LawPublicus
The Legal Portal

Volume 1 : Issue 2
2020

December 2020

Email ID: Lawpublicusportal@gmail.com
Website: www.Lawpublicus.com
Address: A18 Dayanand Colony Lajpat Nagar - 4
New Delhi

Disclaimer

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of ***LawPublicus*** The Legal Portal. The Editorial Team of ***LawPublicus*** holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of ***LawPublicus***. Though all efforts are made to ensure the accuracy and correctness of the information published, ***LawPublicus*** shall not be responsible for any errors caused due to oversight or otherwise.

FOR *LawPublicus* The Legal Portal

Editorial Team

Editor-in-Chief

Mr. Nikhil Kumar Chawla
Partner - LawPublicus LLP
Principal Associate Advocate – DKC & Co.
Contact: +91-9654441680
+91-9654030411
Email ID: Nikhilchawla29@gmail.com
Lawpublicusportal@gmail.com

Senior Editor

Ms. Yantakshikaa Sharma
Partner - LawPublicus LLP
Career Counsellor
Email ID: Yantakshika@gmail.com

Senior Editor (Honorary)

Mr. KS Rana
Practising Advocate
Contact: +91-9810326424
Email ID: Jyotideeprana@gmail.com

About Us

LawPublicus The Legal Portal is a leading journal of multidisciplinary research. It is a free, peer-reviewed, open-access journal that provides insight into diverse and dynamic legal matters.

LawPublicus is a novel initiative by legal minds. As the its name suggests, it is platform for young minds to ignite their willingness and inventiveness in order to contribute to the field of law through new ideas, opinions and thereby contributing to an informed citizenry.

We hope to provide a forum for young and enthusiastic writers to voice their feelings and research on interdisciplinary approaches. We also have in view to evaluate, explore and deliberate, under the tutelage of seasoned editors and academic experts, on current trends and projections based thereon in legal studies. LawPublicus focuses not only on the scholarly writings but also on numerous other approaches such as discussions, interviews, and debates with experts and qualified & industrial professionals.

We are determined and excited to bring authentic, creative and individual ideas and socially-related problems into attention.

LawPublicus calls for research papers, articles, short notes, book reviews & case commentaries, that are distinctive and unpublished.

With this thought, we hereby present to you

LawPublicus The Legal Portal

DATA PROTECTION LEGISLATION FOR OUTSOURCING ENTERPRISES: A STUDY

Authored By:
Sarim Husain
E-mail ID: srmhusain@gmail.com
Mob No.: +91-9650645389
Designation: Lawyer
PRAYAGRAJ

Data Protection Legislation for Outsourcing Enterprises: A Study

By: Sarim Hussain

ABSTRACT

Data protection relates to safety issues dealing with the collection, storage, and use of data provided by internet users. Data privacy talks about the personal and limited sharing of personal information. Outsourcing refers to the act of two companies, wherein they come into an agreement for one company to outsource its activities or business processes to the second company; financial benefits being the main reason behind this concept. The activities outsourced may be of any nature. Since the export of any services would also entail the export of client details and other confidential information, which would require stringent data security laws. Many companies don't heed to the issue of Data Protection while outsourcing their activities or business processes to some other company or individual, but different countries have different laws to specifically deal with this issue. Though the concept of data privacy is not directly governed by any legislation, there are various laws indirectly safeguarding it, as in the Information Technology Act, 2000; Indian Penal Code, Intellectual Property Law, Credit Information Companies Regulation Act, 2005(CICRA).

This paper aims to briefly examine the data protection legislation of the UK and USA regarding the data security of outsourcing companies. The author also analyzes the laws for the same in India along with problems and possible measures for it. The paper shall also cover the need for data protection laws and their current position of the same, in India.

I. INTRODUCTION

In the last few years Indian industries in the field of data collection, its storage, and transmission have made rapid progress. In the 21st century itself, the processing, storage, and transmission of personal data have become an essential factor to the success of any business especially outsourcing business. India is experiencing a major change with respect to the use of state-of-the-art technology. Some of the significant changes are the digitalization of governmental and other authorities established by law, the use of smartphones in public places, and the use of identification cards carrying an individual's necessary information, etc. With the rapid growth of the digital age more and more personal information of customers is held in vast databases that are controlled by private companies and so the need for data protection arises. Safeguarding sensitive data is a very important element in the field of outsourcing related business. A lot of data (both common and sensitive) is traded between an outsourcing company and its client during the entire process of outsourcing. With the aim of getting more outsourcing projects, it is demanded by the concerned companies as to the formation of a legal framework having nature, which would guarantee the data traded between the client and companies' service provider, good security. Lack of such a legal framework prevents the enterprises from trusting with outsourcing their monetary projects to enterprises situated abroad.

India has emerged as the outsourcing hub but then the need arises to guesstimate provisions related to law with respect to guard the data. The factor on which the outsourcing industry is principally setup is the exchange of data, and adequate provisions in the legal system safeguarding the same. On one hand, there is the UK and USA which have appropriate and definite legislation to handle data protection. On the other hand, there is India which has very few provisions in its Information Technology Act, 2000 for handling data protection albeit recently proposed changes. This poses a great challenge for India which is still on a developing stage and the lack of proper legislation with respect to data protection could diminish its opportunity to grow in the outsourcing sector.

This paper aims to examine the various legislations regarding data protection of outsourcing companies with special reference to legislation of the UK and US. The author shall also analyze the problems with data protection legislation in India and the possible measures for it.

II. DATA PROTECTION

A. Concept:

The primary reason for a company to outsource is to lessen its operational expenses. Developing countries like India provide labor force at a comparatively cheaper cost which makes it easier for such companies to cut operational costs that would otherwise be expensive for them. Generally, Business Process Outsourcing **(hereafter referred to as BPO)** especially the one related to IT, does not have enough capital resource to hire experts, and therefore their first choice is outsourcing. India provides a good quality workforce at a lower cost which makes it a global destination for outsourcing. The socio-economic as well as political factors contribute to the same.

Every citizen as a consumer must possess the legal rights as well as the means through which he or she can exercise such right to protect their important credentials and other personal information from any kind of misuse. The fundamental right to privacy guaranteed under our Constitution and other related international legislation and conventions have the concept of data protection deep-rooted in them.

"Data protection can be defined as the law designed to protect our important personal information, which is collected, processed, and stored by automated means or intended to be part of a filing system. In modern societies, to empower us to control our information and to protect us from abuses, it is important that data protection laws restrict and clarify the activities of companies and governments." In the age of the internet, the constant transfer of data on global sales is expected. While there are several ways in which data privacy can be explained, the phrase usually refers to the privacy of information in relation to a person's private information or the privacy or security of data that is transmitted by electronic means.

The application of computers to process information regarding individuals saw exponential growth throughout the early 1970s. Progress of the European Economic Community led to an increase in trans-border trade, which increased the trading of private information, which was eased by the advances in computer technology which contributed to the aforesaid exponential growth. Public administration and the large corporation were influenced by the fast growth in the arena of electronic data processing and the launch of modern age computers to establish

data banks that helped in improving the storing of data, operating and partaking of private information. Modern occasions for operating data on an international level were a result of the coming together of computers and along the advancement of telecommunications.

Substantial gain with regard to the efficacy in the field of information technology and computers resulted in the risk related to these developments affecting the privacy of people. It was examined that the transmission of data to offshore enterprises would increase the breach of privacy.

III. NEED FOR DATA PROTECTION

Chances and risk of monetary loss was the primary reason to implement data protection and related laws. Data is regarded as an essential property for many enterprises and hence demand protection. This could even lead to the loss of customers due to the distrust caused because of such loss of important information. If there is data theft of any information is hacked and altered in any manner it would lead to an effect on the capital of the business which remains hidden to the company until any other problem arises. Then nothing much could be done about it.

Another factor that creates the want for data privacy is the imposition of statutory provisions by the authorities. Almost all countries have started enacting regulations on Information Technology and saved data. And non-compliance with such regulatory laws may result in negative consequences. “Some countries hold company heads criminally liable for failure to comply with laws regarding electronic communications and documents. These regulations provide as to what information must be retained, for how long, and under what conditions. Other laws are designed to ensure the privacy of the information contained in documents, files, and databases. Loss of critical communications can be construed as a violation of these regulations and may subject the corporation to fines and the managers to legal action.”

Another reason, which is necessary for institutions and yet does not come to the notice of concerned authorities, would be productivity. “Loss of important data lowers overall productivity, as employees have to deal with time-consuming customer issues without the aid of computer databases. Data loss also results in application failures and similar system problems, making it difficult for people to do their jobs. A poor data protection strategy may

leave people waiting for long periods for systems to be restored after a failure. During that time, employees may be idle or able to work only in a reduced capacity, further diminishing productivity".

Generally, it has been observed that customers look forward to constant attention from the companies at all times. Any kind of undue delay or postponement on the part of the companies is not taken positively by the customers. The phenomenon of data loss makes it inefficient for businesses to work and as a result, they have to extend comprehensive data schemes. Problems like these are faced by all categories of businesses. Hence, the need for efficient data protection legislation arises.

IV. DATA PROTECTION LAWS OF THE UNITED KINGDOM

A. Data Protection Act, 1998

"The Data Protection Act, 1998 is considered an umbrella protection law regarding all public and private information within the United Kingdom. It covers all issues related to the collection, storage, processing, and distribution of personal data. The act provides measures for individuals to access their personal information. Upon discovery of false information, the Act allows individuals to claim compensation from obligatory organizations."

The Data Protection Act, 1998 is a United Kingdom Act of Parliament which is formed with the aim of protecting important data and information on computer systems and also covers paper filing system. It is based on principles of **EU Data Protection Directive 1995** protection, operating, and transfer of data. People possess legal rights to supervise information about them. But the major part of the Act lacks any domestic application. A person is legally bound to follow the provisions of the Act if he holds the data for any purposes, except under a few circumstances. The Act provides eight data protection principles that provide for lawful processing of information.

1. Salient Features of the Act:

The Data Protection Act applies to:

1. Automatically processed information (i.e. records which are related to computer);
2. The information noted down on paper (but the record on paper must be accurately arranged, so that a particular fact related to a person may be looked for):

3. Records which concern health and specific records that are related to public authority.
4. The Act contains several rights on individuals which are related to their personal data. Individuals have the right to ask for details about the reasons why their personal data is being used; and other information about the same; the right to prevent such use if it might result in any sort of damage to them or other people; right to oppose to any sort of direct marketing; and the unopposed right to bar computerized decisions that influence them; can even ask for alterations or deletion in their personal data; are eligible to ask for damages if data controllers cause a breach of any of the provisions of the Act.
5. The Act is related to eight Principles on Data Protection. They have to be ensured, during the collection of the data, as well as during its processing. The principles are as follows:

a. Impartial and legal processing of personal data and not processing it, except for:
Fulfilment of at least one of the detailed list of preconditions (for example, the data subject has agreed to or it is necessary to process the data, to result in the execution of a contract to which data subject has entered into with some other party), and where delicate personal data is concerned, the fulfilment of at least one more of a supplementary set of pre-conditions (for example, where the explicit consent of data subject is involved or it is necessary to process the data to enable carrying out of a legal obligation concerning employment).

b. Acquiring personal data only for one or more described and legal purposes, and not processing it for any other purpose(s).

c. Acquiring only that much of personal data which shall be sufficient and satisfactory; nothing in excess to the purpose(s), for which it is acquired.

d. Personal data must be authentic and updated, whenever required.

e. Not storing the personal data processed for more than time than is required for any purpose or purposes.

f. Processing of personal data must be in consonance with the rights granted to data subjects by the Act.

g. Taking pertinent scientific and regulatory steps against unjustified or illegal processing of personal data and against any unexpected injury, harm, or damage caused to personal data.

6. Not transferring personal data to any country or territory which is not included in the European Economic Area, except for, a guarantee by that particular country or territory

that the rights and freedoms of data subjects shall be accorded a suitable level of protection, as far as the processing of their data is concerned.

7. Various violations under the Data Protection Act, 1998 are considered criminal offenses.

In addition, the directors or other prominent officers of a company causing breach may also be made personally accountable. Other results are also possible. In recent years, the people of the UK have become more acquainted with their rights related to the subject of data protection, and some of them are seen accusing the organizations which do not follow the legislation related to data protection, to the Information Commissioner. The legislative costs involved in handling such complaints, and making investigations accordingly becomes costly for the Information Commissioner, who even has to make those complaints public, those are sustained for prosecutions. To enforce the Act, the Information Commissioner can levy a fine of up to the amount of £500,000 on the occasion of organizations voluntarily and breaching the Act. The Information Commissioner may also provide enforcement, and notice giving information, where such notice shall need a controller to administer information to help the Commissioner in deciding whether there has been a violation of data protection principles concerning public bodies. Under some specific situations, the Commissioner can ask the court for an entry and inspection warrant.

The Data Protection Act, 1998 is only one of the UK's statutes deciding the use of personal data. A few more important legislations have also been enacted in the last few years regarding this topic. These legislations have other conclusions too, other than in the field of Data Protection.

B. The Privacy and Electronic Communications (EC Directive) Regulations, 2003

The Privacy and Electronic Communications Regulations (PECR), act side by side with the Data Protection Act. They accord certain privacy rights to people in relation to electronic communications.

They have their roots in European law. They apply European Directive 2002/58/EC, also known as 'the E-privacy Directive'. It aims to strike a balance between the recent information privacy system and the expansion of extra peculiar privacy rights related to the transmission of data. It considers that people can use any modern-day technology related to information technology which in return gives them and other enterprises scope of growth but also poses

certain threats to their personal data. Until now four amendments have taken place related to PECR. The latest changes have taken place in 2015, providing for granting emergency text alerts and to enable proceeding action in case of violation in the marketing rules, and then in 2016 about needing people who make an impact on marketing call to demonstrate their contacts.

C. Human Rights Act, 1998

The Human Rights Act 1998 or HRA enlists the basic liberties which have been given to every person in the UK. Human rights encompass an individual's privacy as well and it is where this Act comes into play.

It includes the power given in the European Convention on Human Rights (ECHR) into the local law. It implies, in case, there has been a violation of somebody's rights; his/her case may be brought before the home court instead of pursuing the case in the European Court of Human Rights in Strasbourg, France. Their law prescribes that all institutions established for the service of the citizens are needed to honor and safeguard human rights. Hence, Parliament is required to confirm whether or not the latest laws passed are in conformity with the standards of the European Convention on Human Rights (even though the Legislature is autonomous and can make laws that do not conform to such requirements). The courts shall also keep in view the Convention rights while enacting other laws. The Human Rights Act was enacted in the UK in October 2000.

D. Regulation of Investigatory Powers Act, 2000 (RIPA)

Secret scrutiny by organizations established by law is controlled by the RIPA. This incorporates inspecting individuals through various modern-day state-of-the-art technologies, and the involvement of undercover agents ('covert human intelligence sources'). RIPA includes cover surveillance by other law enforcement bodies (eg the Serious Fraud Office or the Serious Organized Crime Agency), the security and intelligence services (MI5, MI6, and GCHQ), and various other public bodies, even local government.

E. The Freedom of Information Act, 2000

This statute administers or permits the right to use details of people who are controlled by organizations established under law. It does so by making it compulsory for public

authorities to disclose specific information regarding their working procedures and members of the public are capable of seeking information from public authorities.

The statute covers any crucial details released in all parts of the United Kingdom that are regulated by the institutions established under law. Scotland's Freedom of Information (Scotland) Act, 2002 covers information retained by Scottish institutes formed by law like governmental departments, domestic regulatory agencies, the NHS, government schools, and police. It, however, doesn't explicitly specify every organization and its monetary transactions. Registered details comprise all data stored in the hard or soft form on any medium. This legislation is very clear about not providing any data related to the health of any person. And in order to access any details about themselves that are held by any authority a person needs to apply first under the Data Protection Act 1998.

In short, it can be easily assessed that legislations regarding data protection in the UK are pretty much thorough. They cover a wide array of legal aspects that may arise due to breaches of data privacy. In the author's opinion, the UK's legislation in data privacy matters is adequate.

V. DATA PROTECTION LAWS OF THE UNITED STATES

"As the use of computerized databases to store information about individuals became widespread in Europe and America in the 1970s, data protection legislation began to appear. The rapid uptake of this new information technology by government agencies and businesses sparked fears of potentially deleterious effects, such as errors in the data or secret surveillance by the state or commercial entities, all of which had potentially chilling effects on individual privacy and personal freedoms. Elected representatives seeking to protect their constituents from the potential harms of data processing formulated legislative solutions. The term data protection was coined in Europe to describe privacy-protective legislation while in the United States (US) this effort was more commonly referred to as data privacy."

In the US data protection has no centralized legislation. And for the purpose of getting entry of the private data stored, third party ownership can be accessed to in the field of employment or health or buying automobile, house, or other things bought on loan. But no umbrella legislation could deal with different aspects of data handling like storage and transmission. There is also no regulation that could keep a check on taking permission before the use of

personal data of people in the USA. Nevertheless, there is some important legislation in the USA that deals with data protection and privacy:

A. The Fair Credit Reporting Act (FCRA) is an Act containing the storage of credit data and entry to one's credit report. Having been passed in 1970, it has the object of maintaining fairness, correctness, and production of personal details stored in the list of the agencies meant for reporting credit. It lays down that any individual or commodity asking the legitimate reason for such data before exhibiting it. It even mentions making the FTC as the specialist who can implement the provisions of the Act.

B. Health Insurance Portability and Accountability Act of 1996 or **HIPAA** is a law passed by the US government that mentions data protection and safety provisions to safeguard the medical data of people. Recent cyberattacks and ransomware attacks on health insurers and suppliers resulting in the infringement of health related data have increased the popularity of this law. The Act contains two major objects:

1. Invariable health insurance coverage for the workers who have switched or have been laid off from their employments.
2. Minimizing the managerial duty and expenditure for health care by keeping a check on electronic transfer of managerial and monetary deals.

It has other purposes as well as handling misuse and deceptive health insurance and health care delivery, also improving chances of accessing health care services in the longer run.

C. The Gramm-Leach-Bliley Act (GLBA) enacted in the year 1999 provides personal data security with the main purpose to serve businesses that deal in finance. It states that safety of client's details is of paramount importance and therefore must be protected at all cost from various kinds of cyber threats. It also covers measures for safeguarding unlawful usage of personal details.

D. The Right to Financial Privacy Act of 1978 safeguards the privacy of personal and financial details. It does so by bringing into force a Fourth Amendment protection for bank logs. Basically, the RFPA talks about giving individuals notice and raising objections accordingly before the bank or any other institute mentioned. Such notice should be given by the federal government agencies before they reveal private financial data to a federal government agency, mostly to enforce the law.

E. The Sarbanes-Oxley Act of 2002 (SOX) is legislation which was enacted by US Congress in 2002 to prevent companies from defrauding the investors by their accounting activities. For this, the Act brought necessary changes to amend the release of monetary data from companies and to prevent accounting fraud. Public frauds like Enron Corporation, Tyco International plc, and WorldCom in the early 2000s made everyone doubt the financial settlements and demanded an overtaking of regulatory measures.

As a result, the SOX Act was passed to deal with the various malpractices. The Act made it compulsory for the details of corporations and even the electronic details and messages to be stored for no less than a period of 5 years. On the occasion of a breach of these provisions, individuals and companies should be made liable to imprisonment, fine, or both. The charge of forming and preserving the records of a corporation in a cost-effective manner done by abiding by all the legislative provisions is left to the corporation.

This Act provides that all business records, along with electronic records and messages, must be saved for not less than the period of five years. In case of non-compliance, fines shall be imposable or imprisonment, or both. Companies are left with the operation of forming and maintaining a corporate records archive in a cost-effective manner that fulfills the legislation provisions.

In the author's opinion statutory laws of the USA envelop crucial points like finance, health, accounting, and corporate affairs, that happen to handle a lot of personal information of individuals and thus protecting data privacy. But unlike the UK, the USA doesn't have a centralized regulatory law related to data privacy.

VI. DATA PROTECTION LAWS IN INDIA

India like the USA lacks a common regulatory approach to data protection. However, just as in the United States, India has several laws that regulate data protection in particular fields. For example, telecommunications, public financial institutions, and information technology are all regulated through national legislation. The Telecom Regulatory Authority of India safeguards consumers by providing that telecommunications service-providers guard customer's privacy whenever the safety of the public at large isn't involved. **The Public Financial Institutions Act of 1993** safeguards details with respect to banking activities.

The Information Technology Act of 2000 or the IT Act deals with computer crimes like system hacking, damaging computer source code, hacking into confidential files, and viewing pornography. The IT Act is India's primary data privacy law that encompasses significant subject matter. **Sections 4, 5, 7**, and **79** of the IT Act provides for specific provisions that deal with data protection for the types of information technology frequently involved in outsourcing. **Section 4** protects every kind of digitalized data that can be used in any judicial matter as evidence. **Section 5** legally recognizes digital signatures as a way of establishing digital records and delegates the Centre with power to certify companies before they can lawfully work in India and to maintain all-digital signature certificates as established by the IT Act. Under **Section 7**, records must be retained in their non-altered form, and the specific details that confirm the particular period at which such records were undertaken are to be saved. **Section 79** exonerates all IT related providers, from liability for the disclosure of third-party data when they can prove that the violation was done unbeknownst to such providers and that they performed to the best of their abilities in stopping any unlawful revelation.

In 2006, India further displayed awareness about the significance of safeguarding data protection, perhaps concerning the EU Directive and negative image around data theft in call centers when it passed an amendment to the IT Act that allows a pecuniary penalty of over $1 million on enterprises and individuals who are unable to adequately safeguard personal information. Even though it is a great measure, this legislation is still problematic for three reasons. Firstly, the legislation is a result of a lesson learned from the problem of data security infringement in the IT industry rather than a conscious step by the Government. Secondly, the legislation focuses specifically on the regaining of personal data instead of the wider safeguarding of private data and is thus still limited in its regulatory scope. Thirdly, India has a negative image of showing leniency in enforcing legislation, which results in a risk to offshore companies on the prospective that violations of privacy shall remain unheard. India also relies on DSCI. Data Security Council of India or (DSCI), is a non-profit, organization on data protection in India, started by NASSCOM (a not-for-profit industry association established in 1988), with the sole aim of creating well-protected cyberspace by following the best globally accepted data protection laws and to achieve these aims DSCI in collaboration with governmental agencies plans, schemes, and implements them in various ways.

VII. CURRENT POSITION

The IT Act 2000 is an initiative for laying a legal foundation for the IT industry. NASSCOM is putting up efforts to bring development in the IT law. All such organizations that deal in digital transactions rely upon this kind of law. Intellectual property provisions are not very well dealt with under the statute and call for better safeguard. Any inquiry of cyber offense falls under the authority of police authorities who are mostly not well aware of the cyber laws. This poses a great problem and also makes such inquiries cumbersome. In 2006 the Indian Parliament gave a green signal to a better data protection perspective to fortify and reassure trust in local corporations. This perspective has made the IT Act 2000 much better and more prepared against cyber-attacks and security breaches. Punishments for respective data breaches, cyber-attacks, and abuse of personal information are covered.

Many updates are to be made to the existing Act. The amendments have made any spilling of private information or details criminal activity. Accessing personal details in any manner without proper permission would attract imprisonment punishment. It will be the organization's liability to safeguard the data and failing to take any necessary action on finding any violation would result in civil and criminal punishments.

The Ministry of Electronics and Information Technology on December 11, 2019, introduced a draft data privacy bill in the Lok Sabha. The proposed bill requires the establishment of a Data Protection Authority in the country along with data processing by fiduciaries (an entity or individual who decides the objective of processing personal data) with the individual's permission. The Bill categorizes data into– Personal Data, Critical Personal Data, and Sensitive Personal Data. Sensitive personal data such as financial information, health care data, sexual orientation, biometric data (facial images, fingerprints), etc. may be shared or transferred abroad for processing if an individual expressly consents to it but under some restrictions. But such data should also simultaneously be stored in India. Critical personal data that is not defined by the government can only be processed in India. The Bill also provides for the amendment of the Information Technology Act, 2000 to remove the provisions related to compensation payable by companies for failure to protect personal data. The draft is yet to be enacted.

VIII. MEASURES FOR DATA PROTECTION FOR OUTSOURCING ENTERPRISES

A. Challenges

The Information Technology Act, 2000, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 read together, provide legal provisions for data protection in India. However, despite these legal statutes, there still exist certain shortcomings in them which are unable to deal with the data protection problem as required.

Firstly they do not provide for any permission to be taken to whom the information is related. Rather only the handler of information is required to give any consent. This poses a risk of manhandling of personal credentials that are collected. Chances of variations in data also arise. Secondly, the unrestricted power that the governmental authorities possess personal information is another problem because that results in the breach of an individual's privacy. It must be considered that the rules do not make it compulsory for the government agencies to get a warrant to obtain sensitive details but a request in writing alone would be enough. The law also not specifies if it applies to the governmental authorities formed or other similar authorities working under the government's supervision.

The restrictions on the transfer of data to other nations that do not follow the same legal standards can also seriously affect the home country's business. Inability to transmit the data to their business supervisors may affect the business financially.

Section 46 of the Act states claim that cases involving reward up to Rs. 5,00,00,000 will be taken up by the adjudication officer and claims related to cases involving rewards greater than Rs. 5,00,00,000 would be taken up by civil courts. But in reality, the civil courts in our country are underdeveloped to take up such matters of high monetary value due to mediocre infrastructure, cumbersome procedures, already pending cases, etc.

B. Measures

It doesn't matter where the data is-at home or in other countries as security of data is of utmost problem. The real cause of the whole problem is unethical behavior by employees. Essentially regular checks of data along with goo employee training are very elements for security. In India, many companies working in the outsourcing field have **BS7799**, a popularly

known data protection regulating certification. Today, the BPOs are incorporating a different approach by going digital at offices to better data protection techniques and adopting new methods to secure consumer data from theft and unauthorized access.

According to United Kingdom's Financial Services Authority India despite all the negative image of not having a necessary legal framework for securely handling customer data has one of the best software and hardware production enterprises that operate in the data protection field. BPOs with good reputations follow laws that are prevalent globally. Therefore, the Indian Service providers should give assurance to BPOs that data security will not be compromised in any way.

The Indian Service providers by adopting and executing international standards for information security and privacy can compete with global forces. To achieve such standards the companies must conduct an overall checking of their workers; supervise worker's computer access during their job function thus providing extra safety from cyber threats. Restricting or prohibiting gadgets having the potential to store files should also be done.

Outsourcing corporations require safe checking codes which could be used to check safety at both networking level as well as at a personal level and maintaining the privacy of data like by using CCTVs and anti-cyber threat software. Safety checking on a personal level should be followed before data is sent offshore. These checking consist of safety metallic movable barriers entering which entrants are given identity cards and other area accessing keys. Good quality CCTVs should be installed in every area.

To secure server and other networking points which could be harmed through any cyber attacks must be protected by newly designed security alert devices and programs. Advanced anti-malware software that is well encrypted should also be installed. All the office workers' details should be taken and kept on record and before hiring them all secrecy policies should be explained to them. This should be mandatory in all such enterprises.

Strict checking at all opening and closing points are commonly seen at many big and medium-sized corporations. "Compliance regulations from the Securities and Exchange Commission and other regulatory agencies require internal controls for application development and maintenance that must be extended offshore if any portion of the work is to be outsourced.

Compliance documents from western clients must now include data security and privacy assurances from outsourced companies."

The IT Act, 2000 is not the only legal remedy available against cyber threats to important stored data. The Government of India should form the data protection legal framework in collaboration with authorities that are working in this field only or are specialized in it. Agencies like CERT-In, DSCI should try and adopt ISO 27001 standard, "NIST 800-53, Co BIT, "ITIL, IT Security Guidelines for Certifying Authorities" as given in IT Act 2000. Such steps have also been taken up by many developed countries.

IX. CONCLUSION

India has emerged as one of the primary choices for many outsourcing businesses throughout the globe due to the availability of a cheaper, abundant, and better quality workforce. The only area of concern that this study concludes upon is the lack of comprehensive legislation in relation to privacy and data protection. This concern has been specially brought into notice by international corporations who want to outsource in India but lack confidence in Indian BPOs' law related to data protection resulting in issues while entrusting confidential details of their clients.

Therefore, India which is one of the leading IT-BPO on the global sale needs to come up with the best data protection laws by adopting the international standards like "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", EU Directives, etc. For now, India needs to demonstrate that its IT-BPO industry is ready to work according to the globally recognized standards so that offshore corporations continue to consider it as the first location for the service of their outsourcing requirements. Once an extensive data protection law comes into existence it would further make way for Foreign Direct Investment. A well-protected cyber system with the support of data protection agencies and their internationally accepted legal standards is a must for increasing the chances of the development of outsourcing possibilities in India.
