, finance and accounting industry.

Role of Cloud-Based Solutions

One important development is that cloud-based outsourcing has become an essential component in all kinds of outsourcing. Until a few years ago, the customers in large outsourcing transactions negotiated a specific clause in the outsourcing agreement restricting service providers from using third-party cloud solutions to render the services.

However, with the technological advancements, the reliance on cloud models has increased. Moreover, the cost advantage and the ability to scale as required are among the additional reasons why many users prefer cloud-based models for appropriate projects.

Cybersecurity Issues

In the past few years, more ransomware attacks have been witnessed all over the world than ever before. Many such cases go unreported without any publicity. While technologies have been introduced and are evolving, one of the major concerns and issues currently discussed in the context of IT outsourcing is that of cybersecurity and data breaches.

All countries have legislative initiatives ensure cybersecurity and outsourcing agreements include excessive provisions regarding data security. The Indian government has recently introduced the new Digital Personal Data Protection Act 2023, which also details provisions and compliance requirements for data protection and reporting of cyber-incidents. As many provisions of the new legislation are subject to further consideration and the government has the liberty to legislate as required, the IT industry – along with the outsourcing industry, and other businesses – remain unclear from a practical perspective when it comes to prioritising what

kind of incidents should be reported (and when by), as well as the subsequent measures.

While cybersecurity is a growing concern in the IT services industry, one interesting aspect is that the issues related to cybersecurity are a fast-growing business for the IT industry. Even the large corporations are finding it challenging to keep their cybersecurity and data safety measures up to date with the help of only their internal resources. Businesses without large infrastructure or resources also find it challenging to comply with all the cybersecurity and safety measures, as an internal process. The situation has generated huge demand for outsourcing of data security compliance processes and audits, which in turn generates a new stream of revenue for outsourcing service providers.

Impact of AI and Machine Learning

Another important trend concerns the role of AI and machine learning in the outsourcing sector. In addition to providing AI and machine learning as solutions to the customer, the service providers themselves function using these technologies, which help the service provider to render more efficient and cost-effective services. Many businesses rely on their outsourced service providers' reports based on data analytics – and, therefore, the support of AI – for analysis of trends in the market and changes in customer behaviour, as well as for assistance with predictions for the future.

Outsourcing of certain services is no longer regarded as a measure for cost saving or HR management. However, with the advanced developments in AI, blockchain, and robotic automation, the advantage of availing outsourced services from experienced service providers provides significant additional value to customers.

Challenges and Advantages of Outsourcing

The Indian outsourcing industry is not immune to competition and challenges from other jurisdictions. However, there are many positive factors that may still place Indian outsourcing companies on a higher pedestal compared to other countries. From the outset, India had the early-mover advantage in the field of outsourcing. The talent pool available in India is highly educated and qualified, with decades of experience across all kinds of technology that global customers may need assistance with. India's geopolitically safe position together with a strong legal system (including data protection and IP laws) and English-language skills operate in India's favour when compared to countries such as China or those in Eastern Europe.

Furthermore, challenges faced by IT outsourcing companies are also evolving with the industry's growth and introduction of new technologies and services. These include increasing costs for infrastructure, HR, and the handling of projects by remote working teams, in addition to concerns about potential data security breaches.

Ever since demonetisation (followed by the COVID-19 pandemic), fintech businesses have been growing exponentially. Digital payments and blockchain technology have become part of mainstream business operations. As customers in semi-urban and rural markets prefer digital payment systems, mobile banking, etc, the IT industry's roles in supporting these market-induced requirements are also increasing proportionately. There is similar growth in the field of healthcare, with telemedicine and associated services having become popular.

Another major factor is the use of technology and digital solutions in the education sector, which is rather a recent trend. This has provided

IT outsourcing companies with large volumes of work, along with the associated challenges of scaling up and building infrastructure and safeguards.

Protection of Intellectual Property

An historic concern in the context of outsourcing to India is the protection of IP. Contrary to many perceptions, India has a well-developed IP protection regime and Indian IP laws are in harmony with the current international IP laws. The Indian IP Office and judiciary proceedings have been completely digitised and, since the pandemic, many Indian courts conduct hearings in a hybrid model (ie, physical appearances as well as online representation). Most of the Indian High Courts have been assigning judges with knowledge and experience in IP matters to decide cases relating to IP. Some prominent High Courts such as Delhi and Madras have set up specialised divisions with dedicated judges to handle IP cases and other High Courts are expected to set up similar IP divisions in the near future.

The strategy for IP protection should be adopted with a mix of contractual, practical and legal considerations. Outsourcing contracts should be drafted with all the necessary provisions for IP protection, while addressing the impact of applicable IP laws on the transaction covered by the outsourcing contract. Practical aspects include periodic training programmes for the service provider and their personnel, as well as explaining the importance of confidentiality and IP protection and the potential consequences of a breach. Although Indian law does not provide for indirect or consequential damages, the customer can obtain an agreement for liquidated damages, which are recognised under Indian law.

Conclusion

The Indian employment law regime has always supported the IT and outsourcing industry and it continues to do so, helping IT companies operate relatively free from problems. Further, various exemptions from the applicable labour laws and periodic amendments to improve the functioning of the IT industry have helped the outsourcing industry significantly.

To conclude, the consistent growth and opportunities – together with a supportive legislative and regulatory environment – minimise the impact of the occasional challenges to India's outsourcing industry. The trends and forecasts offer a lot more optimism and indications for increased and more diverse growth for the outsourcing industry in the coming years.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Katie.Burrington@chambers.com