ELP

ECONOMIC LAWS PRACTICE

ADVOCATES & SOLICITORS

Data Protection & Privacy Issues in India

www.elplaw.in /elplaw.in /ELPIndia /company/economic-laws-practice

Table of Contents

Preface

Dear Reader,

Data surrounds us and is generated in virtually everything we do. One type is data that we may voluntarily share, and the second type is the data which is generated literally every time we do something – whether it be travel, order a meal or use transportation. There is no doubt that this data is immensely valuable and several companies are willing to pay for access to this data. Indeed, in this age of universal and virtually free access of internet, data is the new currency. What is even more intriguing that the full potential of the data is not known. As technology progresses, newer applications emerge enhancing the value of the data.

Several questions beg consideration: who does this data belong to? Who can access it? What are the limits, if any, on the exploitation of this data? As in all things technology, the law is paying catch up. Jurists around the world are struggling to marry traditional concepts of the law and the absurdly invasive times we find ourselves in. This position is further complicated by several governments demanding and seeking access to data from its citizens and corporates. On the other hand, what are the limits to privacy? Can data be demanded for the availing of basic services, travel or even government benefits? Does national security override all concerns of privacy?

The debate has now reached new levels. On August 24, 2017, the Supreme Court of India held that the 'right to privacy' is a fundamental right guaranteed by Part III of the Constitution of India. This decision will have far-reaching ramifications on the laws and regulations. New laws will now be tested on the same parameters on which the laws that infringe upon person liberty are tested under Article 21 of the Constitution of India. The right to privacy is now unequivocally available – the question that still remains outstanding is its contours and limits. That will be examined in another matter, i.e. the Aadhar case, which deals with the mandatory biometric registration of all those seeking access to government services in India.

As on date, India does not have a comprehensive legislation which deals with data protection and privacy. The existing legislations and policies are essentially sectoral in nature. Apart from other sectoral legislations, as of now, the relevant provisions of Information Technology Act, 2000 and the rules thereunder, regulate the collection, process and use of 'personal information', and 'sensitive personal data or information' by a 'body corporate' in India.

The Government is also in the process of formulating a detailed legislation governing data privacy and protection. More concrete efforts in this direction started with group of experts on privacy chaired by Justice A.P. Shah, former Chief Justice, Hon'ble High Court of Delhi, which submitted its detailed report on October 16, 2012. Recently government has appointed an expert committee under chairmanship of Justice Srikrishna, a former Judge of the Supreme Court of India, to (i) to study various issues relating to data protection in India; (ii) to make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill. Accordingly, the committee is expected to submit its report along with the bill by the end of the year 2017.

Separately, the Telecom Regulatory Authority of India has also floated a consultation paper on privacy, security and ownership of the data in the telecom sector. Further, the report of the Household Finance Committee of Reserve Bank of India has urged for 'rights based' data protection framework as opposed to using 'consent' as primary mechanism to ensure data protection to improve household financial outcomes.

In the second part, we have discussed in detail the extant legal provisions governing the personal data and privacy protection provisions under the following key legislations:

1. Information Technology Act, 2000 and the rules framed thereunder;
2. The rules and regulations governing the following sectors:
   - 2.1. Telecommunications;
   - 2.2. Banking;
   - 2.3. Medicine and Healthcare; and
   - 2.4. Insurance
3. The Right to Information Act, 2005;
4. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 and the rules framed thereunder; and
5. EU General Data Protection Regulations.

We do hope this makes for an interesting read. We respect every reader's opinion and your feedback is welcome.

ECONOMIC LAWS PRACTICE
ADVOCATES & SOLICITORS

PART I

The Concept of Data

Section 2(1)(o) of the Information Technology Act, 2000 (the "**IT Act**") has defined "data" to mean "*a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer.*" The electronic consent framework issued by the Digital Locker Authority defines 'data' to mean "*any electronic information that is held by a public or private service provider (like a government service department, a bank, a document repository, etc. This may include both static documents and transactional documents'. However, the concept of data is not only restricted to electronic information but also extends to information stored in physical form, e.g. on a piece of paper".*

Privacy of Data

Over last couple of years there has been a substantial increase in the amount of data that is generated through the usage of various electronic devices and applications. Today's businesses derive a substantial value by analyzing the 'big data' and often determine their business strategies based on such analysis. While there is no denying the business efficiency involved, the burning question is 'do individuals have a control over the manner in which information pertaining to them is accessed and processed by others'.

Privacy is the right to be left alone or to be free from misuse or abuse of one's personality. The right of privacy is the right to be free from unwarranted publicity, to live a life of seclusion, and to live without unwarranted interference by the public in matters with which the public is not necessarily concerned.[1]

The right to privacy is not new. It has been a common law concept, and an invasion of privacy gives a right to the individual to claim tort based damages. One of first cases on the said topic was ***Semayne's Case (1604)***[2]. The case related to the entry into a property by the Sheriff of London in order to execute a valid writ. Sir Edward Coke, while recognising a man's right to privacy famously said that "*the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose*". The concept of privacy further developed in England in the 19th century and has been well established in today's world. In case of ***Campbell v. MGN***[3], the court held that if *"there is an intrusion in a situation where a person can reasonably expect his privacy to be respected, that intrusion will be capable of giving rise to liability unless the intrusion can be justified".*

[1] *Strutner v Dispatch Printing Co., 2 Ohio App. 3d 377 (Ohio Ct. App., Franklin County 1982).*
[2] *Peter Semayne v Richard Gresham, 77 ER 194.*
[3] *2004 UKHL 22.*

Indian Jurisprudence on Right to Privacy

i. **Article 21:** Article 21 of the Constitution of India provides that "*No person shall be deprived of his life or personal liberty except according to procedure established by law*". However, the Constitution of India does not specifically recognize 'right to privacy' as a fundamental right.

ii. Whether the 'right to privacy' is a fundamental right was first considered by the Hon'ble Supreme Court in the case of ***M. P. Sharma and Ors. v Satish Chandra, District Magistrate, Delhi and Ors.***[4], wherein the warrant issued for search and seizure under Sections 94 and 96 (1) of the Code of Criminal Procedure was challenged. The Hon'ble Supreme Court had held that the power of search and seizure was not in contravention of any constitutional provision. Further, the Hon'ble Supreme Court refrained from giving recognition to right to privacy as a fundamental right guaranteed by the Constitution of India by observing as under: -

> *"17. A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction. Nor is it legitimate to assume that the constitutional protection under Article 20(3) would be defeated by the statutory provisions for searches."*

iii. Thereafter, in the case of ***Kharak Singh v State of Uttar Pradesh and Ors.***[5], the matter considered by the Hon'ble Supreme Court was, whether the surveillance by domiciliary visits at night against an accused would be an abuse of the right guaranteed under Article 21 of the Constitution of India, thus raising the question as to whether Article 21 was inclusive of right to privacy. The Hon'ble Supreme Court held that such surveillance was, in fact, in contravention of Article 21. The majority judges further went on to hold Article 21 does not expressly provide for a privacy provision, and thus the right to privacy could not be construed as a fundamental right. The Hon'ble Supreme Court observed as under:-

> *"17. Having given the matter our best consideration we are clearly of the opinion that the freedom guaranteed by Article 19(1)(d) is not infringed by a watch being kept over the movements of the suspect. Nor do we consider that Article 21 has any relevance in the context as was sought to be suggested by learned Counsel for the petitioner. As already pointed out, the right of privacy is not a guaranteed right under our Constitution and therefore the attempt to ascertain the movements of an individual which is merely a manner in which privacy is invaded is not an infringement of a fundamental right guaranteed by Part III."*

However, the minority opinion by Hon'ble Mr. Justice Subba Rao recognized privacy as an important facet of personal liberty and thus Article 21 of the Constitution of India by observing as under: -

> *"28. In A.K. Gopalan case [1950 SCR 88], it is described to mean liberty relating to or concerning the person or body of the individual; and personal liberty in this sense is the antithesis of physical restraint or coercion.*

[4] 1954 SCR 1077.
[5] (1964) 1 SCR 334.

The expression is wide enough to take in a right to be free from restrictions placed on his movements. The expression "coercion" in the modern age cannot be construed in a narrow sense. In an uncivilized society where there are no inhibitions, only physical restraints may detract from personal liberty, but as civilization advances the psychological restraints are more effective than physical ones. The scientific methods used to condition a man's mind are in a real sense physical restraints, for they engender physical fear channelling one's actions through anticipated and expected grooves. So also the creation of conditions which necessarily engender inhibitions and fear complexes can be described as physical restraints. Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle"; it is his rampart against encroachment on his personal liberty. The pregnant words of that famous Judge, Frankfurter J., in Wolf v. Colorado [[1949] 238 US 25] pointing out the importance of the security of one's privacy against arbitrary intrusion by the police, could have no less application to an Indian home as to an American one. If physical restraints on a person's movements affect his personal liberty, physical encroachments on his private life would affect it in a larger degree. Indeed, nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy. We would, therefore, define the right of personal liberty in Article 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures. It so understood, all the acts of surveillance under Regulation 236 infringe the fundamental right of the petitioner under Article 21 of the Constitution."

iv. Subsequently, in the case of ***Gobind v State of M.P.***[6] the right of the police to make domiciliary surveillance was challenged to be inconsistent with the right to privacy embodied under Article 21 of the Constitution of India. The Hon'ble Supreme Court held that the police regulations were not in compliance with the essence of personal freedom and also accepted the right to privacy as a fundamental right guaranteed by the Constitution of India but favored evolution of the right to privacy on case to case basis and negated it to be absolute in nature. The Hon'ble Supreme Court observed as under:-

"28. The right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right, we do not think that the right is absolute."

v. A similar proposition has been upheld by the Hon'ble Supreme Court in the case of ***R. Rajagopal and Anr. v State of Tamil Nadu***[7]**,**in the course of its summary of the decision, as under: -

"26. We may now summarise the broad principles flowing from the above discussion:
(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent — whether truthful or otherwise and

[6] (1975) 2 SCC 148.
[7] (1994) 6 SCC 632.

whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy."

vi. Subsequently in the case of ***People's Union for Civil Liberties (PUCL) v Union of India***[8]the Hon'ble Supreme Court clearly held that:-

"17. We have, therefore, no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law".

vii. Recently, this issue was once again raised before the Hon'ble Supreme Court in the case of ***K. S. Puttaswamy (Retd.) v Union of India***[9], in which case the 'Aadhaar Card Scheme' was challenged on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy embodied in Article 21 of the Constitution of India. Given the ambiguity from prior judicial precedents on the constitutional status of right to privacy, the Hon'ble Supreme Court referred the matter to a constitutional bench consisting of 9 (nine) judges.

It was argued on behalf of the Petitioners that the right to privacy is very much a fundamental right which is co-terminus with the liberty and dignity of the individual and this right is found in Articles 14, 19, 20, 21 and 25 of the Constitution of India read with several international covenants. On the contrary, Union of India contended that 'right to privacy' is not a fundamental right guaranteed under the Constitution. The primary defence[10] of the Union of India was that (i) if the framers of the Constitution wanted to include the 'right to privacy' as a fundamental right, the same would have been specifically included within the Constitution; (ii) privacy is inherently a subjective and vague concept. The concept of privacy is difficult to define. Such vague concept cannot be elevated to a fundamental right; (iii) The present laws already confer sufficient protection to individuals against invasion of privacy; and (iv) 'right to privacy' is a legitimate claim having sanction of common law, each such claim cannot be elevated to fundamental right. The Hon'ble Supreme Court by its decision pronounced on August 24, 2017[11] unanimously held as under: -"*821. The reference is disposed of in the following terms:*

(i) The decision in M P Sharma which holds that the right to privacy is not protected by the Constitution stands over-ruled;

(ii) The decision in Kharak Singh to the extent that it holds that the right to privacy is not protected by the Constitution stands over-ruled;

(iii) The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

(iv) Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law."

Hon'ble Mr. Justice D.Y. Chandrachud[12], clearly held that: -

[8] (1997) 1 SCC 301.
[9] (2015) 8 SCC 735.
[10] Supra note 10, at Para 359, 395,530,579, 626, 627, 650.
[11] Justice K.S.Puttaswamy v UOI, 2017 SCC Online 996.
[12] Hon'ble Mr. Justice D.Y. Chandrachud wrote the judgment on his own behalf and on behalf of Hon'ble Mr. Justices J.S. Khehar, R.K. Agrawal & S. Abdul Nazeer.

"459. (A) Life and personal liberty are inalienable rights. These are rights which are inseparable from a dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian Constitution; …
(C) Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III; …
(F) Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Privacy attaches to the person since it is an essential facet of the dignity of the human being; …
(H) Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of (i) legality, which postulates the existence of law; (ii) need, defined in terms of a legitimate state aim; and (iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them; and
(I) Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual."

The Hon'ble Supreme Court rejected the arguments of the Union of India, and while analyzing the nature of right of privacy as regards its origin[13], the Hon'ble Supreme Court held that the right to privacy is intrinsic to and inseparable from human element in human being and core of human dignity[14]. Thus, it was held that privacy has both positive and negative content. The negative content acts as an embargo on the State from committing an intrusion upon the life and personal liberty of a citizen and its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual[15]. Therefore, the constitutional protection of privacy may give rise to two inter-related protections i.e. (i) against world at large, to be respected by all including State: right to choose that what personal information is to be released into the public space (ii) against the State: as necessary concomitant of democratic values, limited government and limitation on power of State[16].

As a result of this judgment the right to privacy has become 'more than mere common law right' and 'more robust and sacrosanct' than just any statutory right. Thus, now in the context of Article 21 of the Constitution, an invasion of privacy must be justified on the basis of 'a law' which stipulates a procedure which is fair, just and reasonable. It is to be noted that since **R.C. Cooper v UOI**[17], 'procedure established by law' in Article 21 has gained substantive

[13] Ibid, para 53-65, 531-536, 718, 736.
[14] Ibid, Para 459.
[15] Ibid, Para 403.
[16] Ibid, Para 304-307.
[17] (1970) 1 SCC 248

due process element as well[18] whereby even the contents of the law can be challenged being not in accordance with requirements of a valid law. Therefore, because of right of privacy being recognised as fundamental right, existing sectoral legislations, if challenged, may now have to pass the rigors of aforesaid test. Same would not have been the position, if privacy would have remained mere statutory or common law right.

As a consequence, now the "Adhaar Card Scheme" which was alleged to be in breach of fundamental right to privacy, will now be tested by the same standards by which a law which invades personal liberty under Article 21 is liable to be tested.

While discussing the right to information privacy in today's world, the Hon'ble Mr. Justice D.Y. Chandrachud concluded as under: -

> "*457. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union government while designing a carefully structured regime for the protection of the data. Since the Union government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in this judgment.*
> *746. We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy.*
> *747. The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State.*"

Current Issues Surrounding Data Privacy

i. The Hon'ble Supreme Court has laid down a threefold requirement for State's interference with the fundamental rights. While the State may intervene to protect legitimate state interests, (a) there must be a law in existence to justify an encroachment on privacy, which is an express requirement of Article 21 of the Constitution, (b) the nature and content of the law which imposes the restriction must fall within the zone of reasonableness mandated by Article 14, and (c) the means which are adopted by the legislature must be proportional to the object and needs sought to be fulfilled by the law[19]. Therefore, going forward any laws which seek to encroach upon the right of privacy of an individual would need to meet the test of proportionality and reasonableness. It will take a few years before jurisprudence around what constitutes reasonable and proportionate State interference settles *temporarily*. The validity of Adhar Scheme will now be tested on the basis of this judgment.

ii. It is often argued that India should adopt 'rights based' data protection model as opposed to today's 'consent based' model. Under the consent based model, the data controller is free to use, process and

[18] Mohd. Arif v Registrar, Supreme Court of India- (2014) 9 SCC 714.
[19] Supra note 10, at para 447.

share the data with any third parties, once the consent of the user is obtained. However, not many are aware of the actual consequences of the indiscreet data sharing at the time of providing consent. On the other hand the 'rights based' model allows the users to have greater rights over his/her data while requiring the data controller to ensure than such rights of the users are not breached. This leads to a greater autonomy of the users over their personal data.

iii. The decision of the Hon'ble Supreme Court empowers the citizens of India to seek judicial relief in case of breach of its data privacy rights. This could have an impact on the privacy and protection policies implemented by tech companies in India. The users can not only raise torts based claims but can also invoke their fundamental right to privacy.

Concerns and Difficulties

(i) What is the nature of data that is protected by the Indian legislature?

Since India does not have a comprehensive data protection mechanism, the main enactment that deals with protection of data is the IT Act and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 (the "**IT Rules**"). Under the IT Act and the IT Rules, what is primarily sought to be protected is 'personal information' and 'sensitive personal data or information', i.e. the information related to (i) password; (ii) financial information such as bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; and (vi) biometric information. However, the information which is freely available in public domain is not considered within the ambit of 'sensitive personal data or information'. Further, the provisions only deal with the collection and dissemination of information by a 'body corporate'.

In addition to the above, the respective sectoral regulators prescribe the data privacy measures required to be undertaken by (i) the telecommunications companies, (ii) the banking companies, (iii) the medical practitioners, and (iv) the insurance companies for protecting the privacy of data collected from the users and to avoid any unauthorised disclosures to third parties.

(ii) Who can collect the personal data?

Rules 5 of the IT Rules prescribes that no body corporate or any person on its behalf shall collect sensitive personal data or information unless (a) the information is collected for a lawful purpose connected with a function or activity of the body corporate; and (b) the collection of such information is considered necessary for that purpose.

Further, while collecting the information, the person sharing the information is required to be made aware of (i) the fact that the information is being collected; (ii) the purpose for which the information is being collected; (iii) the intended recipients of the information; (iv) the name and address of — (a) the agency that is collecting the information; and (b) the agency that will retain the information.

(iii) For what duration can the personal data be stored?

Anybody corporate or persons holding sensitive personal data or information on its behalf cannot retain it for longer than is required for the purposes for which the information may lawfully be used or is otherwise

required under any law for the time being in force and such information can be used only for the purpose for which it is collected.

Further the body corporate or any person on its behalf collecting the information, prior to the collecting of information, is required provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information, at any time while availing the services or otherwise, has the option to withdraw its consent given earlier.

(iv) To what extend can the personal data be shared with third parties?

The body corporate receiving the information can disclose sensitive personal data or information to any third party, provided prior permission from the provider of such information has been received, or such disclosure has been agreed to in the contract between the recipient and the provider of information, or where the disclosure is necessary for compliance of a legal obligation.

However, no such consent from the information provider is required where the information is shared with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.[20]

(v) What are the obligations of the employers in relation to the personal data collected of its employees?

The employers routinely collect 'sensitive personal information' of its employees such as health records, financial information etc. If the employer stores such personal information on a computer resource, such employer, if a body corporate, is required to have in place a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected. Alternatively the employers can implement '*the international Standard IS/ISO/IEC 27001 on Information Technology - Security Techniques - Information Security Management System – Requirements*'.

Further, under Rule 4 of the IT Rules, the employer, being a body corporate, who collects, receives, possess, stores, information of its employees, is required to have in place a privacy policy for handling of or dealing in such personal information. The employer is further required to make the privacy policy available for the employees for their review and publish the same on its website.

It is evident from above, that a comprehensive legislature regulating the collection and dissemination of personal data is the need of the hour. There are no comprehensive regulations which regulate the processing of personal data which is not per se 'sensitive personal data or information'.

Recently, WhatsApp Inc. after being acquired by Facebook Inc. changed its privacy policy, and the users were put to notice that "WhatsApp" account information of users would be shared with "Facebook" to improve "Facebook" ads and products experiences and the users' were asked to agree to the revised terms for continued use of

[20] Rule 6 of IT Rules

WhatsApp on or before September 25, 2016.[21] In view this development Karmanya Singh Sareen and another filed a writ petition before the Hon'ble High Court of Delhi contending that taking away the protection to privacy of data of users of "WhatsApp" and sharing the same with Facebook was in infringement of fundamental rights of the users guaranteed under Article 21 of the Constitution.

The Hon'ble Delhi High Court while deciding upon the case[22]ordered that if the users opt to completely delete the WhatsApp account, WhatsApp shall delete users' data completely from its servers and refrain from sharing users' data with Facebook, and so far as the users who opt to remain in "WhatsApp" are concerned, the existing information/data/details of such users upto September 25, 2016 shall not be shared with "Facebook" or any one of its group companies.

The court also directed the Government to consider whether it is feasible to bring messaging apps like WhatsApp under some statutory regulatory framework. This decision has however, been challenged before the Hon'ble Supreme Court of India through a special leave petition[23]. The matter is sub-judice and is presently pending for decision.[24] The verdict of the Hon'ble Supreme Court and the policy formulated by the Government will, however, have a far reaching impact on the manner in which personal data is handled in India, especially by non-state actors.

[21] Karmanya Singh Sareen v UOI, 2016 SCC Online Del 5334.
[22] Ibid.
[23] SLP (Civil) No. 804/2017
[24] https://www.theguardian.com/technology/2016/nov/08/facebook-pauses-whatsapp-data-sharing-after-ico-intervention

PART II

Protection of personal data is inextricably linked with privacy i.e. right of every person to enjoy his life and liberty without arbitrary interference with his private life, his family, his home or his correspondence etc. The word 'private' must be understood in contradistinction to 'public'. Therefore, the right to be let alone and its protection is extremely important in the present obtrusive information technology age. Since there is no one enactment which comprehensively governs data protection in India, the legal provisions governing the same need to be derived from various legislative enactments. In this part which have examined in detail the relevant legislative provisions which have an impact on the manner which is personal data is collected and handled in India. Further, the European data protection regulations have an extra-territorial applicability and have an impact on data 'controllers' and 'processors' outside of European Union ("**EU**"), but dealing with data subjects within the EU.

In this Section, we will examine the legal provisions under each sectoral legislation.

1. Information and Technology Act, 2000 and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011

The Government has provided a legal framework for data protection and privacy through the IT Act and the IT Rules in following manner:

The IT Act, after its amendments in 2008, is now equipped with multiple provisions catering to data protection, mandatory privacy policies, and penalties to be imposed on breach of such privacy policies. Below are the relevant provisions of the IT Act:

i. **Section 43 (a), (b) and (i) -** This section provides that any person, who without the permission of the owner or, any other person who may be in charge of a computer, computer system or computer network-

   a) accesses or secures access to such computer, computer system or computer network;
   b) downloads, copies, or extracts any data, computer data base or information from such computer, computer system or computer network which includes information or data held or stored in any removal storage medium;
   c) steals, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage shall be liable to pay damages.

shall be liable to pay damages by way of compensation not exceeding the sum of INR 1,00,00,000 (Rupees One Crore) to the person so affected.

ii. **Section 43A -** This section is bedrock of data protection and provides that where a body corporate possessing, dealing or handling any sensitive personal data or information[25] in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures[26] and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation, which shall not exceed a sum of INR 5,00,00,000 (Rupees Five Crore).

iii. **Section 66 C –** This section deals with identity theft and provides that whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment for a term which may extend up to three years and shall also be liable to pay a fine of up to INR 1,00,000 (Rupees One Lakh)

iv. **Section 66 E –** This section provides that whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy[27] of that person shall be punished with imprisonment which may extend up to three years or with fine not exceeding INR 200,000/- (Indian Rupees Two Lakh) or with both.

v. **Section 72 –** This section provides that any person who has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned and thereafter, discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to INR 1,00,000 (Rupees One Lakh) , or with both.

vi. **Section 72A -** This section provides that, any person, including an intermediary[28] who, while providing services under the terms of a lawful contract, has secured access to any material containing personal information

---

[25] The term "**sensitive personal data or information**" of a person is defined to mean *such personal information which consists of information relating to— (i) password; (ii) financial information such as Bank account or credit card or debit card or other payment instrument details; (iii) physical, physiological and mental health condition; (iv) sexual orientation; (v) medical records and history; (vi) biometric information; (vii) any detail relating to the above clauses as provided to body corporate for providing service; and (viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise: provided that, any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of these regulations.*

[26] The term "**reasonable security practices and procedures**" has been defined to mean *security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.*

[27] The term "**under circumstances violating privacy**" has been defined to mean *circumstances in which a person can have a reasonable expectation that— (i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.*

[28] The term "**intermediary**" with respect to any particular electronic records, has been defined to mean *any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes.*

about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend up to three years, or with a fine which may extend up to INR 5,00,000 (Rupees Five Lakh), or with both.

The IT Rules require body corporates[29] holding sensitive personal information of users to maintain certain specified security standards. Below are the relevant provisions of the IT Rules:

vii. **Rule 4 -** This rule mandates that corporate bodies or any person who on behalf of body corporate, collects, receives, possesses, stores, deals or handles information of provider of information should provide for a privacy policy for handling of or dealing in personal information[30] including sensitive personal data or information and ensure that the same are available for view by such providers of information who have provided such information under lawful contract. Such policy shall be published on the website of the body corporate or any person on its behalf and shall provide for—

a) clear and easily accessible statements of its practices and policies;
b) type of personal or sensitive personal data or information collected under rule 3[31];
c) purpose of collection and usage of such information;
d) disclosure of information including sensitive personal data or information as provided in rule 6;
e) reasonable security practices and procedures as provided under rule 8.

viii. **Rule 5 –** This rule lays down the procedure to be followed for the collection of information by the body corporate or any person on its behalf.

A. Consent has to be obtained in writing through letter or fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.

B. The body corporate or any person on its behalf shall not collect sensitive personal data or information unless —

a) the information is collected for a lawful purpose connected with a function or activity of the body corporate or any person on its behalf; and
b) the collection of the sensitive personal data or information is considered necessary for that purpose.

C. While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of —

[29] The term body corporate has been defined in explanation (i) to Section 43A of IT Act as "body corporate" means "*any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities*".
[30] The term "**personal information**" has been explained to mean *any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such person.*
[31] Rule 3 of the IT Rules provides for the definition of 'sensitive personal data or information'.

a) the fact that the information is being collected;
b) the purpose for which the information is being collected;
c) the intended recipients of the information; and
d) the name and address of —
(i) the agency that is collecting the information; and
(ii) the agency that will retain the information.

D. Further, the body corporate or any person on its behalf holding sensitive personal data or information cannot not retain that information for longer than is required for the purpose for which the information may lawfully be used or is otherwise required under any other law for the time being in force. The information collected can only be used for the purpose for which it has been collected.

E. Body corporate or any person on its behalf shall permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal information or sensitive personal data or information found to be inaccurate or deficient is corrected or amended as feasible. However, a body corporate is not responsible for the authenticity of the personal information or sensitive personal data or information supplied by the provider of information to such boy corporate or any other person acting on behalf of such body corporate.

F. Body corporate or any person on its behalf shall, prior to the collection of information including sensitive personal data or information, provide an option to the provider of the information to not to provide the data or information sought to be collected. The provider of information shall, at any time while availing the services or otherwise, also have an option to withdraw its consent given earlier to the body corporate. Such withdrawal of the consent shall be sent in writing to the body corporate. In the case of provider of information not providing or later on withdrawing its consent, the body corporate has the option not to provide goods or services for which the said information was sought.

G. Body corporate or any person on its behalf is required keep the information secure as provided in rule 8 (set out below).

ix. **Rule 6 -** This rule pertains to the disclosure of information by the body corporate to any third party.

A. It provides that, disclosure of sensitive personal data or information by body corporate to any third party shall require prior permission from the provider of such information, who has provided such information under lawful contract or otherwise, unless such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation. However, its mandatory to share the information, without obtaining prior consent from provider of information, with Government agencies as mandated under law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency has to send a request in writing to the body corporate possessing the sensitive personal data or information

stating clearly the purpose of seeking such information. The Government agency shall also state that the information so obtained shall not be published or shared with any other person.

B. Notwithstanding anything contain in such Rule, any sensitive personal data on information can disclosed to any third party by an order under the law for the time being in force.

C. The body corporate or any person on its behalf cannot publish the sensitive personal data or information.

D. The third party receiving the sensitive personal data or information from body corporate or any person on its behalf cannot disclose it further.

x. **Rule 8** - While handling such personal information or sensitive personal data or information, the corporate body is required to comply with reasonable security practices and procedures.

A. A body corporate or a person on its behalf is considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security program and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.

B. In the event of an information security breach, the body corporate or a person on its behalf is required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security program and information security policies. The international Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" is one such standard which must be adhered to.

C. Any industry association or an entity formed by such an association, whose members are self-regulating by following other than IS/ISO/IEC codes of best practices for data protection, shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.

The body corporate or a person on its behalf who has implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection, is deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures ate to be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf, undertake significant up gradation of its process and computer resource.

2. Regulatory Bodies

3.1 Telecom Regulatory Authority of India

In the process of providing services, the telecom service providers have the ability to gain access to substantial personal information of the service recipient. In order to protect the data of the service recipients, a number of sector specific rules and regulations have been formulated:

A. Indian Telegraph Act, 1885 ("Telegraph Act**"):**

i. **Section 5 -** This section lays down the power of the Government to take possession of licensed telegraphs and to order interception of messages on the occurrence of any public emergency, or in the interest of the public safety, or in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence. In such an event the Central Government or a State Government or any officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order. Provided that press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under such section.

ii. **Section 24 -** This section provides for the consequences of attempting to learn the contents of messages unlawfully. If any person does any of the acts mentioned in section 23[32] with the intention of unlawfully learning the contents of any message, or of committing any offence punishable under the Telegraph Act, he may (in addition to the fine with which he is punishable under section 23) be punished with imprisonment for a term which may extend to one year.

iii. **Section 25 -** The section provides for the consequences of intentionally damaging or tampering with telegraphs. If any person, intending to prevent or obstruct the transmission or delivery of any message, or to intercept or to acquaint himself with the contents of any message, or to commit mischief, damages, removes, tampers with or touches any battery, machinery, telegraph line, post or other thing whatever, being part of or used in or about any telegraph or in the working thereof, shall be punished with imprisonment for a term which may extend to three years, or with fine or with both.

[32] Section 23 provides that any person, who without permission of a competent authority, enters the signal-room of a telegraph office of the Government, or of a person licensed under the Telegraph Act, or, enters a fenced enclosure round such a telegraph office in contravention of any rule or notice not to do so, or refuses to quit such room or enclosure on being requested to do so by any officer or servant employed therein, or willfully obstructs or impedes any such officer or servant in the performance of his duty, shall be punished with fine which may extend to INR 500 (Rupees Five Hundred).

iv. **Section 26 -** This section states that, if any telegraph officer, or any person, not being a telegraph officer but having official duties connected with any office which is used as a telegraph office, willfully, secrets, makes away with or alters any message which he has received for transmission or delivery, or willfully, and otherwise than in obedience to an order of the Central Government or of a State Government, or of an officer specially authorized by the Central or a State Government to make the order, omits to transmit, or intercepts or detains, any message or any part thereof, or otherwise than in pursuance of his official duty or in obedience to the direction of a competent court, discloses the contents or any part the contents of any message, to any person not entitled to receive the same, or divulges the purport of any telegraphic signal to any person not entitled to become acquainted with the same, shall be punished with imprisonment for a term which may extend to three years, or with fine, or with both.

v. **Section 30 -** The section provides that, if any person fraudulently retains, or willfully secretes, makes away with or detains a message which ought to have been delivered to some other person, or, being required by a telegraph officer to deliver up any such message, neglects of refuses to do so, shall be punished with imprisonment for a term which may extend to two years, or with fine, or with both.

B. The Department of Telecommunications has provided various standard form agreements for its stakeholders and service providers pursuant to the Telegraph Rules. Listed below are the privacy protection provisions enumerated under these agreements:

i. **Clause 21 of the National Long Distance Licence requires** the licensee, i.e., the telecommunication provider to adhere to certain confidentiality conditions with respect to customer information. It provides that, any encryption equipment connected to the licensee's network for specific requirements should have prior evaluation and the approval of the licensor or officer specially designated for this purpose. However, the licensee shall have the responsibility to ensure protection of privacy of communications and to ensure that unauthorised interception of message does not take place.

Further, the licensee must take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business, to whom it provides the service, and from whom it has acquired such information by virtue of those services, and shall use its best endeavours to secure that:

a) No person acting on behalf of the licensee, or the licensee, divulges or uses any such information, except as may be necessary in the course of providing such services to the third party; and
b) No such person seeks such information other than is necessary for the purpose of providing services to the third party.

Provided that this shall not apply where, the information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or the information is already open to the public and otherwise is known.

The licensee also has the obligation to take necessary steps to ensure that the licensee, and any person(s) acting on its behalf, its employees, observe confidentiality of customer information.

ii. **Clause 37, 39 of the Unified Access Service License and Clause 42 of the Cellular Mobile Telephone Service License** require the licensee, i.e., the telecommunication provider to adhere to certain confidentiality conditions with respect to customer information to ensure protection of privacy of communication and to ensure that unauthorised interception of message does not take place. It provides that the licensee shall not employ bulk encryption equipment in its network. Any encryption equipment connected to the licensee's network for specific requirements has to have prior evaluation and approval of the licensor or officer specially designated for the purpose.

Further, the licensee has to take all necessary steps to safeguard the privacy and confidentiality of any information about a third party and its business to whom it provides the service and from whom it has acquired such information by virtue of the service provided and shall use its best endeavors to secure that:

a) No person acting on behalf of the licensee or the licensee divulges or uses any such information except as may be necessary in the course of providing such service to the third party;
b) No such person seeks such information other than is necessary for the purpose of providing service to the third party.

However the aforesaid provisions do not apply where the information relates to a specific party and that party has consented in writing to such information being divulged or used, and such information is divulged or used in accordance with the terms of that consent; or the information is already open to the public and otherwise known.

The licensee also has the obligation to take necessary steps to ensure that the licensee, and any person(s) acting on its behalf, its employees, observes confidentiality of customer information.

The Telecom Regulatory Authority of India (TRAI) has issued a directive[33] to all telecom and Internet service providers (TSPs) requiring them to ensure compliance of the terms and conditions of the licence regarding confidentiality of information of subscribers and privacy of communications.

C. Further, telephone tapping, sharing of a person's personal data by messaging apps to other entities are certain issues that have been delved upon by the courts of India.

i. In the case of ***PUCL v Union of India,***[34] the petitioner challenged the constitutional validity of section 5(2) of the Telegraph Act; in the alternative it was contended that the said provisions be suitably read-down to include procedural safeguards to rule out arbitrariness and to prevent the indiscriminate telephone-tapping. While analyzing section 5(2) of the RTI Act, the Hon'ble Supreme Court held that the section clearly lays down

[33] http://www.trai.gov.in/sites/default/files/Directions-26-Feb-10.pdf, last accessed on 30.08.2017.
[34] (1997) 1 SCC 301.

the situations and conditions under which the power to intercept messages or conversations can be exercised. However, since rules under section 7(2)(b) have not been framed, the substantive law does not have procedural backing to ensure fair and reasonable exercise of power. The Hon'ble Supreme Court held *"that right to privacy is part of the right to life under Article 21, a requisite of which is procedure established by law*." Further, the Hon'ble Supreme Court observed that *"telephone tapping, unless it is within the restrictions of Article 19(2), is a violation of the right to privacy; and the laying down of procedural safeguards was necessary to protect the aforementioned right of the people*." The Hon'ble Supreme Court held that an order for telephone-tapping under section 5(2) shall be issued by Home Secretary of Central or State Government who shall maintain proper records of intercepted communications and disclosure of materials intercepted, additionally these orders would be examined by a review committee, which would set aside orders in contravention with the mentioned provision. Further, the total period for operation of the order shall not exceed six months.

ii. Post the above mentioned judgment, **Rule 419A** was inserted in Indian Telegraph Rules, 1951 ("**Telegraph Rules**") which states that the directions for interception of any message or class of messages under section 5 of the Telegraph Act shall not be issued except by an order made by the Secretary to the Government of India in the Ministry of Home Affairs in the case of Government of India and by the Secretary to the State Government in-charge of the Home Department in the case of a State Government. In unavoidable circumstances, such order may be made by an officer, not below the rank of a Joint Secretary to the Government of India, who has been duly authorized by the Union Home Secretary or the State Home Secretary, as the case may be:

In emergent cases, however,— (i) in remote areas, where obtaining of prior directions for interception of messages or class of messages is not feasible; or (ii)
(ii) for operational reasons, where obtaining of prior directions for interception of message or class of messages is not feasible; the required interception of any message or class of messages shall be carried out with the prior approval of the Head or the second senior most officer of the authorized security *i.e.* Law Enforcement Agency at the Central Level and the officers authorised in this behalf, not below the rank of Inspector General of Police at the state level but the concerned competent authority shall be informed of such interceptions by the approving authority within three working days and that such interceptions shall be got confirmed by the concerned competent authority within a period of seven working days. If the confirmation from the competent authority is not received within the stipulated seven days, such interception shall cease and the same message or class of messages shall not be intercepted thereafter without the prior approval of the Union Home Secretary or the State Home Secretary, as the case may be. Further, records pertaining to such directions for interception and of intercepted messages shall be destroyed by the relevant competent authority and the authorized security and Law Enforcement Agencies every six months unless these are, or likely to be, required for functional requirements. The service providers shall destroy records pertaining to directions for interception of message within two months of discontinuance of the interception of such messages and in doing so they shall maintain extreme secrecy.

iii. In case of Amar Singh v Union of India[35], the Hon'ble Supreme Court while dealing with allegation of beach of fundamental right to privacy relating to telephone interception, imposed "*a kind of duty to care*" upon non-State service providers and held that "*service provider has to act as a responsible agency and cannot act on any communication*". The Hon'ble Supreme Court further held that "*act immediately but verify simultaneously*".

D. Consultation Paper issued by the Telecom Regulatory Authority of India ("**TRAI**")

Keeping in mind the quantum of personal data collected by the telecom operators, the manners in which the data pertaining to users can be accessed and controlled, and the general lack of awareness amongst users about the harmful objectives for which such information can be utilized, the TRAI on August 9, 2017 released a consultation paper on 'privacy, security and ownership of the data in the telecom sector', inviting comments from the stakeholders. TRAI has requested comments primarily on the following issues:

i. Are the data protection requirements currently applicable to all the players in the eco-system in India sufficient to protect the interests of telecom subscribers?

ii. Should the user's consent be taken before sharing his/her personal data for commercial purposes? What are the measures that should be considered in order to empower users to own and take control of his/her personal data?

iii. Given the fears related to abuse of this data, is it advisable to create a technology enabled architecture to audit the use of personal data, and associated consent?

iv. Should government or its authorized authority setup a data sandbox, which allows the regulated companies to create anonymized data sets which can be used for the development of newer services?

v. What are the key issues of data protection pertaining to the collection and use of data by various other stakeholders in the digital ecosystem, including content and application service providers, device manufacturers, operating systems, browsers, etc.?

vi. Is there a need for bringing about greater parity in the data protection norms applicable to telecom service providers and other communication service providers offering comparable services (such as Internet based voice and messaging services)?

vii. What should be the legitimate exceptions to the data protection requirements imposed on telecom service providers and other providers in the digital ecosystem and how should these be designed?

[35] (2011) 7 SCC 69.

viii. What are the measures that can be considered in order to address the potential issues arising from cross border flow of information and jurisdictional challenges in the digital ecosystem?

3.2 Banking Regulators

A. State Bank of India Act, 1955

i. **Section 44 -** This section provides for a secrecy clause by virtue of which, the bank as a whole and its directors, local boards, auditors, advisers, officers or other employees of the State Bank are obligated as to fidelity and secrecy, by a declaration in prescribed form. It provides that, the State Bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with the law or practice and usage customary among bankers, necessary or appropriate for the State Bank to divulge such information.

B. Banking Companies (Transfer and Acquisition of Undertakings) Act, 1980

i. **Section 13 –** This section provides that, every corresponding new bank shall observe, except as otherwise required by law, the practices and usages customary among bankers, and, in particular, it shall not divulge any information relating to or to the affairs of its constituents except in circumstances in which it is, in accordance with law or practices and usages customary among bankers, necessary or appropriate for the corresponding new bank to divulge such information.

Further, every Director, member of a local Board or a committee, or Auditor, Adviser, officer or other employee, custodian of a corresponding new bank shall, before entering upon his duties, make a declaration of fidelity and secrecy in the prescribed form.

C. Credit Information Companies (Regulation) Act, 2005 ("CIC Act**") and Credit Information Companies Regulations, 2006 ("**CIC Regulations**")**

i. **Section 19 -** This section requires a credit information company[36], credit institutions[37] and specified users[38] to take steps in order preserve accuracy and security of credit information[39], to ensure that the data relating to the credit information maintained by them is accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure thereof.

ii. **Section 20 –** This section provides that every credit information company, credit institutions and specified users shall adopt privacy principles in relation to credit information and shall adopt the following privacy principles in relation to collection, processing, collating, recording, preservation, secrecy, sharing and usage of credit information, namely:

a) the principles—

(i) which may be followed by every credit institution for collection of information from its borrowers and clients and by every credit information company, for collection of information from its member credit institutions or credit information companies, for processing, recording, protecting the data relating to credit information furnished by, or obtained from, their member credit institutions or credit information companies, as the case may be, and sharing of such data with specified users;
(ii) which may be adopted by every specified user for processing, recording, preserving and protecting the data relating to credit information furnished, or received, as the case may be, by it;
(iii) which may be adopted by every credit information company for allowing access to records containing credit information of borrowers and clients and alteration of such records in case of need to do so;

b) the purpose for which the credit information may be used, restriction on such use and disclosure thereof;

---

[36] *The term "**credit information company**" has been defined to mean a company formed and registered under the Companies Act, 1956 (1 of 1956) and which has been granted a certificate of registration under sub-section (2) of section 5.*

[37] The term "**credit institution**" has been defined to mean *a banking company and includes—(i) a corresponding new bank, the State Bank of India, a subsidiary bank, a co-operative bank, the National Bank and regional rural bank; (ii) a non-banking financial company as defined under clause (f) of section 45-I of the Reserve Bank of India Act, 1934 (2 of 1934); (iii) a public financial institution referred to in section 4A of the Companies Act, 1956 (1 of 1956); (iv) the financial corporation established by a State under section 3 of the State Financial Corporation Act, 1951 (63 of 1951); (v) the housing finance institution referred to in clause (d) of section 2 of the National Housing Bank Act, 1987 (53 of 1987); (vi) the companies engaged in the business of credit cards and other similar cards and companies dealing with distribution of credit in any other manner; (vii) any other institution which the Reserve Bank may specify, from time to time, for the purposes of this clause.*

[38] The term "**specified user**" has been defined to mean *any credit institution, a credit information company being a member under sub-section (3) of section 15, and includes such other person or institution as may be specified by regulations made, from time to time, by the Reserve Bank for the purpose of obtaining credit information from a credit information company.*

[39] The term "**credit information**" has been defined to mean *any information relating to—(i) the amounts and the nature of loans or advances, amounts outstanding under credit cards and other credit facilities granted or to be granted, by a credit institution to any borrower; (ii) the nature of security taken or proposed to be taken by a credit institution from any borrower for credit facilities granted or proposed to be granted to him; (iii) the guarantee furnished or any other non-fund based facility granted or proposed to be granted by a credit institution for any of its borrowers; (iv) the credit worthiness of any borrower of a credit institution; (v) any other matter which the Reserve Bank may, consider necessary for inclusion in the credit information to be collected and maintained by credit information companies, and, specify, by notification, in this behalf.*

c) the extent of obligation to check accuracy of credit information before furnishing of such information to credit information companies or credit institutions or specified users, as the case may be;
d) preservation of credit information maintained by every credit information company, credit institution, and specified user as the case may be (including the period for which such information may be maintained, manner of deletion of such information and maintenance of records of credit information);
e) networking of credit information companies, credit institutions and specified users through electronic mode;
f) any other principles and procedures relating to credit information which the Reserve Bank may consider necessary and appropriate and may be specified by regulations.

iii. **Section 22** - This section provides that any unauthorized access to credit information in the possession or control of a credit information company or a credit institution or a specified user shall be punishable with fine which may extend to INR 1,00,000 (Rupees One Lakh) in respect of each offence and if he continues to have such unauthorised access, with further fine which may extend to INR 10,000 (Rupees Ten Thousand) for every day on which the default continues and such unauthorised credit information shall not be taken into account for any purpose.

iv. **Section 29 –** This section provides for secrecy and fidelity to be maintained by every credit information company with respect to the credit information except as otherwise required by law, the practices and usages customary among credit information companies and it shall not divulge any information relating to, or to the affairs of, its members or specified users. Further, every chairperson, director, member, auditor, adviser, officer or other employee of a credit information company shall, before entering upon his duties, make a declaration of fidelity and secrecy.

v. **Regulation 10** – This regulation specifies that in addition to section 20 of the CIC Act, every credit information company, credit institution and specified user, shall adopt the following privacy principles in relation to their functioning, namely:

a) Care in collection of credit information - properly and accurately recorded, collated and processed; protected against loss, unauthorised access, use, modification or disclosure thereof;
b) Keep the credit information furnished by it updated, accurate and complete;
c) Establish and adopt procedures relating to disclosure to a person, upon his request, his own credit information and subject to his satisfactory identification;
d) Retain credit information collected, maintained and disseminated by them for a minimum period of seven years;
e) Develop guidelines and procedures to be adopted by them, with the approval of the Reserve Bank of India in respect of preservation and destruction of credit information.

vi. **Regulation 11** – This regulation provides for the principles and procedures relating to personal data. Every credit information company, credit institution and specified user, shall adopt the following principles:

a) Personal data shall not be collected, or published or disclosed except for the purposes relating to their functions under the CIC Act, or in relation to their capacity and function as an employer of an individual who is or has been in their employment;
b) Ensure that, before such data is collected or, if that is not practicable, as soon as practicable after such data is collected, the individual concerned is informed about such collection; and such data maintained by the should be protected against any loss, or unauthorized access, or use, or modification or disclosure, thereof;
c) Retain personal data collected, maintained and disseminated by them for a minimum period of seven years;
d) Develop guidelines and procedures to be adopted by them, with the approval of the Reserve Bank of India in respect of preservation and destruction of such personal data.

D. The Public Financial Institutions (Obligation As To Fidelity And Secrecy) Act, 1983 ("PFI Act**")**

i. **Section 3 -** This section provides that a public financial institution shall not, except as otherwise provided in any other law for the time being in force, divulge any information relating to, or to the affairs of, its constituents except in circumstances in which it is, in accordance with the law or practice and usage, customary among bankers, necessary or appropriate for the public financial institution to divulge such information.

ii. **Section 4 -** This section provides that, every director, member of any committee, auditor or officer or any other employee of a public financial institution to which the PFI Act applies, shall, before entering upon his duties make a declaration of fidelity and secrecy in the form set out in the PFI Act.

E. Financial Privacy.

In the case of ***District Registrar and Collector, Hyderabad v Canara Bank***[40], the Hon'ble Supreme Court clearly held and recognized that right to privacy of person extends to documents of the person/customer which are with bank and must remain confidential. Accordingly, the Hon'ble Supreme Court upheld the order of the High Court, which has invalidated Section 43 of the Stamp Act (as amended in Andhra Pradesh), which empowered the Collector to inspect registers, books and records, papers, documents and proceedings in the custody of any public officer 'to secure any duty or to prove or would lead to the discovery of a fraud or omission'.

3.3 Medicine and Healthcare

A. Mental Health Act, 1987 ("MH Act**")**

i. **Section 13 -** This section provides for inspection of psychiatric hospitals and psychiatric nursing homes and visiting patients by an inspecting officer at any time and the inspecting officer may require the production of

[40] (2005) 1 SCC 496.

any records maintained as per the MH Act. Provided that any personal records of a patient so inspected shall be kept confidential except wherein the inspecting officer is satisfied that any in-patient in a psychiatric hospital or psychiatric nursing home is not receiving proper treatment and care, he may report the matter to the licensing authority and thereupon the licensing authority may issue such direction as it may deem fit to the medical officer-in charge of the licensee of the psychiatric hospital, or, as the case may be, the psychiatric nursing home and every such medical officer-in-charge or licensee shall be bound to comply with such directions.

ii. **Section 38 –** This section provides that visitors of psychiatric patients will not be entitled to inspect any personal records of an in-patient which in the opinion of the medical officer-in-charge are confidential in nature.

B. Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002

ix. **Regulation 7.14** – This regulation provides that, the registered medical practitioner shall not disclose the secrets of a patient that have been learnt in the exercise of his / her profession except – in a court of law under orders of the presiding judge; in circumstances where there is a serious and identified risk to a specific person and / or community; and notifiable diseases. In case of communicable / notifiable diseases, concerned public health authorities should be informed immediately.

C. Health record privacy and harm to others.

In case of Mr X v Hospital Z[41] the Hon'ble Supreme Court held that the right to privacy of the patient and duty to maintain confidentiality on part of doctor is subject to protection of health of others. Accordingly, in this case it was held that the disclosure that the appellant was HIV+ was held not to violate the right to privacy of the appellant on the ground that the woman to whom he was to be married 'was saved in time by such disclosure and from the risk of being infected'.

3.4 Insurance

A. Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017

i. **Regulation 9 –** This regulation provides that a referral company[42] approved by the IRDAI and registered with the insurer will not provide details of customers without their prior written consent or provide details of any person/firm/company with whom they have not had any recorded business transaction.

[41] (1998) 8 SCC 296. Also see (2003) 1 SCC 500.
[42] The term "**referral company**" has been defined to mean *a company formed and registered under the Companies Act, 1956 and approved by the IRDAI under sub-regulation (3) of regulation 6 except as otherwise permitted in these regulations.*

B. Insurance Regulatory and Development Authority of India (Maintenance of Insurance Records) Regulations, 2015

i. **Regulation 3 –** This rule states that every insurer maintaining records of the insurance policies and its relevant data and such a system of maintenance should have the necessary security features. The manner and maintenance of the records shall be as per policy framed by the insurers and approved by their board. For maintaining records in electronic form, the policy should include:

a) Processing and electronic maintenance of records,
b) Privacy and security of policyholder and claim data,
c) Handling virus, vulnerability issues,
d) Security of hardware and software,
e) Backups, disaster recovery and business continuity; and
f) Data archival.

The policy will also include a detailed plan to review the implementation of the maintenance and storage of records which will be overseen by the risk management committee of the board of the insurers. The records will be held in data centres located and maintained in India only.

C. Insurance Regulatory and Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017

These regulations mandate that the board of directors of the insurance to formulate an outsourcing policy wherein assessment of risks involved in outsourcing including the confidentiality of data, quality of services rendered under outsourcing contracts is addressed.[43] Further, the outsourcing agreements are required to contain information and asset ownership rights, information technology, data security and protection of confidential information, contract termination clause specifying orderly handing over of data, assets etc.[44]

i. **Regulation 12** – This regulation provides for confidentiality and security measures to be undertaken by the insurers while outsourcing its services. The insurer shall satisfy itself that the outsourcing service provider's security policies, procedures and controls will enable the insurer to protect confidentiality and security of policyholders' information even after the contract terminates. It shall be the responsibility of the insurer to ensure that the data or information parted to any outsourcing service provider under the outsourcing agreements remains confidential. An insurer shall take into account any legal or contractual obligations on the part of the outsourcing service provider to disclose the outsourcing arrangement and circumstances under which insurer's customer data may be disclosed. In the event of termination of the outsourcing agreement, the insurer should ensure that the customer data is retrieved from the service provider and ensure there is no further use of customer data by the service provider.

[43] Regulation 7
[44] Regulation 11

3. Right to Information Act, 2005 ("RTI Act")

The RTI Act was enacted to enable private citizens to access information[45] under the control of public authorities[46] in order to promote transparency and accountability in the working of every public authority. Nevertheless, the RTI Act also provides for exceptions to disclosure of information.

i. **Section 8 (1)(j)** – This section provides that the authorities are under no obligation to provide information to citizens regarding *inter alia* information which relates to personal information, the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information. Provided that the information that cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

There have been several decisions of the courts of India which elucidate the above provisions.

ii. In the case of ***Secretary General, Supreme Court of India v Subhash Chandra Agarwal,***[47] the matter before the Hon'ble High Court of Delhi was whether right to information could be asserted and maintained with regard to information about the declaration of personal assets of Judges. The Hon'ble Delhi High Court held that the respondent "*had right to information in respect of the information regarding making of declarations by the judges of the Supreme Court pursuant to the 1997 Resolution"*[48]*. The duty to confirm or deny the compliance with the 1997 Resolution would not amount to a breach of confidentiality unless the request is such that mere confirmation would reveal the gist of the information. The disclosure of contents of the aforementioned declaration must be assessed subject to conditions laid down in section 8(1)(j)*. In view of section 8(1)(j), *personal information including tax returns, medical records etc. cannot be disclosed*. *This bar is lifted if the applicant can show sufficient public interest in disclosure and the authority duly notifies and considers the views of the individual concerned with the information*.

---

[45] The term "**information**" has been defined to mean *any material in any form, including records, documents, memos, e-mails, opinions, advices, press releases, circulars, orders, logbooks, contracts, reports, papers, samples, models, data material held in any electronic form and information relating to any private body which can be accessed by a public authority under any other law from the time being in force.*

[46] The term "**public authority**" has been defined to mean *any authority or body or institution of self-government established or constituted – (a) by or under the Constitution; (b) by any other law made by the Parliament; (c) by any other law made by the State Legislature; (d) by notification issued or order made by the appropriate Government , and includes any – (i) body owned, controlled or substantially financed; (ii) non-Government organisation substantially financed, directly or indirectly by funds provided by the appropriate Government.*

[47] AIR 2010 Delhi 159

[48] Resolution adopted on May 7, 1997 that *"every Judge should make a declaration of all his/her assets in the form of real estate or investments (held by him/her in his/her own name or in the name of his/her spouse or any person dependent on him/her) within a reasonable time of assuming office and in the case of sitting Judges within a reasonable time of adoption of this Resolution and thereafter whenever any acquisition of a substantial nature is made, it shall be disclosed within a reasonable time. The declaration so made should be to the Chief Justice of the Court. The Chief Justice should make a similar declaration for the purpose of the record. The declaration made by the Judges or the Chief Justice, as the case may be, shall be confidential."*

iii. In the case of ***Girish Ramchandra Deshpande v Central Information Commissioner and Ors.***[49]**,** the question before the Hon'ble Supreme Court was whether matters pertaining to an individual's service career and details of his assets and liabilities, movable and immovable properties, etc. can be given treated as personal information as defined under section 8(1)(j) of the RTI, Act. The Hon'ble Supreme Court held that "*performance of an employee in an organization is a matter between the employer and the employee and the particulars called for by the petitioner including show-cause notices and orders of censure and/or punishment, fall under the ambit of personal information*. *Details disclosed under income tax returns are also to be treated similarly*". It can only be disclosed if the Central Public Information Officer, State Public Information Officer or the Appellate Authority is satisfied that the larger public interest justifies the disclosure of such information.

iv. In the case of ***Mr. Surupsingh Hrya Naik v State of Maharashtra through Additional Secretary, General Administration Department and Ors.***[50]**,** the matter before the Hon'ble Supreme Court was whether the petitioner can be allowed to claim privilege or confidentially in respect of the medical records maintained by a public authority, during the period of his incarceration. The petitioner in this case was a member of the Legislative Assembly. The Hon'ble Supreme Court held that the confidentiality required to be maintained of the medical records of a patient, including a convict, considering the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Regulations) cannot override the provisions of the RTI Act. "*If there be inconsistency between the Regulations and the RTI Act, the provisions of the RTI Act would prevail over the Regulations. The Act carves out some exceptions, including the release of personal information, the disclosure of which has no relationship to any public activity or interest or which would cause unwarranted invasion of the right to privacy*. In such cases disclosure is made if the larger public interest justifies the same. *Normally records of a person sentenced or convicted or remanded to police or judicial custody, if during that period such person is admitted in hospital and nursing home, should be made available to the person asking the information provided such hospital nursing home is maintained by the state or public authority or any other public body*. It is only in rare and in exceptional cases and for good and valid reasons recorded in writing can the information may be denied. *However, before disclosing to third party, the petitioner must be given the right to be heard as to why the information should not be disclosed".*

v. In the case of ***Subhash Chandra Agarwal v The Registrar, Supreme Court of India and Ors.***[51], the question before the Hon'ble Delhi High Court was regarding the disclosure of information including details of medical facilities availed by individual judges. The Hon'ble Delhi High Court considered the fact that the total expenditure incurred for the medical treatment of the judges for the period in question was already furnished by the Central Public Information Officer and that it is not the case of the appellant that the said expenditure is excessive or exorbitant, and held that the "*details of medical facilities availed is personal information and there is no public interest warranting the disclosure of the same*".

[49] (2013)1 SCC 212
[50] AIR 2007 Bom 121
[51] 2015 (150) DRJ 628

4. The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 ("Aadhaar Act"), Aadhaar (Data Security) Regulations, 2016 ("Aadhaar DS Regulations") and Aadhaar (Sharing of Information) Regulations, 2016 ("Sharing Regulations")

The Government has recently mandated the use of the biometric database - Aadhaar to deliver targeted subsidies, benefits and services.

i. **Section 28 –** This section provides that subject to the provisions of the Aadhaar Act, the relevant authorities shall ensure the security of identity information and authentication records of individuals. The authority has to take all necessary measures to ensure that the information in the possession or control of the authority, including information stored in the Central Identities Data Repository, is secured and protected against access, use or disclosure not permitted under the Aadhaar Act or regulations made thereunder, and against accidental or intentional destruction, loss or damage.

ii. **Section 29** – This section prohibits the sharing of core biometric information[52] collected or created under the Aadhaar Act, with anyone for any reason; or be used for any purpose other than generation of Aadhaar numbers and authentication under the Aadhaar Act. No identity information available with a requesting entity shall be (*a*) used for any purpose, other than that specified to the individual at the time of submitting any identity information for authentication; or (*b*) disclosed further, except with the prior consent of the individual to whom such information relates. No Aadhaar number or core biometric information shall be published, displayed or posted publicly, except for the purposes as may be specified by regulations.

iii. **Section 30 –** This section states that biometric information will be deemed to be sensitive personal information and the provisions contained in the IT Act and the rules made thereunder shall apply to such information, in addition to, and to the extent not in derogation of the provisions of the Aadhaar Act.

iv. **Section 33** – This section provides that information as mentioned in sections 28 and 29 may be disclosed in the event of an pursuant to an order of a court not inferior to that of a District Judge; or in the interest of national security in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India specially authorised in this behalf by an order of the Central Government.

[52] The term "**core biometric information**" has been defined to mean *finger print, iris scan, or such other biological attributes of an individual as may be specified by regulations*.

v. **Section 37**– This section provides for penalty for disclosing identity information[53] and whoever does so will be punishable with imprisonment for a term which may extend to three years or with a fine which may extend to INR 10,000/- (Rupees Ten Thousand) or, in the case of a company, with a fine which may extend to INR 1,00,000/- (Rupees One Lakh) or with both

vi. **Aadhaar DS Regulation 3** – This regulation specifies that the authority may specify an information security policy setting out *inter alia* the technical and organisational measures to be adopted by the authority and its personnel, and also security measures to be adopted by agencies, advisors, consultants and other service providers engaged by the Authority, registrar, enrolling agency, requesting entities, and authentication service agencies. Such information security policy may *inter-alia* provide for controlled access to confidential information; restrictions on personnel relating to processes, systems and networks; and inclusion of security and confidentiality obligations in the agreements or arrangements with the agencies, consultants, advisors or other persons engaged by the authority.

vii. **Sharing Regulations 3 and 4** – These regulations provide that core biometric information collected by the authority/requesting entity will not be shared with anyone for any reason whatsoever. Further, demographic information and photograph of an individual collected by the authority may be shared with a requesting entity in response to an authentication request for e-KYC data pertaining to such individual, upon the requesting entity obtaining consent from the Aadhaar number holder.

viii. **Sharing Regulation 5** – This regulation provides that any individual, agency or entity which collects Aadhaar number or any document containing the Aadhaar number, shall: (a) collect, store and use the Aadhaar number for a lawful purpose; (b) inform the Aadhaar number holder the following details:— i. the purpose for which the information is collected; ii. whether submission of Aadhaar number or proof of Aadhaar for such purpose is mandatory or voluntary, and if mandatory, the legal provision mandating it; iii. alternatives to submission of Aadhaar number or the document containing Aadhaar number, if any; (c) obtain consent of the Aadhaar number holder to the collection, storage and use of his Aadhaar number for the specified purposes. Such individual, agency or entity shall not use the Aadhaar number for any purpose other than those specified to the Aadhaar number holder at the time of obtaining his consent and shall not share the Aadhaar number with any person without the consent of the Aadhaar number holder.

[53] The term "**identity information**" has been defined to mean *in respect of an individual, includes his Aadhaar number, his biometric information and his demographic information*.

5. General Data Protection Regulations (Regulation (EU) 2016/679) ("GDPR")

GDPR was approved and adopted by European Parliament ("**EU**") in April 2016 and will come into force on May 25, 2018 without the need for implementing national legislation. GDPR will replace the EU Directive 95/46/EC adopted by the European Parliament and Council on October 24, 1995. [54]

The GDPR extends its geographical reach and will not only apply to organisations located within the EU but it will also apply to organisations located outside of the EU if they (a) process personal data in the context of the activities of an establishment of a 'controller' or a 'processor' in the EU, or (b) process personal data of EU data subjects, where the processing activities relate to offering of goods or services (including for free); or (c) monitor the behaviour if the behaviour takes place within EU.[55]

However, mere website accessibility of a service in the EU is not sufficient to trigger application of the GDPR. However, Factors such as offering a service in the languages or currencies used in a Member State (if not also used in the third country), or mentioning customers or users in a Member State may trigger application of the GDPR.[56]

Further, the conditions for consent have been strengthened. The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent - meaning it must be unambiguous. Consent must be clear and distinguishable from other matters and provided in an intelligible and easily accessible form, using clear and plain language.[57] It must be as easy to withdraw consent as it is to give it. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for performance of that contract.[58]

In case of breach under GDPR, an entity can be fined up to the higher of 4% of annual worldwide turnover and EUR20 million. GDPR implements a tiered approach. Other specified infringements would attract a fine of up to the higher of 2% of annual worldwide turnover and EUR 10 million.[59]

---

[54] http://www.eugdpr.org/gdpr-faqs.html
[55] Article 3 of GDPR
[56]http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf
[57] Article 7 of GDPR
[58] *Ibid*
[59]http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf

MUMBAI
109 A, 1st Floor
Dalamal Towers
Free Press Journal Road
Nariman Point
Mumbai 400 021
T: +91 22 6636 7000
F: +91 22 6636 7172
E: mumbai@elp-in.com

DELHI
801 A, 8th Floor
Konnectus Tower
Bhavbhuti Marg
Opp. Ajmeri Gate Railway Station
Nr. Minto Bridge
New Delhi 110 001
T: +91 11 4152 8400
F: +91 11 4152 8404
E: delhi@elp-in.com

AHMEDABAD
801, 8th Floor
Abhijeet III
Mithakali Six Road,
Ellisbridge
Ahmedabad 380 006
T: +91 79 6605 4480/8
F: +91 79 6605 4482
E: ahmedabad@elp-in.com

PUNE
202, 2nd Floor
Vascon Eco Tower
Baner Pashan Road
Pune 411 045
T: +91 20 49127400
E: pune@elp-in.com

BENGALURU
6th Floor, Rockline Centre
54, Richmond Road
Bangalore 560 025
T: +91 80 4168 5530/1
E: bengaluru@elp-in.com

CHENNAI
No. 6, 4th Lane
Nungambakkam High Road
Chennai 600 034
T: +91 44 4210 4863
E: chennai@elp-in.com

Published on September 01, 2017