UNIT 13 BPOs AND THE LEGAL REGIME IN INDIA

Structure

13.1 INTRODUCTION

Business Process Outsourcing ("BPO") has emerged as the most challenging sector that has not only generated employment potential in India, but has also brought huge inflow of foreign exchange into the country. Today, India is home to some of the world's leading BPO companies. In this context, it is becoming increasingly important to study and examine the legal regime in India pertaining to BPOs and to undertake an examination of data protection laws in the light of the growing concern that data transferred to India may not be adequately protected. The purpose is to identify the deficiencies in Indian law, if any, examine the well known global regulations that impact the Indian BPO industry and suggest amendments to the existing laws in India, to bring them in conformity with the international standards.

A BPO takes within its fold various elements such as finance and accounting, customer relationship management, human resources, business process, transcription, and so on. A parent company instead of performing these operations delegates them to a BPO. It may be an in house operation or a different company may be engaged to perform a particular task. It may be in the same country or in a different country. The BPO sector in India has an extremely advantageous position because of its low cost structure and large pool of skilled manpower. The foreign companies gain significant advantages due to cost savings as regards the price of production, and also the ability to concentrate on its core business, instead of having to bother with the back office operations.

There are various statutory, legal, regulatory and contractual requirements in the area of Business Process Outsourcing. These include certain tax complications that may arise as the activity may have originated in one country and profits may have been in another country. The nature of the outsourced work holds a certain value and profits of the

parent company may be attributed to these operations making it difficult to segregate the costs and profit, thus making the rules for the calculation of tax for BPOs becomes very complicated. However, it still continues to be a sunshine sector for the Indian economy, and, as a result certain tax exemptions have been provided as an incentive to foreign companies to outsource their work. BPOs are privy to confidential information of the outsourcing companies. This is an important concern due to some of the recent scandals that have in some measure deterred the potential clients from outsourcing their work to India.

The Data Protection provisions are written into the service contracts between the Indian and the foreign parties. These agreements govern a number of issues ranging from the services that should be provided and provisions relating to the termination of contract, detailed provisions as regards "escrow" of the source code of software which guards the companies against the breakdown of business relationships. The seat of arbitration in case of an infringement could be in a European Union ("EU"), therefore these service contracts may also be governed by the EU laws. In this context, the provisions of the Service Contracts assume great significance.

13.2 OBJECTIVES

After studying this unit, you should be able to:

- explain the legal process of setting up a BPO in India;
- list the issues related to data protection in the BPO industry;
- discuss legal remedies as available in India to address issues related to data protection; and
- discuss the possibility of exploring available options for creating and strengthening existing legal framework of data protection.

13.3 LEGAL FORMALITIES FOR SETTING UP A BPO IN INDIA

In order to set up a call center in India, certain guidelines stipulated by DoT have to be followed:

- The call centers are permitted to be Indian registered companies on a non-exclusive basis.
- The call centers are registered under the 'other service provider' category as defined in the National Telecom Policy, 1999.
- The validity of this permission is up to 20 years from the date of issue of the permission letter.
- 100% Foreign Direct Investment is permitted in call centers.
- The call centers have to ensure that no change in the Indian or Foreign promoters/ partners or their equity participation is made without prior approval of competent authority or as per prevailing regulations.
- The call centers can utilize resources of any authorized service provider i.e IPLC from the authorized International Long Distance operators and local leased line from any authorized Service Provider.

- The service providers would examine the network diagram and grant resources to the other service providers as per terms and condition of the govt. approval and the prevailing guidelines and policy for the service from where the resources are being taken. Both service provider and the OSP will be responsible for any violation in the use of the resources.
- The domestic call centers are set up using separate infrastructure. However, the request of the domestic call center to run on the existing private networks is evaluated on a case-by-case basis.

There are many incentives that have been provided by the Central and state Governments to ensure the growth of BPOs and have aimed at providing an enabling environment, which helps BPOs to grow with minimal interference. Special provisions have been provided for the setting up of BPO units in Software Technology Parks (STPs), Software Export Zones (SEZs), Free Trade Zones (FTZs) or Electric Hardware Technology Parks (EHTPs).

However, in spite of all these measures, there still exist many hurdles in the formation and operation of BPOs in India. Some of the problems that need to be addressed expeditiously are below.

13.3.1 Compliance Issues in the BPO Sector

Operational issues such as planning, facility, design or site location are not given much attention by BPOs. While deciding on a location, the future capacity requirements must be kept in mind. Ideally, there should be a large enough area, where there is sufficient scope for expansion because getting clearances and establishing even basic infrastructure pose a major challenge, as there are multiple agencies involved. Before setting up, a DoT license needs to be obtained, which can take anywhere between 4 to 12 weeks.

Further the telecom sector is not fully liberalized in India, call centers depend on the DoT for providing a connection to the IPLC (International Private Leased Circuit). This is not a very reliable link, especially for a business like call centers that need to run on a 24x7 basis. To operationalise a call center, multiplexers between India and the other country where the IPLC terminates are required. RBI clearance is another requirement, which can take anywhere between four to eight weeks or more.

As the focus shifts towards IT-enabled services such as call centers, it becomes essential to create a favourable growth environment. Industry bodies such as Nasscom and CII have been putting forth suggestions pertaining to areas where action is required.

Highlights

- Need to appoint a single, national level, licensing and monitoring authority for the IT-enabled services (ITeS) industry that can provide approvals for multi-facility operations all at once.
- Provision for sharing of bandwidth within the same entities and group companies in India.
- Approval for each new customer with DoT to be removed.
- Allowing IPLC connectivity on the same Local Area Network.
- Removal of bandwidth licenses.
- Declare ITeS as an ISP and allow owning their satellite gateways.
- Introduce the option to buy, sell and reserve bandwidth.

- Need to categorise ITeS as a special service under labour laws to allow 24x7 operations including night and shift operations.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 3 Min.*

What are the important legal steps for setting up a BPO in India?

.....

.....

.....

.....

.....

.....

13.4 BPO TAXATION

The taxation of BPOs is governed mainly by the interpretation of two circulars that have been issued by the Central Board of Direct Taxes and also by section 10A and 10B of the Income Tax Act. Greater details are provided in the Block which discusses taxation as a separate Unit.

13.5 DATA PROTECTION AND PRIVACY ISSUES IN THE BPO INDUSTRY

It is increasingly being realised that it is necessary to create appropriate confidence among investors and foreign companies, to the effect that the data they send to India for back-office operations is indeed safe, and that there are appropriate statutory mechanisms in place, should a breach of data take place.

While most Indian IT and ITES-BPO companies have come to be recognised for their high quality processes and information security orientation, in the wake of recent scandals and the loss of lucrative contracts in key segments for Indian companies, it has become almost mandatory for Indian BPO firms to create strong data privacy and information security strategies to still the existing criticism and skepticism associated with outsourcing.

The shift from low-end services such as customer support and medical transcription towards high-end services such as medical insurance processing and media services, engineering design and legal research, will naturally require the BPO outfits to comply with several regulations, particularly where the outsourced work is in Intellectual Property Rights – intensive areas.

However, while the absence of data protection laws in India is a serious deterrent, Indian BPO'S are trying to deal with the issue by attempting to adhere to major US and European regulations. According to NASSCOM, the Indian outsourcing industry can be broadly categorised into two segments — in-house or captive centers and third party providers. In the former, outsourcing is done by a subsidiary of the parent organization, and the central unit itself takes care of, and enforces all the regulatory issues that the offshore center is subject to. In the latter however, the service providers have the responsibility of protecting the crucial organizational data.

By adopting world-class privacy-norms and complying with security and privacy regulations, Indian service providers can ensure that they remain the preferred option for worldwide customers when it comes to offshore outsourcing. Many BPO outfits today have certifications that comply with regulations, though the number still remains miniscule. Until a tighter data protection legal regime is in place, foreign customers are relying upon contractual obligations to impose obligations for protecting and preserving data.

The principal regulations that affect Indian BPOs are:

- US-EU Safe Harbor Agreement;
- UK Data Protection Act, 1998;
- The Sarbanes-Oxley Act;
- Gramm-Leach-Bliley Act (GLBA);
- Healthcare Insurance Portability and Accountability Act (HIPPA);
- USA Patriot Act, 2001;
- Homeland Security Act;
- Children's Online Privacy Protection Act (COPPA);
- CAN SPAM Act, 2003.

The US approach to the protection of personal privacy differs from that of the EU, in that the US has a number of statutory protections which are specific to sectors or particular problems and there is no single law that provides a comprehensive treatment of data protection on privacy issues, while the EU has a universally applicable law — the Data Protection Act of 1998.

The Directive on Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector Directive 2002/58/EC is part of the new European regulatory framework for electronic communications networks and services. The underlying purpose of the new directive is to protect fundamental rights and freedoms of the individual.

The EU directive on data protection is particular to ensure that transfer of personal data only takes place to a third country, which has an adequate level of protection. However it is also significant to note that the EU directive does not define adequacy, but rather provides that it will be determined on a case-by-case basis.

Clearly, the EU data protection regime is much more rigid than that of the US. In order to bridge these different privacy approaches and provide a streamlined means for US organizations to comply with the Directive, the US Department of Commerce in consultation with the European Commission developed a "Safe Harbor" framework.

The Safe Harbor approved by the EU in July of 2000 is an important way for U.S. companies to avoid experiencing interruptions in their business dealings with the EU. Certifying to the Safe Harbor would assure that EU organizations know that the company provides "adequate" privacy protection, as defined by the Directive.

The decision by U.S. organizations to enter the safe harbor is entirely voluntary. Organizations that decide to participate in the safe harbor must comply with the safe harbor's requirements and publicly declare that they do so.

Interestingly, though the US and particularly the UK have created a framework to protect individual's personal information from misuse and abuse, such a protection

would be very fragile if the protection afforded by it were to fall apart as soon as the information left the boundaries of the countries subject to the data protection laws. It has therefore become imperative for companies to take appropriate due diligence measures on the service providers in addition to the inclusion of clauses in their contracts ensuring compliance by service providers with international data protection standards. Quite evidently, data protection in the outsourcing space remains dependant on the structure and enforceability of agreements between foreign companies and Indian service providers.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 4 Min.*

(a) What is the main legislation which provides for data protection in the EU concerning the data travelling to US?

.....

.....

.....

.....

.....

.....

.....

(b) What are the various foreign legislations which affect BPOs in India?

.....

.....

.....

.....

.....

.....

.....

13.6 CURRENT METHODS – SERVICE CONTRACTS

Currently, data-protection provisions are written into the service contracts between Indian and foreign businesses. These service contracts are governed by the EU laws with the seat of arbitration in case of infringement of the law, being an EU country. Most BPO contracts provide for stringent obligations on service providers to protect personal data of the clients of outsourcers and for tough penalties on misuse. UK, for one, seems to find this adequate. While the industry is for self-regulation, there are several problems with the current state of affairs. It may be necessary to enact firm legislation in order to bring about uniformity of regulation in this area, and to ensure data privacy and internal checks within businesses. Some form of state regulation would also have the effect of marking India as a safe destination for outsourcing activities. This would certainly help in building customer confidence and support the growth of the BPO industry.

Answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What are service contracts?

.....

.....

.....

.....

.....

.....

13.7 DATA PROTECTION LAW IN INDIA

It must be submitted at the outset that the Indian Constitution does not expressly recognise the right to privacy as a fundamental right. However, the Supreme Court has held that there is a right of privacy implicit in Article 21 of the Constitution. There is no clear law (i.e. general date protection law) regarding privacy of personal information and details etc.

An important issue is whether the legislation on data protection militates against the right to information. The Indian Supreme Court has held that access to government information was an essential part of the fundamental rights to freedom of speech and expression. Following this, several states have passed Acts recognising this right to information.

It is submitted that there is no absolute right to information recognised by the Indian Supreme Court. It is a qualified right, subject to reasonable qualifications. Since the right to privacy is also subject to restrictions such as national security and public interest, this would imply that there is no conflict between these two seemingly opposing concepts. Both the Safe Harbor Principles and the EU directive allow disclosure of personal data, if it threatens national safety, aids terrorism, is against public interest etc.

13.7.1 Exploring the Options for a Data Protection Law

Three broad options are available for creating and strengthening the existing legal framework relating to data protection.

Firstly, like the European Union, India could enact a new legislation to deal with data protection.

Secondly, India may opt for amending an existing law, such as the Information Technology Act that already contains some provisions relating to revealing of electronic information. The IT Act 2000 is aimed at providing a comprehensive regulatory environment for electronic commerce. The advantage of such a move is that existing administrative mechanisms which have been contemplated under the Information Technology Act can be used to administer data protection as well.

Thirdly, India may also choose to enter into bilateral or multilateral agreements, like the US 'Safe Harbor' regulations, with countries that are its major business partners in the field of outsourcing.

The first method seems to have found favour with the Indian government. In fact a law on data privacy has been in the offing for quite some time. In June 2000 the National Association of Software and Service Companies (NASSCOM) urged the government to pass a data protection law to ensure the privacy of information supplied over computer networks and to meet European data protection standards. The UK Data Protection Act was examined as a model and several cyber laws were recommended including ones on privacy and encryption. In May of 2000, the Government passed the Information Technology Act, intended to provide a comprehensive regulatory environment for electronic commerce.

Following the enactment of the IT Act the Ministry of Information Technology adopted the Information Technology (Certifying Authorities) Rules in October 2000 to regulate the application of digital signatures and to provide guidelines for Certifying Authorities. In March 2000 the Central Bureau of Investigation set up the Cyber Crime Investigation Cell (CCIC) to investigate offences under the IT Act and other high-tech crimes.

However, rather than have a separate law to deal with data security and privacy issues, the present government is considering an amendment to its Information Technology Act of 2000. An Expert Committee has been set-up, with an objective to review the Information Technology Act, 2000, in the light of the latest developments nationally and internationally particularly with regard to provisions related to data protection and privacy in the context of BPO operations, liabilities of network service providers, computer related offences and regulation of cyber cafes. The committee recently submitted its proposal for amendments to the Indian Information Technology Act 2000.

13.7.2 Some Proposed Amendments

In this report, the existing Sections (viz. 43, 65, 66 and 72) have been revisited and some amendments have been provided for. There is a proposal to add Sec. 43(2) related to handling of sensitive personal data or information with reasonable security practices and procedures thereto. According to provisions of section 43 (2), If any body corporate, that owns or handles sensitive personal data or information in a computer resource that it owns or operates, is found to have been negligent in implementing and maintaining reasonable security practices and procedures, it shall be liable to pay damages by way of compensation not exceeding Rs. 1 crore approx. $220,000, to the person so affected. Also a gradation has been made of severity of computer related offences committed dishonestly or fraudulently and punishment thereof under Section 66.

Further, with the intent to protect the privacy of the individual subscribers, there is also a proposal for inserting an additional Section 72 (2) that deals with breach of confidentiality with intent to cause injury to a subscriber. According to this section, "if any intermediary who by virtue of any subscriber availing his services has secured access to any material or other information relating to such subscriber, discloses such information or material to any other person, without the consent of such subscriber and with intent to cause injury to him, such intermediary shall be liable to pay damages by way of compensation not exceeding Rs. 25 lakhs to the subscriber so affected."

The proposed amendments add a paragraph to the IT Act which states, "Whoever intentionally captures or broadcasts an image of an individual without consent, and knowingly does so under circumstances violating the privacy of that individual, shall be held liable." This is the first time that a right to privacy has so expressly found its way into the statute books in India.

The Act also recommends a compensation of Rs 25 lakh to the person whose privacy has been infringed. The offender can also be jailed for one year with a fine of Rs 2 lakh.

The proposal for the insertion of new clauses in the law, is currently being reviewed by the government, so as to meet the regulatory requirements of major customers of the Indian BPO industry. The Information Technology Act of 2000 at present covers only unauthorized access and data theft from computers and networks, with a maximum penalty of about $220,000, and does not have specific provisions relating to privacy of data. The new clauses are likely to enable the Act to conform to the so-called adequacy norms of the European Union's (EU) Data Protection Directive and the Safe Harbor privacy principles of the U.S.

It is also relevant to address the issues that arise due to the trans-border nature of data transfers in the outsourcing space, as well as the rights and liabilities of the various parties involved in the process and the steps which can be taken to curb future misuse of sensitive personal data of offshore clients.

Please answer the following Self Assessment Question.

Self Assessment Question 4 *Spend 3 Min.*

What are the legislative provisions for data protection available in India?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

13.8 SUMMARY

- Clearly, as the trend towards outsourcing steps up further, Information Security will become an even more critical element of the customer strategies of service providers.
- There is strict legislation governing privacy in all developed countries, but this is the first time these issues have been addressed in India.
- The law on privacy in India, as it stands today, is limited to the right enshrined under Article 21 of the Constitution, case law on the subject. However, like other fundamental rights, it is not absolute, and is subject to reasonable restrictions imposed by the state.
- At present the IT Act is the only substantive safeguard for companies outsourcing work to India, which cannot be considered adequate for providing stringent security measures so India may emerge as a viable offshore destination.
- Given the situation, global customers will continue to feel insecure about the issue of outsourcing which can severely hinder the growth of the Indian BPO industry.

- The increasing trend of outsourcing, and the concerns of losing customers to competing countries, makes it almost obligatory for India to put in place stringent data protection law.
- With the growth of the BPO space legal complications will only increase necessitating a comprehensive and rigid legal regime.

13.9 TERMINAL QUESTIONS

1. What are the salient features of a BPO?
2. What are the issues which affect the functioning of BPOs?
3. What are proposed legislative changes to the IT Act which address the data security requirement of the BPOs?

13.10 ANSWERS AND HINTS

Self Assessment Questions

1. A BPO can be set up in India only by getting a license from the DoT. The DoT have stipulated certain steps/guidelines which must be followed:
   - The call centers are permitted to be Indian registered companies on a non-exclusive basis.
   - The call centers are registered under the 'other service provider' category as defined in the National Telecom Policy, 1999.
   - The call centers have to ensure that no change in the Indian or Foreign promoters/partners or their equity participation is made without prior approval of competent authority or as per prevailing regulations.
   - The call centers can utilize resources of any authorized service provider i.e IPLC from the authorized International Long Distance operators and local leased line from any authorized Service Provider.
   - The service providers would examine the network diagram and grant resources to the other service providers as per terms and condition of the govt. approval and the prevailing guidelines and policy for the service from where the resources are being taken. Both service provider and the OSP will be responsible for any violation in the use of the resources.
   - The domestic call centers are set up using separate infrastructure. However, the request of the domestic call center to run on the existing private networks is evaluated on a case-by-case basis.
2. (a) The Safe Harbor approved by the EU in July 2000 is the main legislation which provides for data protection in the EU concerning the data travelling to the US. Certifying to the Safe Harbor would assure that EU organizations know that the company provides "adequate" privacy protection as defined by the EU Directive.

   (b) The various foreign regulations/legislations which affect BPOs in India are:
   - US-EU Safe Harbor Agreement;
   - UK Data Protection Act, 1998;
   - The Sarbanes-Oxley Act;

- Gramm-Leach-Bliley Act (GLBA);
- Healthcare Insurance Portability and Accountability Act (HIPPA);
- USA Patriot Act, 2001;
- Homeland Security Act;
- Children's Online Privacy Protection Act (COPPA);
- CAN SPAM Act, 2003.

3. Service contracts are those contracts which are entered into by Indian and foreign companies and include amongst other things provisions for data protection. These service contracts are governed by the EU laws with the seat of arbitration in case of infringement of the law, being an EU country.
4. There is as such no specific Act enacted to deal with data protection. However, Article 21 of the Constitution of India, which deals with the protection of personal life and liberty, includes the right to privacy also

Terminal Questions

1. Refer to section 13.1 of the unit.
2. Refer to section 13.5 of the unit.
3. Refer to section 13.7 of the unit.