Volume 14, January 2021 ISSN 2581-5504

# "Data Protection in the Insurance Sector"

***Aditi Garg*[1]**
***GNLU,***
***Gandhinagar***

The insurance sector is an extremely vital part of our country. Not only does it help in reducing the financial burden of individuals, but it also is imperative for a country's economy. This sector has always been data-driven. Insurers require personal and sensitive information for a variety of reasons. For starters, in order to market their services, insurers use the data of potential customers and accordingly personalize their marketing. Personal data is also required to accurately do the risk pricing while entering into an insurance contract with an individual and deciding claims. Further, regulatory compliances such as 'Know Your Customer' also require collection of data. Thus, the insurance sector deals heavily with collection, storage and retention of personal and sensitive data. This data may also be transmitted to third parties and insurance intermediaries by such insurers. Moreover, with the introduction of new technologies, the collection of data has become extremely easy. On a daily basis, individuals give their consent to collection of data by various websites and applications. In the insurance sector as well, insurers are employing new technologies such as the blockchain and artificial intelligence, etc. While technology has its own advantages, it has led to increased concerns about data protection and privacy. Hence, at this point in time, it is important that insurance regulators such as the IRDAI are proactive in their approach to data protection. In this context, the present study examines the data protection regime in India as well as in global regimes and analyses how the Indian regime can be improved upon.

***Keywords:*** *Insurance, data protection, confidentiality, privacy, IRDAI*

## 1 INTRODUCTION

Risk is a given part of everyone's life. Be it inside our homes or in a car or on a bus, this risk follows us everywhere. While risk can never be eradicated, one can be compensated for it to some extent. This is where insurance comes in. Even though fire cannot always be avoided or predicted, the loss can be compensated against. When it comes to life, insurance cannot bring a person back, but it can help the dependents of such person financially. Insurance is not only vital for managing the financials of a person but also for the country's economy.[2] These objects led to the development of the institution of insurance.[3]

While there is no fixed definition of insurance in any legislature, the same has been defined in terms of risk minimization. Life Insurance Corporation (**"LIC"**) defines insurance as,

[1] Student, LLM, Gujarat National Law University, Gandhinagar
[2] Syed Salman, Hafiz Rashid & Sheila Htya, 'The Progressive Development of India's Insurance Industry from Ancient to Present Times' (2016) 6 Human Resource Management Research 91
[3] Sumeet Malik, *Law of Insurance* (1st vol, 2nd ed, Eastern Book Company 2016)

Volume 14, January 2021 ISSN 2581-5504

*"Social device for minimizing risk of uncertainty regarding loss by spreading the risk over a large enough number of similar exposures to predict the individual chance of loss."*[4]

***History of Insurance in India:*** It will be wrong to say that the concept of insurance is a western one or has been popularised only in the last few decades in India. Its existence can be found in the writings of Manu and Kautilya. It was termed as 'Yogaksdhama' in the Rig Vedas which denotes community insurance. In those times, insurance existed in the sense of pooling of community resources and creating a fund to be used in case of calamities. This may be termed as a pre-cursor to the modern concept of insurance.

Insurance as it is understood presently in India can also be traced back to many countries and in particular, England wherein the business of insurance has been ongoing for several centuries. India saw its first organised insurance venture in the form of Oriental Life Insurance Company in the year 1818 in Calcutta. The main reason behind the establishment of this Company was to financially protect English widows. As far as Indians were concerned, they had to pay higher premiums on account of their lives being considered "high risk" at the time.[5] In the nineteenth century, there were several attempts to control the insurance sector by the British (for instance, the British Insurance Act in 1870), but ultimately foreign companies like Royal Insurance dominated the sector.

In 1912, to regulate the insurance sector in India, the Indian Life Assurance Companies Act was enacted. This was the first legislative measure for the sector in India and led to the enactment of the Indian Insurance Companies Act, 1928 which enabled the Government to collect data with respect to life and non-life insurance business in India.[6] Ultimately, in 1938, the earlier Act was consolidated in the form of the Insurance Act, 1938. Since then, this Act has been subject to various amendments. In 1956, LIC was created to nationalize the life insurance sector in India. Further, in 1972 the general insurance was also nationalized in the country by the creation of National Insurance Company Ltd., the New India Assurance Company Ltd., the Oriental Insurance Company Ltd, and the United India Insurance Company Ltd.[7]

In 1999, the Insurance Regulatory and Development Authority of India (**"IRDAI"**) was constituted[8], based on the recommendations of the Malhotra Committee Report[9]. The autonomous body was created to *"protect the interests of holders of insurance policies, to regulate, promote and ensure orderly growth of the insurance industry*".[10]

[4] 'Glossary' (*Life Insurance Corporation*) <https://licindia.in/Bottom-Links/glOSSORY> accessed 1 January 2021
[5] Sumeet Malik, *Law of Insurance* (1st vol, 2nd ed, Eastern Book Company 2016)
[6] 'History of Insurance in India (*Insurance Regulatory and Development Authority of India,* 12 July 2007) <https://www.irdai.gov.in/ADMINCMS/cms/NormalData_Layout.aspx?page=PageNo4&mid=2> accessed 1 January 2021
[7] See, General Insurance Business (Nationalisation) Act 1972
[8] Insurance Regulatory and Development Authority of India Act 1999
[9] Malhotra Committee, *Reforms in the Insurance Sector* (Ministry of Finance, 1994)
[10] Insurance Regulatory and Development Authority of India Act, 1999, Preamble

***Increased use of data:*** As the above part portrays, insurance has developed quite a lot over the decades. However, despite all the developments, there is one constant: the insurance industry has always been data-driven as compared to other industries. From marketing to risk analysis, the industry relies heavily on personal data on potential and actual customers. [11] On top of this, legal requirements such as KYC have also left no option but to collect personal and sensitive information. With the advent of technology, the industry has found new ways and reasons to collect even more information. The new technologies pose new problems and accordingly, require new solutions. The existing data protection laws enacted generally for all industries may not be adequate to keep up with these new problems. The amount and kind of data collected vary from one industry to another. In the insurance industry, not only is the volume of the data collected very high but most of this data is also highly sensitive. To keep up with this, the insurance regulators as well as insurers must step up and take responsibility to retain customers' confidence in the industry. This paper studies the global as well as Indian regime in this context and examines how data protection in the Indian insurance sector can be ensured.

### *1.1 Research Objectives*

i. To evaluate the need for a comprehensive regime on data protection in the insurance sector.
ii. To analyze the legal framework on data protection in the insurance sector in India as well as in other jurisdictions.
iii. To examine how this legal framework in India can be enhanced.

### *1.2 Scope and Limitation of the Study*

The study focuses on data protection and privacy concerns in the insurance sector. As discussed above, like any other industry, the insurance industry has also become even more data-driven in light of the recent technological advancements. Not only do insurers collect enormous amounts of personal and sensitive data from their customers, but data of potential customers is also acquired for marketing and risk pricing. This study first examines the global regime in order to understand the possible lacunae and solutions in the Indian model. For this purpose, the laws in the European Union and the United States of America have been looked into. After this, the legal framework in India has been studied.

This study is not an examination of the impact of technology on society and data protection. It does not delve into the debate on privacy as a fundamental right or the issues of national security and compromise of privacy in the national interest. It is only limited to data protection in the insurance sector and should not be referred to as a general study of data protection in India.

[11] Juliana De Groot, 'Top Security Considerations for Insurance Companies' (*Data Insider*, 20 January 2020) <https://digitalguardian.com/blog/top-security-considerations-insurance-companies> accessed 1 January 2021

Volume 14, January 2021 ISSN 2581-5504

Moreover, due to Covid-19, the research methodology has been restricted to the doctrinal mode of study. The study makes use of both primary and secondary sources of data for this purpose.

### *1.3 Research Methodology*

Research has been undertaken through the doctrinal method and is current to January 2021. As a matter of organization and ease of reading, technical granularity and any additional background information are placed within the footnotes. The research papers, news articles, and reports relied upon have also been footnoted with relevant URLs.

The research uses both a descriptive and analytical method of writing. The researcher has relied on both primary sources (Regulations and legal framework) and secondary sources (official reports, journals, newspaper articles).

## 2 GLOBAL REGIME

### *2.1 European Union*

Since its approval in 2016, the EU's General Data Protection Regulation[12] (**"GDPR"**) has become one of the most important data protection legislation in the world. GDPR, which came into full force on May 25, 2018, has introduced much stringent provisions as compared to its predecessor, the Directive 95/46/EC.

The Regulation covers in its ambit all organizations that offer goods and services to, or monitor the behaviour of EU residents, and has had a profound effect on the insurance industry. Insurers have had to change their entire systems and processes in order to ensure GDPR compliance.

Categories of personal data : Insurance involves a high degree of due diligence of customers and policyholders. This is done by engaging underwriters. An underwriter will, irrespective of the type and nature of insurance, come across, collect and review the personal data of customers. This includes not only data like demographics but also highly sensitive data such as genetic history, health history, and psychological traits. The latter has been categorized by GDPR as "**special categories of data**". Under Article 9, misprocessing of such data would impose a high penalty (i.e. 4% of global annual turnover or EUR 20 million). The insurer must obtain the express consent of the consumer in order to collect such data unless it is necessary for purposes such as security of the vital interests of individuals or for the public interest. Further, as per Article 35, large scale processing of sensitive personal data would require companies to carry out formal **data protection impact assessments.** Insurance companies deal with large volumes of data, for underwriting, fraud prevention, claims, etc. and thus, will automatically fall within the ambit of this provision.

[12] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119

Volume 14, January 2021 ISSN 2581-5504

Processing of Claims: Processing and handling of claims is a data-intensive function. The capacity of insurers to manage and pay claims is dependent on the availability of the correct data, which is often sensitive. As discussed above, such data can only be processed with the express consent and any misprocessing would attract a high penalty. Data minimization is one of GDPR's main governing principles and thus, insurers must abide by it. It is of utmost importance that they determine the legally permissible limits of data collection.

Marketing: In order to find new clients, insurance firms use direct marketing extensively. Not only do they obtain data directly from people, but they also buy data from third-party providers. However, insurance firms require positive opt-in by individuals to express their consent and expectations as to how, when, and if they wanted to be contacted. This consent must be:

i. Freely given,
ii. Based upon a genuine choice,
iii. Easily withdrawable. [13]

Further, individuals also have a right to object to this personal data processing where it relates to direct marketing.[14]

Right to Data Portability and Erasure: In accordance with Article 20, data subjects have the right to receive their personal data held by a controller or to transmit it from one controller to another. Insurers will have to adopt innovative technologies such as cloud, AI, etc. to ensure the portability of data. Moreover, the data subjects also have the right to have this data erased unless there is a legal requirement to retain the same.

While these rights and requests may sound easy and basic, the readiness required by controllers is a challenge in its own sense. Insurers will have to revisit their data retention and disposal policies and mechanisms. Even documenting a clear legal justification for retaining data will require a lot of introspection and brainstorming.[15]

Data Retention: GDPR imposes a storage limitation under Article 5. Data retention and preservation is only allowed for as long as it is appropriate for the reason for which it has been obtained, after which it must be removed or anonymized. Storage for longer periods is only permissible when the processing of such data is merely for archival purposes and in the public interest. However, this is also subject to further technical and organizational protections such as **pseudonymization**.

[13] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119, art 7
[14] Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L 119, art 21
[15] Luke Irwin, 'A guide to the GDPR for insurance companies' (*IT Governance Blog*, 30 May 2018) <https://www.itgovernance.co.uk/blog/a-guide-to-the-gdpr-for-insurance-companies> accessed 1 January 2021

Breach Reporting: Under Article 33, data controllers must, mandatorily report data breaches without undue delay and if feasible, within 72 hours, to the relevant supervisory authority. In cases where reporting is not done within 72 hours, the reasons for the same must be stated. However, it is not mandatory to report the violation if it is improbable to affect the risk to the rights and freedoms of the data subjects.

The insurers must:

- Evaluate their processes to ensure that breaches can be easily and promptly identified and managed;
- Formulate a response plan to decide responsibilities if a breach occurs;
- Consider cyber insurance

Data Protection Officers: In accordance with Article 37, all data controllers and processors have to appoint Data Protection Officers (**"DPOs"**) in the following situations:

i. They are a public body; or
ii. Their core activities need monitoring of personal data on a large scare and a regular basis; or
iii. Their core activities include the processing of sensitive personal data on a large scale.

Further, the data controllers and processors must inform DPOs of all the data protection issues in the organization and provide them with adequate resources to fulfil their job.

While para 7 of the introduction to GDPR explains that the mandate of DPO is applicable only in limited circumstances, the provision is still likely to have a wide impact and could bring within its purview, majority of large companies. This will include large insurers and brokers as well. In the EU, most insurers already had DPOs in place, but the specifications and conditions will have to be reviewed.[16] The insurers may opt to nominate a board member to sponsor a team of auditors.[17]

The GDPR is both a threat and an opportunity for the insurance sector. While it has increased customer awareness and may boost cyber insurance, [18] GDPR has also placed a huge compliance burden on insurers, who till now had been using old systems and processes. However, insurers who try to not only comply with GDPR but also take some enforcement initiatives will be able to use data protection to build trust and a lasting relationship with their customers.[19]

[16] Rhiannon Webster & Jade Kowalski, 'The European General Data Protection Regulation, A guide for the insurance industry' (*Dac Beachcroft,* May 2016) <https://www.dacbeachcroft.com/media/889655/european-data-protection-insurance-industry-interactive-version.pdf> accessed 1 January 2021

[17] Luke Irwin, 'A guide to the GDPR for insurance companies' (*IT Governance Blog,* 30 May 2018) <https://www.itgovernance.co.uk/blog/a-guide-to-the-gdpr-for-insurance-companies> accessed 1 January 2021

[18] Mohit Manchanda, Prakhar Agrawal & Shweta Agrawal, 'GDPR and its Impact on Insurance Companies' (2017) EXL White Paper

[19] Nicholas Blackmore, 'What GDPR means for the insurance industry' (*Privsec Report,* 29 June 2018) <https://gdpr.report/news/2018/06/29/what-gdpr-means-for-the-insurance-industry/> accessed 1 January 2021

Volume 14, January 2021 ISSN 2581-5504

### *2.2 United States of America*

With the regard to the insurance sector in the US, most of the laws are made by individual states. However, there are some federal legislations like the Gramm-Leach-Bliley Act in 1999, the Patient Protection and Affordable Care Act in 2010, and the Health Insurance Portability and Accountability Act. The Dodd–Frank Wall Street Reform and Consumer Protection Act has also made a significant impact on the insurance sector. As far as data protection laws are concerned, the US employs a sectoral approach.[20] What this means is that the issue is not governed by one authority but rather, the laws are fragmented and spread across government and industry-specific regulations. When it comes to fundamental right of privacy, it has been nowhere mentioned or recognized in the country[21] or its constitution[22]. However, it can be indirectly arrived at from the 1st, 3rd, 4th, 5th and 14th amendments.[23] This part examines some of these federal laws which have a considerable impact on the insurance sector vis-à-vis data protection.

*Federal Trade Commission Act 1914:* The FTC Act was enacted to curb misleading or unfair trade practices and is now applicable to various policies in relation to privacy and data security. It bans are activities that could theoretically put a customer's personal information at risk of misuse and hacking.[24] Such personal information would include online user searches, web pages accessed, content downloaded, etc.[25]

In the past, there has been extensive debate over whether FTC applies to insurance companies. It has been argued time and again that the McCarran-Ferguson Act exempts insurance companies from FTC because it provides that *"the Federal Trade Commission Act, as amended, shall be applicable to the business of insurance to the extent that such business is not regulated by state law."*[26] In *Union Labor Life Insurance Co. v Pireno*[27], it was clarified by the Supreme Court that to ascertain whether an activity constituted the business of insurance under the McCarran-Ferguson Act, a three-step factual inquiry is necessary:

i. Does the activity have the effect of transferring or spreading a policyholder's risk;
ii. Is the activity an integral part of the policy relationship between the insurer and the insured; and
iii. Is the practice limited to entities within the insurance industry?

[20] Oindrila Bhowmik, 'Threats to Offshore Outsourcing - Current Legal Scenario and the Road Ahead' (2012) 1 NSLJ 36
[21] Alan F Westin, 'Science, Privacy, and Freedom: Issues and Proposals for the 1970's: Part I - The Current Impact of Surveillance on Privacy' (1966) 66 Colum. L. Rev. 1003, 1032
[22] Shatakshi Singh, 'Data Protection - Protection of What, Protection from Whom & Protection for Whom - An Analysis of the Legal and Judicial Provisions in India and Abroad' (2018) 7 NLIU LR 79, 86
[23] *Griswold v Connecticut* 381 US 479 (1965); *Roe v Wade* 410 US 113 (1973)
[24] Federal Trade Commission Act, 15 USC § 45b(b)2 (1914)
[25] Shatakshi Singh, 'Data Protection - Protection of What, Protection from Whom & Protection for Whom - An Analysis of the Legal and Judicial Provisions in India and Abroad' (2018) 7 NLIU LR 79, 86
[26] McCarran-Ferguson Act, 15 USC §1012(b) (1945)
[27] 458 US 119 (1982)

This investigation involves a factual review of the activity in question. Even if the activity constitutes the business of insurance as per these questions, it must also be examined whether such activity is subject to any state regulation.[28] In the event of an interstate sale of insurance, it is important to determine not only whether the activity is controlled by the States in which the practice has an effect[29], but also whether those States are in a position to exercise local control through their provisions, instruments, and procedures.[30]

Citing these case, the FTC clarified that McCarran-Ferguson Act does not exempt insurance companies from the FTC's jurisdiction, but rather exempts only those activities that constitute "the business of insurance," regardless of who performs them, and then only to the extent that such activities are regulated by state law.[31] Thus, FTC applies to insurance companies and related entities in absence of state laws.

*The Financial Services Modernisation Act 1999:* The FSM Act (also known as the **Gramm-Leach-Bliley Act**) regulates the use, disclosure, and collection of financial information.[32] It prohibits the disclosure of non-public personal information obtained by a financial institution,[33] i.e. an institution engaged in activities of a financial in nature.[34] **Insurance against illness, damage, harm, disability, death, or less is also classified as a financial activity.[35]** Therefore, insurance companies are subject to this Act. The Act mandates that a financial institution must send privacy notices to customers. There are also certain limitations placed on the sharing of financial information and the duty to protect and secure customer data is also imposed.[36] When there is a possibility that non-personal public data may be revealed to a non-affiliated third party, the customers must be notified of the same, after which they may refuse to permit such disclosure to a third party except when it is for processing transactions or fraud prevention.[37] The Act does not limit the use of personal information and thus does not prohibit the possibility of using big data to personalize insurance contracts.[38]

*The Health Insurance Portability and Accountability Act, 1996 (**"HIPPA"**):* HIPPA's main focus is on the healthcare sector but it deals with privacy concerns in the insurance sector as

[28] *Autry v Northwest Premium Services, Inc* 144 F.3d 1037(7th Cir 1998)
[29] *FTC v Travelers Health Ass'n* 362 US 293 (1960)
[30] *Travelers Health Ass'n v FTC* 298 F.2d 820 (8th Cir. 1962)
[31] 'Advisory Opinions: Opinion 03-1' (*Federal Trade Commission*, 19 August 2003) <https://www.ftc.gov/policy/advisory-opinions/opinion-03-1-1> accessed 1 January 2021
[32] Shatakshi Singh, 'Data Protection - Protection of What, Protection from Whom & Protection for Whom - An Analysis of the Legal and Judicial Provisions in India and Abroad' (2018) 7 NLIU LR 79
[33] John T Soma, *Privacy Law in a nutshell* (2nd edn, WestAcademic Publishing 2014)
[34] The Financial Services Modernisation Act 1999, 15 U.S.C. § 6809(3)(A) and 12 U.S.C. § 1843(k)
[35] The Financial Services Modernisation Act 1999, 15 U.S.C. § 6809(3)(A) and 12 U.S.C. § 1843(k)(4)(B)
[36] Kurt Wimmer, *Data Protection & Privacy: International Series* (3rd ed, Thomson Reuters 2016)
[37] Lothar Determann, *California Privacy Law* (3rd ed, The International Association of Privacy Professionals 2018)
[38] Florent Thouvenin, Fabienne Suter, Damian George & Rolf H. Weber, 'Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts' (2019) 10 JIPITEC 209 <https://www.jipitec.eu/issues/jipitec-10-2-2019/4916/JIPITEC_10_2_2019_209_Thouvenin_Suter_George_and_Weber> accessed 1 January 2021

well. The covered entities in the Act includes health insurers. The Act protects individuals availing healthcare and insurance services. It ensures that the information provided by a person to the healthcare or insurance service provider is kept secure and is not disclosed without the express consent of such person. Certain exceptions are provided to this rule wherein the information can be disclosed in the interest of the patient, insurer, or law enforcement. Thus, the Act ensures that disclosure is only within the requisite limits.[39] Pursuant to this Act, certain Privacy[40] and Security Rules[41] have also been formulated. These regulations ensure that individuals are sent a notice delineating how their information is used.

*The Dodd–Frank Wall Street Reform and Consumer Protection Act, 2010:* While the main focus of this Act is on financial services, it has also had significant ramifications on the insurance sector. Considering how the insurance sector is left for the states to regulate, this Act is one of the first steps taken by the federal government to regulate the area.

Large banking and non-banking financial institutions pose a great systematic risk to a country's economy. To identify and act on such risks in the US, the Act has created the Financial Stability Oversight Council. This Council can also make large insurance companies subject to the Federal Reserve Board[42] and its supervision. This is a noteworthy development because while non-banking financial institutions like insurance companies are important in the context of systematic risk, these companies have escaped the authority of the federal system till the enactment of this Act. Among other risks, insurance companies present risks with respect to data protection which is of concern to the federal government.

Further, it was recognized by Congress that in order to regulate the insurance industry and the risks posed by it, regulators should have adequate expertise and knowledge of the industry. However, since the insurance industry is rarely regulated by the federal government, the federal regulators don't possess such knowledge. Thus, the Federal Insurance Office has been created by the Act which is tasked with the responsibility to monitor the insurance industry, gather relevant data, and report the same to the federal government. However, it is pertinent to note that the Act doesn't grant this Office the regulatory power over the insurance industry.[43]

*Fair Credit Reporting Act 1970 (**"FCRA"**):* The FCRA was enacted to protect consumers from inappropriate, deceptive, unfair or inaccurate use of their personal information in credit reports.[44] The primary purpose of the Act is to govern the disclosure and usage of personal information supplied by Credit Rating Agencies (**"CRA"**) and , the use of consumer reports[45]

[39] Agnidipto Tarafder, 'Surveillance, Privacy and Technology: A Comparative Critique of the Laws of USA and India' (2015) 57 JILI 550, 558
[40] HIPAA Security and Privacy Regulations 2018
[41] General Security and Privacy Provisions 2018
[42] *see* Federal Reserve Act 1913
[43] Frank A. Mayer, III , Deborah F. Cohen & David W. Freese, 'The Dodd-Frank Act and the insurance industry' (*Lexology*, 10 March 2011) <https://www.lexology.com/library/detail.aspx?g=6a278b3d-8b0d-44d8-b454-49f610cde7f5> accessed 1 January 2021
[44] Fair Credit Reporting Act 1970, 15 U.S.C. §§ 1681-1681x
[45] *see*, Fair Credit Reporting Act 1970, 15 U.S.C. § 1681a(d)).

for adverse actions. These consumer reports are often used by insurers for insurance contracts in order to ascertain the willingness to pay of consumers. When such reports are used to deny, cancel, adversely, or unfavourably change coverage or amount charged for any insurance, these actions are deemed to be adverse actions.[46] Therefore, to use consumer reports, insurance companies must comply with this Act.

According to Section 604, a consumer report requested by a person may only be provided by a CRA if the consumer so consents or when the requesting person has a permissible purpose to obtain the report. Underwriting of insurance has been listed as one of such permissible purposes.[47] FCRA requires the user of consumer reports to disclose to the consumer, any adverse action taken based on the report.[48] Similarly, if the insurer uses the report for big data analytics which further leads to an adverse action, the consumer must be informed. However, when data is derived from the insurer's customer relationship and used for decision making or when the data for big data analysis is directly received from the consumers and not a CRA, the FCRA would not apply.[49]
Thus, it is only when insurers or any company in general, use consumer reports or data from a Credit Rating Agency to take adverse actions that the FCRA comes into the picture. [50]

*Genetic Information Nondiscrimination Act 2008:* This Act forbids employers and health insurance providers from discriminating against people on the basis of their genetic information. Further, it emphasizes on the collection of minimum data except for when it is absolutely necessary and allowed by law.[51] In particular, health insurers are prohibited from collecting, requesting, or buying genetic data for underwriting or prior to enrolment under a plan.[52]

## 3 INDIAN REGIME

### *3.1 Information Technology ACT 2000*

The Information Technology Act 2000 (**"IT Act"**) sets out the data privacy regime in India and is further supplemented by various rules such as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (**"Privacy Rules"**). The IT Act covers, *inter alia,* the following offences:

[46] Fair Credit Reporting Act 1970, 15 U.S.C. § 1681a(k)(1)(B)(i)
[47] Fair Credit Reporting Act 1970, 15 U.S.C. § 1681b(a)(3)(C)
[48] Fair Credit Reporting Act 1970, 15 U.S.C. § 1681m(a)(1)
[49] Fair Credit Reporting Act 1970, 15 U.S.C. § 1681a(d)(2)(A)(i)
[50] Florent Thouvenin, Fabienne Suter, Damian George & Rolf H. Weber, 'Big Data in the Insurance Industry: Leeway and Limits for Individualising Insurance Contracts' (2019) 10 JIPITEC 209 < https://www.jipitec.eu/issues/jipitec-10-2-2019/4916/JIPITEC_10_2_2019_209_Thouvenin_Suter_George_and_Weber> accessed 1 January 2021
[51] Lothar Determann, *California Privacy Law* (3rd ed, The International Association of Privacy Professionals 2018)
[52] Genetic Information Nondiscrimination Act 2008, 29 U.S.C. § 1182(c)(4)(C); 29 U.S.C. § 1182(d)

- Identity theft
- Privacy violations
- Cyber terrorism
- Computer related offences
- Sending offensive material through communication services

The IT Act has also empowered police officers to investigate these offences. The Indian Penal Code, 1860 also lays down the punishments for certain cybercrimes like email spoofing, cyber fraud, etc. Further, as the national agency responsible for responding to cyber complaints, the Indian Computer Emergency Response Team (**"CERT-In"**), assists in reducing the risk of cybersecurity incidents. Further, when any entity collects or processes sensitive personal data pertaining to an individual, it must establish a privacy policy[53], provide mandatory notice/disclosure to the data subject before collecting the information[54], and appoint a grievance officer[55] etc.

These legal requirements under the IT Act and Privacy Rules shall apply to insurers, insurance intermediaries etc. The intermediaries also need to follow certain requirements in order to escape liability for any third-party information, data, or communication links made available or hosted by it. These include observing due diligence, informing users of their data protection policy, and disable content that violates the IT Act or any regulations under it.

This framework however fails to provide an exhaustive list of permitted uses for sensitive and personal data. Moreover, the Government has been vested by wide powers to collect data which is only subject to the 'communication of purpose' requirement. This may lead to situations akin to the leaks involving the NHS database in the UK.[56]

The Rules under the IT Act provide a beginning to the cause of data protection in India. However, there is still a large scope for misuse.[57] The same has also been realized by the Government who has formulated a draft personal data protection bill[58] that seeks to introduce a more comprehensive data protection regime that can strike the appropriate balance between protecting the interests of individuals and the legitimate use of data by the state and private businesses.

[53] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rule 4
[54] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rule 5
[55] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, rule 5(9)
[56] Nimisha Srinivas & Arpita Biswas, 'Protecting Patient Information in India: Data Privacy Law and its Challenges' (2012) 5 NUJS L Rev 411, 424
[57] Rishika Taneja & Sidhant Kumar, *Privacy Law: Principles, Injunctions and Compensation* (1st ed, Eastern Book Company 2014)
[58] The Personal Data Protection Bill, 2019

### *3.2 IRDAI Regulations*

The IRDAI has issued several Regulations that touch upon data protection regime as applicable to insurance companies. These Regulations have been discussed below:

*IRDAI(Protection of Policyholders' Interests) Regulations 2017:* In a significant move to safeguard customer interests and curb malpractices in the insurance sector of India, the IRDAI notified these Regulations on 30 June 2017. These Regulations are applicable not only to all insurers but also to intermediaries, disturbance channels, insurance intermediaries, other regulated entities and policyholders.[59]

As per Regulation 19(5), insurers are under an obligation to maintain, at all times, total confidentiality of policyholder information. The only exception to this rule is when disclosure of such information to statutory authorities becomes necessary due to the operation of any law. It is clear that the regulation imposes a very basic but vital duty on the insurers, though it doesn't mandate how this duty has to be fulfilled. However, the IRDAI has the power to initiate action under the Insurance Act, 1938 or the IRDAI Act, 1999 against any insurer or distribution channel etc who breaches this obligation.

*IRDAI (Maintenance of Insurance Records) Regulations, 2015:* Up until 2015, insurers used to maintain their register of policies and claims in accordance with the Insurance Act, 1938. In light of the growing use and utility of electronic means, the Insurance Act, 1938 was amended in 2015 to encourage maintenance of such records in electronic form.[60] In furtherance of this move, the IRDAI (Maintenance of Insurance Records) Regulations, 2015 were issued in August 2015 to complement the Act. These Regulations mandate the recording of every policy and claim in electronic form. Further, the system of maintenance of such records must have the necessary and adequate security features. Moreover, to ensure the safety of the data, insurers are allowed to store the records pertaining to all the policies issued and all claims made in India in centers located and maintained in India only. The access of such records must be provides to IRDAI for onsite as well as offsite inspection. Further, with regard to storage of records in the electronic form, the insurer's policy should ensure, *inter alia,* the following:

- Processing and electronic maintenance of records,
- Privacy and security of policyholder and claim data,
- Handling of Virus, Vulnerability issues
- A detailed plan to review the implementation of the maintenance and storage of records

The review of every policy of the insurer shall be done once in a year within 90 days from the expiry of the financial year. Further, any change in a policy must be notified within 30 days of such revision.

[59] IRDAI(Protection of Policyholders' Interests) Regulations 2017, regulation 2
[60] Insurance Act 1938, s 14

Volume 14, January 2021 ISSN 2581-5504

These Regulations are an attempt to embrace the technology and ensure that the insurance sector keeps up with it. At the same time, IRDAI has recognized the risks involved and challenges posed by such technology and has accordingly, issued regulations to manage such risks and challenges.

*IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017:* In the insurance sector, several non-core activities are outsourced by insurers. This poses several risks since such outsourcing may otherwise leave security gaps and may be detrimental to the policyholders' interests. Recognizing this, in 2017, IRDAI issued the (Outsourcing of Activities by Indian Insurers) Regulations, 2017. The objectives of this Regulation are to ensure that even when insurers are outsourcing certain activities, the interests of the policyholders are protected by them. Accordingly, insurers have to follow appropriate practices to mitigate the risk involved with outsourcing and carry out due diligence with regard to such outsourced activities and parties.[61]

These Regulations are applicable to all registered Insurers excluding those engaged in reinsurance business. If an Insurer is engaged in both direct Insurance as well as Reinsurance business, these regulations are applicable only in respect of direct Insurance business of such Insurers.

Certain activities like compliance with AML and KYC, Policyholders Grievances Redressal, etc. cannot be outsourced by the insurer. Further, with regard to outsourced activities the following steps shall be taken by the insurer to maintain the confidentiality and security of policyholders' information:

- The insurer must carry out due diligence before choosing an outsourcing service provider that has appropriate security policies to ensure that confidentiality and security of policyholders' information is protected.
- It is the responsibility of the insurer to ensure that confidentially is maintained by the outsourcing service provider.
- If any legal and contractual disclosure obligations of the outsourcing service provider would result in disclosure of the insurer's customer data, the same must be considered by the insurer.
- In case of termination of the outsourcing agreement, the customer data shall be retrieved back from the service provider by the insurer and it shall be ensured that the service provider doesn't continue to use such data.

*Insurance Regulatory and Development Authority of India (Health Insurance) Regulations 2016:* In order to update the regime on health insurance and after considering the

[61] IRDAI (Outsourcing of Activities by Indian Insurers) Regulations 2017, regulation 3

representations by various stakeholders[62], the IRDAI in 2016, replaced the Health Regulations 2013 with the IRDAI (Health Insurance) Regulations 2016. These Regulations are applicable to all registered Life Insurers, General Insurers, and Health insurers, conducting health insurance business, as defined under the Insurance Act 1938 as well as to all Third Party Administrators (TPAs) wherever mentioned.

As per Regulation 35, a seamless flow of data transfer for all claims shall be established by the insurer and the TPA. The Regulations encourage but don't mandate the electronic flow of data. Further, IRDAI may require insurers, TPAs, and network providers to comply with data related matters and settlement of claims through electronic means as per the guidelines as may be specified by it from time to time. It is pertinent to note that as per the IRDAI (Maintenance of Insurance Records) Regulations, 2015 discussed above, it is mandatory for the insurer to record policy and claims in an electronic form. Thus, it follows that any data transfer should also be electronic, if possible.

*Insurance Regulatory and Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017:* As per Regulation 9, a referral company approved by the IRDAI and registered with the insurer shall 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.

*Regulatory Framework Governing Insurance Intermediaries:* Like any other sector, intermediaries in the insurance sector play a vital role. They act as a conduit between insurance companies and customers and facilitate the whole insurance process, be it the selection of an insurer or assessment of claims. These intermediaries include TPAs, brokers, corporate agents, web aggregators, loss assessors, and individual agents. While there are separation regulations and code of conduct for each kind of insurance intermediary, in relation to data protection and confidentiality, the obligations are more or less the same. All insurance intermediaries must:

i. treat all information given to them by prospective clients as fully confidential to themselves and to the insurer to whom the business is being offered;
ii. Take effective measures to ensure the protection of confidential documents in their custody, including by restricting access to such records, the execution of confidentiality undertakings, etc.[63]

In relation to TPAs, the IRDAI (Third Party Administrators – Health Services) Regulations 2016 have been issued. According to Regulation 19, TPA shall strictly maintain professional

[62] Celia Jenkins, Damini Ghosh & Priya Misra, 'Health Insurance Regulations & Guidelines: The Recent Overhaul' (*Mondaq*, 6 September 2016) <https://www.mondaq.com/india/insurance-laws-and-products/524342/health-insurance-regulations-guidelines-the-recent-overhaul> accessed 1 January 2021

[63] *see,* IRDAI (Licensing of Banks as Insurance Brokers) Regulations 2013, regulation 2; IRDAI (Insurance Brokers) Regulations 2018, schedule I and II; IRDAI (Registration of Corporate Agents) Regulations 2015, schedule III; IRDAI (Insurance Services by Common Service Centres) Regulations 2015, schedule IV; IRDAI (Insurance Surveyors and Loss Assessors) Regulations 2015, regulation 16

confidentiality between the parties as required. However, this does not prohibit the TPA from revealing the relevant details relating to the business of TPA to any court of law, tribunal, government, or authority in the event of any inquiry being carried out or proposed to be carried out against the insurer, TPA or any other entity or for any other purpose. Further, the TPA must not share any data and personal information except as per the above exception. The Code of conduct for the TPAs also prescribes that every TPA, and its CEO, employees, etc. shall maintain such confidentiality.[64]

*Guidelines on Cyber Security:* The IRDAI, in March 2017, published an exposure draft on the draft framework for cyber security guidelines and invited feedback on the same. This was followed by the issue of the "Guidelines on Information and Cyber Security for insurers" by IRDAI in April 2017.

The guidelines only apply to insurers, who are also responsible for ensuring that sufficient data protection measures are employed by the intermediaries and other controlled organizations with whom they exchange policyholder information. Further, the guidelines apply to all data produced, obtained, or retained by insurers wherever and in whatever form they are in, in the course of carrying out their specified duties and functions.

IRDAI has recognized that data security is important at every stage i.e. data at source, in motion, in use, at rest, and at destruction, and to emphasize this, a detailed data protection framework has been formulated. Insurers have several obligations under this framework. First, they have to classify data as 'critical' and 'not critical'. This classification is based on the insurer's standards. The insurer must, with regard to critical data, establish and formulate security processes such as maintenance of an audit trail of critical data access. Secondly, access to data should be minimized and should only be allowed on a 'need to know basis'. These access rights should be reviewed by the insurer on a periodical basis. Further, to prevent the leak of data or any other data incident, insurer should obtain confidentiality undertakings from every user having access to data.

In case, sensitive data is required to be sent to third parties or outsourced service providers for business purposes, the insurer shall obtain approval for the same from the information owner. Other design controls like right protected emails, non-disclosure agreements, etc. should also be put in place to prevent misuse of data by a third party. And ultimately, there must be an effective method in place for the destruction of data.

Further, cyber security incidents that have a vital effect on business operations and a large number of customers should be reported to IRDAI within a maximum time of 48 hours, upon knowledge. Information security incidents wherein the credibility, availability, or confidentiality of sensitive information is potentially compromised should be reported to the IRDAI as well as the Cert-Fin within 48 hours of being detected by the Organization's Information Security Team, Security Operations Center (SOC), or information technology

[64] IRDAI (Third Party Administrators – Health Services) Regulations 2016, regulation 23

department. Relevant documents and data elements should be given alongside. In certain instances, it may not be possible to provide accurate and confirmed information prior to reporting. Organizations give their best estimate at the time of notification and update the information as it becomes available. Although these Guidelines are only are prescriptive in nature, they require insurance companies and intermediaries to follow certain laws such as the IT Act.

Further, insurance companies and their intermediaries are required to have the following:

i. a uniform and comprehensive framework for cloud, data, cyber and mobile security;
ii. an integrated governance system to resolve security concerns on regularly. This shall include a board approved policy on information and cyber security, a chief information security of governance framework.

Moreover, the following measures must be taken:

i. appointment of a chief information security officer and creating of the Information Security Committee;
ii. preparation of a gap analysis report;
iii. creation of a cyber crisis management plan;
iv. finalization of the board approved policy on cyber security;
v. creation of an information and cyber security assurance Programme
vi. completion of the comprehensive information and cyber security assurance audit in a phased manner.

From the above requirements and in the absence of any contrary law, IRDAI appears to have made it possible for information, records, and data to be exchanged with third parties for business purposes, provided that sufficient consents are obtained; and security measures are placed in place to ensure confidentiality and security of such information and record.[65]

*Guidelines of E-commerce:* E-commerce has hugely impacted and changed the trade systems in more ways than one. There is no stopping e-commerce and as more and more people gain access to the Internet, the traditional assumptions and methods of trade are slowly being replaced.

The Indian e-commerce industry has been on an upward growth trajectory and is expected to surpass the US to become the second largest e-commerce market in the world by 2034. With growing internet penetration, internet users in India are expected to increase from 445.96

[65] Indranath Bishnu & Supriya Aakulu, 'Data Protection in the Indian Insurance Sector – Regulatory Framework Part II' (*Indian Corporate Law*, 14 May 2019) <https://corporate.cyrilamarchandblogs.com/2019/05/data-protection-indian-insurance-sector-regulatory-framework-part-2/> accessed on 1 January 2021

million in 2017 to 829 million by 2021.[66] Soon paperless transactions will be as high as cash transactions in the economy, if not higher.[67]

Mostly, the financial sector has been trying to keep up with the advent of the Internet and e-commerce, however, the insurance industry has been slow to adapt to and adopt the Internet. [68] E-commerce is an effective way to increase insurance penetration and financial inclusion across the country. In furtherance of this, IRDAI issued these 'Guidelines on lnsurance e-commerce' in 2017. These guidelines have been issued to increase electronic transactions in the insurance sector, but they are merely enabling in nature. They apply to insurance companies, intermediaries, etc. who set up an Insurance Self Network Platform ("**ISNP"**) (i.e., a website or mobile application), for selling and servicing insurance products.

Under these guidelines, an ISNP is required to have appropriate internal mechanisms to review, monitor, and assess its systems, procedures etc to ensure that:

i. the integrity of the automatic data processing systems is safeguarded;
ii. privacy is maintained at all times.

Further, these mechanisms should be reviewed annually by certain specified persons. The Guidelines also lay down some additional obligations that ISNP is expected to comply with, to ensure the protection of personal information and data security, including:

i. preserving confidentiality and preventing misuse of personal information obtained during an insurance transaction;
ii. adopting measures to ensure the privacy of data and installation of adequate systems, to prevent manipulation of records and transactions prior to commencing operations;
iii. to assess and report such safeguards to the sub-committees of its board of directors for corrective action, if necessary.

## 4 ANALYSIS AND CONCLUSION

With the advent of technology and digitization, businesses and organizations across industries are collecting, storing, and using more and more data every day. When it comes to the insurance industry, insurance companies face a rather unique challenge. Not only is an extraordinary amount of data collected but this data is more often than not highly personal

[66] 'E-Commerce' (*India Brand Equity Foundation*, July 2019) <https://www.ibef.org/download/E-Commerce-July-2019.pdf> accessed 1 January 2021
[67] Kamalji Sahay, 'How e-commerce in insurance can be a game-changer' (*Financial Express*, 24 June 2016) <http://www.financialexpress.com/industry/banking-finance/how-e-commerce-in-insurance-can-be-a-game-changer/283778/> accessed 1 January 2021
[68] 'PwC's Insurance Insights Analysis of regulatory changes and impact assessment for March 2017' (*PwC*, May 2017) <https://www.pwc.in/assets/pdfs/ras/financial-services/compliance-cco-advisory-services/insurance/pwcs-insurance-insights-analysis-of-regulatory-changes-and-impact-assessment-for-march-2017.pdf> accessed 1 January 2021

and sensitive.[69] Further, in order to have accurate pricing of risk, insurance companies are increasing their usage of data.[70] While this has many benefits, the risks involved are also enormous when it comes to data protection. Major risks involved are:

***Lack of privacy:*** In India, the right to privacy is now recognized. In 2017, the Hon'ble Supreme Court in the case of *K.S. Puttaswamy v Union of India*[71] held that the right to privacy forms a part of the right to life and liberty under Article 21 of the Indian Constitution. The Court also struck down the previous judgments[72] which held that the right to privacy is not a constitutionally protected right. Thus, in India, individuals have the right to decide how their personal data is collected, even though this is not an absolute right. The collection of sensitive and personal data by insurers can undermine this right.

***Exclusion:*** Based on the data collected by insurers, they may discriminate in granting insurance contracts and risk pricing. This is especially relevant in terms of genetic discrimination. An insurer may use genetic information to deny insurance to individuals. The right to privacy should also be extended in order to protect an individual's genetic information.[73] Further, compelling new customers to undergo genetic testing also poses the issue of privacy from the context that do individuals have a right to not have a genetic condition disclosed even to themselves.[74]

The Delhi High Court in *United India Insurance Company Limited v Jai Prakash Tayal,*[75] emphasized on the need for a framework to ensure confidentially of genetic information and prevent genetic discrimination. It was observed that insurance companies cannot use genetic disorders as a general exclusion in insurance contracts under the guise of freedom to contract. After this decision, IRDAI directed insurance companies to not include genetic disorders as one of the exclusions while granting health insurance policies. [76] However, there is still no framework to ensure the confidentiality of such data.

***Insurtech:*** The most relevant technological advancement in the insurance industry is insurtech. **Insurtech is *'technology developed or used specifically for insurance operations applications.'*** [77] It includes, within its purview, various innovations that can potentially cause

[69] Juliana De Groot, 'Top Security Considerations for Insurance Companies' (*Data Insider*, 20 January 2020) <https://digitalguardian.com/blog/top-security-considerations-insurance-companies> accessed 1 January 2021

[70] *The role of insurance regulators in dealing with consumer data protection risks arising from increased data availability and usage?* (Access to Insurance Initiative, 2018)

[71] (2017) 10 SCC 1

[72] *MP Sharma v Satish Chandra* AIR 1954 SC 300; *Kharak Singh v State of UP* AIR 1963 SC 12952

[73] Janet A Kobrin, 'Confidentiality of Genetic Information' (1983) 30 CLA Law Review 1283

[74] Subhash Chandra Singh, 'Protection of Human Genetic Information: Balancing Interests in the use of Personal Genetic Data' (2013) 55 JILI 175

[75] (2018) 247 DLT 379

[76] *see, Religare Health Insurance Co Ltd v Arpan Dhawan* 2018 SCC OnLine NCDRC 1207; IRDAI Directions of High Court of Delhi at New Delhi on Exclusions related to Genetic Disorders <https://www.irdai.gov.in/ADMINCMS/cms/whatsNew_Layout.aspx?page=PageNo3426&flag=1> accessed 1 January 2021

[77] Faith Roberts Neale, Pamela Peterson Drake & Theodoros Konstantopoulos, 'InsurTech and the Disruption of the Insurance Industry' (2020) 43 Journal of Insurance Issues 64

major disruptions in the insurance sector. Examples of the same are Big Data, Internet of Things, DLT, smart contracts, etc.

In 2018, the IRDAI's Working Group on InsurTech published its report[78]. The responsibility of the Working Group was to make look into the regulatory framework surrounding InsurTech and make recommendations to improve the same. One of the recommendations of the Working Group was for IRDAI to set up a regulatory sandbox. In light of this recommendation, a Committee was set up by the IRDAI took look into the same. Considering the enormous potential of insurtech innovations and today's rapid pace of change, it was observed that regulations have to evolve in order to both protect policyholders and promote innovation. The Report of the Committee[79] laid down a draft framework for the regulatory sandbox to be set up by IRDAI. In July 2019, the Insurance Regulatory and Development Authority of India (Regulatory Sandbox) Regulations, 2019 were notified.

There is no single definition of "regulatory sandbox," and sandboxes have been implemented in various ways by different regulators. However, in general, it can be understood as a process for companies to test new products, services, delivery channels, or business models in a live environment, subject to appropriate conditions and safeguards.[80] The critical feature that distinguishes a regulatory sandbox from other tools used to facilitate innovation is testing in a live environment—that is, real transactions with real customers or counterparties.

With respect to confidentiality of personal information and data security, the 2019 Regulations provide that personal data collected during testing must be kept confidential and misuse of the same must be prevented. To ensure this, the applicant must put in place measures to maintain the confidentiality of policyholder data and adequate systems to prevent manipulation of records and transactions, before commencing the testing. Where any other person (other than an insurer or an insurance intermediary) engages with an insurer or insurance intermediary in executing the innovation, it is the responsibility of the insurer or the insurance intermediary, as the case may be, to ensure that no personal information pertaining to the policyholders is parted or retained with that other person. Similarly, where an insurer, insurance intermediary, and the third party are jointly involved in implementing the innovation, it is the duty of the insurer and insurance intermediary to ensure that personal data of the policyholder is not parted or retained by the third party.

While IRDAI has provided some guidelines on data security, there is still ambiguity. For instance, IRDAI has failed to explain how consumers shall be compensated in case the experimentation goes south. This could have been easily avoided by ensuring that sandbox

[78] Working Group to examine innovations in insurance involving wearable/portable devices, *InsurTech - Working Group Findings & Recommendations* (Insurance Regulatory and Development Authority of India, 2018)

[79] Committee On Regulatory Sandbox In Insurance Sector In India, *Report of the Committee On Regulatory Sandbox In Insurance Sector In India* (Insurance Regulatory and Development Authority of India, 2019)

[80] Michael Wechsler, Leon Perlman & Nora Gurung, 'The State of Regulatory Sandboxes in Developing Countries' (2018) SSRN Electronic Journal < https://ssrn.com/abstract=3285938> accessed 1 January 2020

entities have to take indemnity insurance of an adequate amount. This has been done by RBI in its sandbox.[81] Further, despite their guidelines on this issue, IRDAI has not undertaken any risk analysis before formulating the guidelines on consumer and data protection. This may act as a deterrent for potential consumers of the sandbox entities as the guidelines may not be enough if they aren't based on a proper analysis of the risks involved in the Indian context. Further, IRDAI also did not consult the Central Government in this regard.

***Data theft:*** If the personal and sensitive data received from customers is not properly encrypted and secured, the same can be misused to inflict harm on such individuals.

***Financial loss:*** Data theft leads to the exploitation of data in order to financially harm the individuals. With new technologies, it has become even more easier to fraud people.

***Reputation risk:*** A customer's information may be accidentally used in a way that harms their reputation. This is especially true for health information.[82]

**Sectoral Laws & Co-regulation**

Jurisdictions can choose between a single regulator for data protection or having sectoral regulators like the financial authority or the securities regulators making appropriate data protection laws. The latter has been employed by the US as discussed previously. In general, having adequate regulations by relevant regulatory authorities seems to be more favourable than having a single piece of legislation.[83] This way the regulators can keep up with the changing demands of the relevant technologies in their sector which the Legislature or the courts may not adequate expertise in. Further, it is more feasible for the regulators to update these regulations as and when required in their jurisdiction instead of amending a central legislation. Moreover, the kind of data an individual may be willing to disclose will depend on the kind of activity involved. This reasoning also favours sectoral laws over a unified law. As per the challenges and demands of its industry, the finance, securities, insurance, health regulators, etc. can set their data protection standards and regulations.

It has also been argued time and again that sectoral laws would lead to gaps and lacunae in the coverage of the law.[84] However, to conciliate these two opposite approaches, jurisdictions can have a general unified law that oversees data protection in the country but at the same time, regulators should be empowered to make specific additional regulations and requirements for their sectors.[85] For instance, while drafting the Personal Data Protection Bill

[81] Reserve Bank of India, Enabling Framework for Regulatory Sandbox

[82] *The role of insurance regulators in dealing with consumer data protection risks arising from increased data availability and usage?* (Access to Insurance Initiative, 2018)

[83] Lalit Panda, 'The Weight of Secrets : Assessing the Regulatory Burden for Informational Privacy in India' (2019) 15 IJLT 40

[84] Paul M Schwartz, *The Value of Privacy Federalism' in Social Dimensions of Privacy : Interdisciplinary Perspectives* (Cambridge University Press, 2015)

[85] Lalit Panda, 'The Weight of Secrets : Assessing the Regulatory Burden for Informational Privacy in India' (2019) 15 IJLT 40

2018, the Srikrishna Committee envisaged the requirement of the Data Protection Authority to consult with different regulators.[86]

Additionally, apart from sectoral regulations and laws, an environment should be inculcated by the regulators to encourage best practices and codes of conduct in their sectors. This is called co-regulation and involves private entities' active participation.[87] In 2012, the AP Shah Group of Experts[88] recommended this approach of co-regulation in data and privacy protection. The Srikrishna Committee also endorsed it as *"an appropriate middle path that combines the flexibility of self-regulation with the rigour of government rulemaking".*[89]

Thus, keeping the approach of sectoral laws and co-regulation in mind, it is imperative that IRDAI formulates appropriate regulations. While IRDAI mandates insurers as well as insurance intermediaries to ensure the protection and confidentiality of data, there are no further compliances on how this is to be achieved. The only guidance is in the form of cyber security and e-commerce guidelines prescribed by the IRDAI however, these are mere directory and not mandatory. While they may act as adequate codes of conduct, there is still a need for a comprehensive regulation on the same which makes it obligatory on the insurers and intermediaries to install certain systems and safeguards to ensure data protection and privacy. Looking at EU's comprehensive GDPR law, these regulations must take into account data handling requirements, consent requirements, reasonable use, classification of data, etc.

[86] Committee of Experts under the Chairmanship of Justice B.N. Srikrishna, *A Free and Fair Digital Economy : Protecting Privacy, Empowering Indians* (Ministry of Electronics and Information Technology, 2018)
[87] Rukhmini Bobde, 'Data Protection and the Indian BPO Industry' (2002) 2 Law Rev GLC 79
[88] Planning Commission, *Report of the Group of Experts on Privacy* (Government of India, 2012)
[89] Committee of Experts, *White Paper of the Committee of Experts on a Data Protection Framework for India* (Ministry of Electronics and Information Technology, 2017)