PERSONAL DATA PRIVACY

Overview of Justice Srikrishna Committee Report

Dr. Karnika Seth

PERSONAL DATA PRIVACY

Overview of Justice Srikrishna Committee Report

By

Dr. Karnika Seth

Cyber law Expert & Advocate, Supreme Court of India

LL.B (Faculty of Law, University of Delhi),

LL.M (Kings' college, University of London)

Ph.D. (Noida International University)

Visiting Faculty, National Judicial Academy, National Police Academy,

Central Bureau of Investigations and National Investigations Agency

Printed in India.

PREFACE

At a time when Cambridge Analytica episode flashed in the media world over, personal data and privacy has been a major subject of deliberation in India. This wave began with Aadhar being challenged in the Supreme Court of India. The Recommendations of the Justice Srikrishna Committee on Personal data, the Personal data protection bill which the Committee culled out put the spotlight on issues of data protection and privacy in India in an unprecedented manner. The Justice K.S Puttaswamy v UOI case was finally decided this year by the Apex Court, a landmark judgement upholding the Right to Privacy as a fundamental right of every citizen of India. The Supreme Court of India also put to rest many concerns over Aadhar card usage by upholding constitutionality of the Aadhar Act but striking down many provisions of the Act, interalia, and declaring collection by private operators and banks without express consent of citizens as illegal.

While reading the Justice Srikrishna Report, I realised it may be onerous and time consuming for a reader to read and understand the 213 page document. In this book, I have encapsulated the key recommendations of the Committee for easy understanding of wide range of readers. The language used is kept consciously simple and summary of recommendations has been provided with my views on the key focal points therein. I hope the readers will find it informative & useful!

Your questions are welcome. Please feel free to write to me at: karnika@sethassociates.com.

Dr. Karnika Seth

ABOUT THE AUTHOR

Dr. Karnika Seth is an internationally renowned Cyber law expert & is the Founder Partner at Seth Associates law firm in India. Dr. Seth is also the Chairperson of Lex Cyberia at Seth Associates, the World's first integrated cyber laws research, forensics and legal consulting centre. Dr. Seth is one of World's leading authorities on cyber law & also known as a prolific Author & Educator on the subject. Her contribution to growth & development of cyber laws and spreading its awareness internationally and in India is widely acknowledged in the corporate world and by International organisations. She contributes to various Working Group Consultations and ICANN discussion forums aimed at designing policies for Next Generation Internet. She is part of Expert Panel of UNICEF working on children safety in the online world and actively associates with International Centre for Missing and Exploited Children (ICMEC) in its Think Tanks & cyber awareness activities in India. She is also associated with the International Telecommunication Union's initiatives and is a member of the Global Cyber Security Forum. Her expert views on cyber safety have been solicited by Indian Parliament and the Ministry of Information Technology, National Commission for the Protection of Child Rights for strengthening cyberlaws in India. She is empanelled as legal expert to advise National Internet Exchange of India and the Office of Comptroller of Certifying Authorities constituted under the IT Act, 2000. She is member of Advisory Board of various educational institutions and was conferred title of Honorary Professor by Amity University in 2017.

Dr. Seth practices law at the Supreme Court of India and is principal legal advisor to many multinational groups and government entities. She has actively resolved complex Cybercrime cases in conjunction with the law enforcement authorities in India. She is also an Expert IT law Educator & Trainer to law enforcement authorities in India including the National Judicial and Police Academy, Central Bureau of Investigations and The National Investigation agency.

Dr. Seth writes extensively on key legal and cyber awareness issues for newspapers, journals and periodicals from time to time. Ms. Seth's book titled 'Computers, Internet and New Technology Laws' published by Lexis Nexis Butterworths elucidates the key developments in the field of Cyber laws across many important jurisdictions, India, United States and European nations. Dr. Seth was conferred the Law Day Award from the Chief Justice of India for authoring the comprehensive reference book in 2012. She received the Digital Empowerment Award for the year 2015 and the Law Day Award in 2015 for authoring the book, Protection of Children on Internet. In 2017, Dr. Seth was conferred the National Gaurav Award for exemplary contribution to the field of cyber laws in India. In 2018, she received the Law day award for authoring the Manual for e-filing in High courts & district courts as probono support to national e-courts project to be used by 18000+ courts in India. She regularly contributes her views on the subject in conferences, print & electronic media and television.

Table of Contents

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA

CHAPTER IV

GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

CHAPTER V

PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

CHAPTER VI

DATA PRINCIPAL RIGHTS

CHAPTER VII

TRANSPARENCY AND ACCOUNTABILITY MEASURES

CHAPTER VIII

TRANSFER OF PERSONAL DATA OUTSIDE INDIA

CHAPTER IX

EXEMPTIONS

CHAPTER X

DATA PROTECTION AUTHORITY OF INDIA

CHAPTER XI

PENALTIES AND REMEDIES

CHAPTER XII

APPELLATE TRIBUNAL

CHAPTER XIII

OFFENCES

CHAPTER XIV

TRANSITIONAL PROVISIONS

CHAPTER XV

MISCELLANEOUS

CHAPTER 1

INTRODUCTION

1.1 BACKGROUND

In India, Data Protection and privacy has been the focus of debates and discussions with legislators and other stakeholders throughout 2017-18.2018 proved to be an important year in the evolution of privacy rights in the country. The Supreme Court of India passed a landmark judgment in the *Puttu Swamy's case*[1] upholding the right to privacy as a fundamental right under Article 21 of the Constitution of India. The Supreme Court also passed the Judgement declaring Aadhar card is not mandatory unless a citizen voluntarily applies for subsidies offered by the government or consents to parting his own information[2]. The question of

[1] (2017) 10 SCC 1. see https://www.livelaw.in/aadhaar-judgment-certain-concerns/

[2] Aadhaar was introduced under the Planning Commission during in 2009. The Aadhaar Bill was introduced in 2010 but it was rejected by a parliamentary Committee over security, and privacy concerns. The NDA government passed the Aadhaar Act as a Money Bill in March 2016,

dignity, right to disclosure of own information and consent formed the basis for the privacy rights with respect to the Aadhar scheme. While upholding the constitutional validity of Aadhaar scheme, the Constitution Bench of the Supreme Court in **Justice K.S. Puttaswamy vs Union of India** has ruled that Aadhaar Act doesn't violate your right to privacy when you voluntarily agree to share biometric data. Private entities have been barred from using Aadhaar card for KYC authentication purposes but one still requires Aadhaar for various other purposes including PAN card and ITR filing.

When the Aadhar matter was pending before the Supreme court of India several incidents of security threats to one's personal information were reported in media. In one such report, an expose by Rachna Khaira in the Tribune revealed that Aadhar Data base could be purchased for a meagre amount of Rs.500. This raised privacy concerns and consumer groups voiced their concerns at various forums across India. Subsequently, A FIR was registered to investigate the alleged data breach. The vulnerability of the people is accentuated by the fact that State collects sensitive personal information such as religion and caste in their State Resident Data along with Biometrics. UIDAI (Unique Identification Authority of India) collects the same as part of the enrolment and use of software with terms 'DBT Seeding Data Viewer' and in new code 'Rapid Aadhar Seeding Framework (RASF)'. In a state like Andhra Pradesh even minor traffic offences are linked with Aadhar. The police also have access to Biometrics for identifying criminals and missing children. Although

UIDAI claimed that its server is secured and no data has been breached on their server, Opposers' of UIDAI claimed it has no capability to audit the security practices of even its licensed ecosystem of 300 agencies who have access to the main data base, sub licensed access and combined with other data. Through the Aadhar judgement, the constitutional validity of the Act has been upheld and the apex court has struck down provisions such as section 33(2) [allowing for disclosure of information in case of national security exception] as well as section 57 [which allows the private entities to use Aadhaar for identification]. However, the security concerns of Aadhar database ought to be stepped up to alleviate the security concerns of its citizens. In the U.S, the social Security Number is protected with a fool proof security though it does not have a photo identity and only collects demographic information & excludes biometric data. Apart from security concerns, legal concerns currently coexist due to fact that if a new law is brought into place that allows private entities to collect Aadhar data for authentication purposes, it may fall within "procedure established by law" and seek a way to invade the privacy of citizens and circumvent protection offered by Art.21 of the Constitution. The right to privacy cannot be invaded except according to procedure established by law. Article 21 Provides that: *"No person shall be deprived of his life or personal liberty except according to procedure established by law."*

Amidst this controversy that surrounded Aadhar, another issue that challenged privacy regime was proposal of government to establish a social media hub. The recent

proposal of the Government to establish a Social Media Hub was largely opposed by the public on the ground that it would clearly violate its right to privacy. The opposition was so strong that the same would amount to 24X7 surveillance on its citizens the Government was compelled to withdraw the said proposal. In my own view, such social media hub could mean open surveillance by government as their electronic communications cannot be scrutinised without any reasonable cause of conducting such surveillance. It would tantamount to fishing expedition directly invading privacy of citizens. Thus rightly so, Indian citizens urged the government to uphold the principles of democracy and voiced their concerns over data protection and privacy.

Justice B.N Shri Krishna Data Protection Committee Report has come at an apt time when it is imperative for India to form a comprehensive legal frame work to protect personal data of its citizens. While the US follows a laissez faire approach and does not have 'overarching data protection framework', the US courts have recognized the right to privacy as reflected in first, fourth, fifth and fourteen amendments to the US Constitution. In US certain laws such as the Privacy Act, 1974, the Electronic Communications Privacy Act, 1986 and the right to Financial Privacy Act,1978 protect the citizens against the federal government. As regards private entities there are sector specific laws such as the GLB Act has provisions to collect and use financial data. In European Union, the GDPR was brought into force on 25th May,2018 and repeals the Data Protection Directive of 1995. China also

enacted a special law known as the Cyber Security Law in 2017 mainly to avert National Security risks. In *Justice K. S. Putta Swamy's (retd.) versus Union of India*, the right to privacy was recognised as a fundamental right incorporated in Article 21 of the Constitution. The terms of reference of the Justice Srikrishna Committee required study of various data protection issues in India and make recommendations for its framework and a draft bill. The objective of the government of India in setting up of the Committee as contained in the terms of reference stated 'to unlock the data economy by keeping the data of citizens secured and protected'. The Committee realised that this objective is based on the fact that data can both empower as well as harm an individual. While formulating the report the Committee was seized with the fact that in today's world digital economy is growing and concepts like artificial intelligence and big data can be useful for profit of the society. It noted that a breach of personal data can also play havoc in the society. The recent revelation that data of 87 million users was shared by Facebook with Cambridge Analytica through a third party application which extracted the personal data of its Facebook users who downloaded the application shows such possible harm. This data was further used to place targeted advertisements around the US Elections. In a scenario where companies are continuing to use ambiguous data collection policies and practices and obtaining consent through its terms and conditions in lengthy fine print, the common man may neither read nor understand them. He/she may not realise that with a click he/she has

formed a legal contract which is deemed to be a valid consent. It is thus imperative to devise concrete principles to define the valid means of obtaining consent, contours to define the limits of reasonableness also become necessary.

1.2 Current Provisions of IT Act, 2000 & Privacy

As on date when the Committee was formulating its recommendations the current IT Act, 2000 had little to protect the privacy of its citizens. Section 43A of the IT Act, 2000 obligates a body corporate to maintain reasonable security practices to safeguard any data it collects, possesses, deals or handles which is of sensitive nature. Any negligence in doing so which causes wrongful loss or wrongful gain to any person is liable to pay damages to such person affected. Sensitive Personal Information was defined by the Rules issued under Section 43A of the IT Act. [3] 'Sensitive Personal Data' means such information which consists of Password, Financial Information such as bank account, credit card or debit card, physical, physiological, metal health condition, sexual orientation, medical records and history, biometric information any such detail provided to body corporate for providing any service and any information received by body corporate for processing or storing under a lawful contract or otherwise[4].

[3] Rule 3, IT (Reasonable Security practices and procedures and Sensitive personal Data Protection Rules), 2011('SPD rules')
[4] ibid

Any information which is freely available in public domain or furnished under the Right to Information Act, 2005 or other law is excluded from the purview of Sensitive Personal Data by these Rules. The SPD Rules requires prior consent of a user before disclosing Sensitive Personal Data to a third party.[5] It requires anybody corporate who collects, receives, possesses, stores or deals with personal information of a user to provide a detailed privacy policy on its website explaining the purpose of collection of specific types of personal information, its use and disclosure practices and deployment of reasonable security practices to protect it. A recommended standard therefor is ISO 27001. Rule 5 of the said Rules require any body corporate to obtain consent in writing through letter or fax or email from the provider of such information regarding the purpose of its use. A body corporate can collection information only for a lawful purpose and connected with the function or activity it engages in. Moreover, collection of Sensitive Personal Data is only allowed when it is necessary for that purpose. The Rules also mandate that such body corporate shall retain Sensitive Personal Data or Information i.e. for a period no longer than what is required.[6] The body corporate needs to keep the data accurate and review it to correct it if found incorrect or deficient. However, the body corporate is not responsible for authenticity of information provided by a user. A body corporate before collecting information is required to give an option to the provider not to give the data

[5] Rule 6 of SPD rules
[6] Rule 5(4) of SPD Rules

sought to be collected and the provider also has an option to withdraw its consent. Such consent is required to be in writing and after withdrawal of consent the body corporate is entitled to stop providing its goods and services. [7] Transfer of Sensitive Personal Data to outside India is permitted only if the other country ensures the same level of data protection as is adhered to in India and only for the lawful contract to be performed or where such person has consented to such data transfer. [8] Another important provision that requires mention herein is that everybody corporate is required to designate a Grievance Officer and publish his name and contact details on its website. Such officer is required to redress the grievance within one month from the date of receipt of the grievance.[9] Justice Srikrishna Committee rightly noted that with the growing digital economy these rules do not sufficiently protect the users and their data. For instance, the definition of Sensitive Personal Data is very narrow and it fails to take into account many aspects of personal data. [10] Further, the obligations in the SPD Rules are inapplicable to the government and may be even overridden by contract. In addition, there are also implementation issues owing to delay in the appointment of Adjudicating Authority under the IT Act.

---

[7] Rule 5(7) of SPD Rules

[8] Rule 7 SPD Rules,2011.

[9] Rule 5(9) of SPD Rules,2011

[10] Graham Green Leaf, India – Confusion Raj with outsourcing in Asian Data Privacy Laws; Trade and Human Rights Perspectives (Oxford University Press, 2017) at page 415

The Committee used new terms to denote a Data Controller as 'Data Fiduciary' and a Data Subject as a 'Data Principal' primarily with the aim of empowering the user and imposing a clear obligation on the collector of Data as Data Fiduciary. The term 'Data Fiduciary' is based on a Fundamental expectation of Trust. An individual expects that one's personal data will be used fairly that and the data collector would have a duty of care to deal with such data for fairly and responsibly and for the purposes reasonably expected by the user. [11]

1.3 CHAPTERISATION IN THE REPORT

In Chapter 1 the Committee gives an introduction and background of the formation of the Committee and the fundamental principles while formulating the report to ensure a free and fair digital economy and preparing frame work of law that protects personal data. In Chapter 2 there is a discussion of main question relating to scope and applicability of such a law. The Committee was of the view that the question of scope and applicability ought to be answered according to the objective of securing free and fair digital economy. It thus considered that the substantive obligations contained in our law must be observed if the data of Indians is processed even abroad. However, it recognised that such objectives

[11] Tamar Franken, Fiduciary Law, 71(3) California Law Review (1983) at page 795. The Data Protection Committee Report 2018, page 8

cannot be achieved without observing international comity and respective sovereignty of other jurisdiction in enforcing its own rules. This is particularly important, in my view since 90% of data of Indian citizen is parked in servers abroad and is processed by entities abroad such as by google, facebook, whatsapp, and other service providers.

In Chapter 3, the Committee observes that the primary basis for processing any personal data is the individual consent. The Committee has proposed form and substance obligations on entities that require consent and effective means for individuals to withdraw consent. Chapters 4 and 5 elucidate the obligations on data fiduciaries and the rights of data principals. The use of data as well as its collection and use ought to be for fair and lawful purposes. Here the scope of such rights, the limitations and enforcement mechanism are discussed in detail. Chapter 6 deals with the localisation of personal data for local storage and processing requirements. Chapter 7 deals with the impact of the proposed data protection framework on allied laws particularly the IT Act, the Aadhar Act and the RTI Act. Chapter 8 discusses those grounds where consent may not be required for processing personal data such as national security, prevention and investigation of crime, allocation of resources for human development, protection of revenue. These have been also recognized in the *Putta Swamy's case* as legitimate interest of state. The Committee recognised two categories of such situation, one where processing can take place without consent

(non-consensual grounds) and secondly where substantive obligations of the law applied partially (exemptions). The Committee is of the view that the enforcement of law can be achieved by both internal and external measures. While enforcement requires setting up of an authority with sufficient powers to enforce a law pertaining to data protection, internal enforcement requires adoption of policy measures such as code of practice which may be developed in consultation with sectoral regulators, regulated entities and data principals through an open and participatory process.

Chapter 9 describes the enforcement machinery under the proposed framework. In the conclusion part the report contains the summary of recommendations to the Government of India to enact the Data Protection Law. The Committee also provided a draft of such a law, the Personal Data Protection bill along with the report. In order to formulate the report, the Committee conducted wide consultations with the public a white paper was published by the Committee on 27th November, 2017 for comments. Four public consultations were conducted in New Delhi on 5th January, 2018, Hyderabad on 12th January, 2018, Bengaluru on 13th January, 2018 and Mumbai on 23rd January, 2018.

CHAPTER 2

RECOMMENDATIONS ON JURISDICTION, PROCESSING, DATA FIDUCIARIES

2.1 JURISDICTION

On the issue of jurisdiction, the Justice Srikrishna Committee was of the view that the Data Protection Law will have the jurisdiction over the processing of personal data if such data has been used, shared, disclosed, collected or otherwise processed in India. In case such data is processed by fiduciaries outside India, the law shall apply to those who carry business in India or other activities such as profiling that may cause privacy harm to data principals in India. In case personal data is collected, used, shared, disclosed or otherwise processed by companies set up under Indian Law, these will be covered irrespective of where it is actually processed in India. The Committee was of the view that the data protection law may empower Central Government to

exempt those companies which only process personal data of foreign nationals who are not present in India.[1] Further, this law has been proposed to come into force in a structured and phased manner. It will apply to processing which is ongoing after the law is brought into force. It is envisaged that different time lines should bring into force different parts of the law.[2] The Committee rightly considered that the fiduciaries physically not present in India but operating its websites need to be regulated under Indian Law. The Indian Courts have recognised the difference between active websites and passive websites in a number of cases and considered the target viewers' approach in a forum state for commercial transactions resulting in harm in the forum state. The Courts have interpreted the principles of Trade Mark Act and the Copy right Act are applicable to those persons who are not residents of India but carrying on business in India.[3]

2.2 Identifying Personal data

The Committee considered various categories of data such as financial details, password, biometric data, religious and political views amongst other types of data. It also considered

[1] Section 2 and 104 of Personal Data Protection Bill

[2] Section 97 of the Personal Data Protection Bill

[3] Banyan Tree Holding versus Murali Krishna 2010(42) ptc 361, Icon Health and Fitness Inc. versus Sheriff Osman and others 2017 SCC Online 10481, World Wrestling Entertainment versus Reshma Collection and others 2014 SCC Online Del. 2031

the challenge of identification and de-identification of data. It noted that in some cases it could be possible to identify individuals from data sets which are seemingly anonymised[4]. In some countries like Europe and South Africa anonymised data[5] is out of the purview of the Data Protection Law and in some country pseudonymisation[6] is also encouraged. The Committee recommended the definition of 'Sensitive Personal Data' will include passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data and data that reveals trans-genders status, inter-sex status, caste, tribe, religious or political believes or affiliations of an individual. According to the Committee, the Data Protection Authority would have the residuary power to notify further categories in accordance with the criteria set by law[7].

The proposed Data Protection Law would cover processing of personal data both by public and private entities.[8] The standard for anonymization and de-identification will be laid down by the Data Protection Authority. The de-identified data will continue to be within the scope of the Data Protection Law, but the anonymised Data that fulfils the standards laid down by the Data Protection Authority will be exempted from the law.[9]

---

[4] Paul Ohm, Broken promises of privacy; responding to the surprising failure of anonymization, 57 UCLA Law Review (2010) Act pages 1717 to 1722.

[5] See Recital 26, EU GDPR, Section 6, POPI Act

[6] Article 4(5), Articles 25 and 32, EU GDPR

[7] Sections 3 (35) and 22 of the Bill.

[8] Sections 3(13) and 3(15) of the Bill

[9] Sections 3(3), 3(16) and 61(6) and (m) of the Bill

2.3 Valid Consent

The Committee recommended that the consent will be the legal basis for processing personal data and proposed a modified consent framework that will apply a product liability regime. In order to make the data fiduciary liable in case any harm is caused to the data principal[10],the Committee laid down a criteria for a consent to be valid, namely, it should be free, informed, specific, clear and capable of being withdrawn and in case of Sensitive Personal Data consent is required to be explicit.[11]Explicit consent needs to be in clear form , prominently placed to draw significant attention of a reader, for example in bold letters and express and not hidden in small print in ambiguous words in a document.

2.4 Consent from children

With a view to protect children and their data online, the Committee recommended that a data principal below the age of 18 years will be considered children. The data fiduciaries will be under a general obligation to ensure that any data is collected and processed with respect to children have their best interest in mind. The data fiduciaries that may cause significant harm to children will be identified as Guardian Data Fiduciaries. All Data Fiduciaries including

[10] Section 12 of the Bill
[11] Section 12 and 18 of the bill

the Guardian Data Fiduciaries shall adopt appropriate age verification mechanism and obtain parental consent. It is suggested by the Committee that the Guardian Fiduciaries should be barred from certain practices, but those exclusively offering counselling services or other similar services will not be required to obtain parental consent.[12]

2.5 PURPOSE LIMITATION

In Chapter 4 of the Committee Report the Committee examined the new challenges brought by the growing digital economy and the emerging technologies of the big data and artificial intelligence and machine learning. The Committee emphasised on the importance of planning for a data protection framework which respects individual autonomy and ensures fairness and transparency. The Committee noted that the obligations of fiduciary need clear delineation. This is essential to prevent abuse of power and ensure accountability and responsibility on the part of a data fiduciary. The processing of data must be within the reasonable expectations of the data principals and the same applies to entities with whom the fiduciaries shares such data in order to perform its services. It also laid stress on the purpose limitation and data minimization requirements. This requires two factors- first the purpose for which the personal data is processed should be clearly specified and the processing should be limited to

[12] Section 23 of the Personal Data Protection bill.

such purposes. Minimum data necessary for achieving the purpose could be collected and used only for the specified purpose and other compatible purposes. Big data processing includes data collection from volunteered, observed, inferred or legally mandated data sets, involves big data storage and aggregation, analysis of such aggregated data through machine learning and use for prediction and targeting.[13] The Committee noted that while big data analytics may not relate to identify individuals such as predictions of weather patterns, it could be also used to target products through particular individuals through behavioural advertising. Such targeting can be useful to provide quicker emergency care or track students' performance but it may lead to tangible harms such as inaccurate personal data, denial of service and discrimination. Thus, the Committee considered big data processing poses a challenge to principals of collection limitation and purpose limitation. The Committee recommended that the relationship between the 'data subject' and 'data controller' is reformulated as fiduciary relationship between the 'data principal' and the 'data fiduciary'.[14] The Committee suggested that all processing of personal data ought to be fair and reasonable.[15] The principles of collection and purpose limitation applies to all data fiduciaries unless

[13] International Working Group on Data Protection in Telecommunications, working paper in big data and privacy, privacy principals under the age of big data analytics (2014)

[14] Section 3(13), 3(14) of the Personal Data Protection bill

[15] Section 4 of the Personal Data Protection bill

specifically exempted.[162] Processing of personal data with big data analytics in cases where the purpose of processing is not known at the time of its collection and cannot be communicated to the data principal can be performed only after exclusive consent is obtained from him. The Committee puts the obligation to maintain transparency and provide notice to the data principal before or at the time of collection of one's personal data.[17]

2.6 STORAGE OF PERSONAL DATA

Obligations of data quality and storage limitation on data fiduciaries was also suggested though the main responsibility to ensure accuracy of data lies with the data principal.[18] The Committee suggested a provision of personal data breach notification to the Data Protection Authority and in some cases to the Data Principal. Data security obligations such as maintaining reasonable security practices as described under Rule 8 of the SPD Rules will be followed e.g. ISO 27001 is an international standard recognised under IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. Industry Associations which follow their own standard need to get these approved and notified by the Central Government. These obligations to ensure data security are also found in EU GDPR which adopts

[16] Section 5 and 6 of the bill
[17] Section 8 and 28 of the bill
[18] Section 9 and 10 of the Personal Data Protection bill

the principles of confidentiality, principle of transparency, security of data.[19] Even the OECD principals elucidates security safeguards involving physical, organisational and informational measures to protect data.[20]

2.7 Data breach notification

The Committee explained that the definition of personal data breach would account for three main principles of information security, confidentiality, integrity and availability.[21] Confidentiality breach means an unauthorised or accidental disclosure of or access to personal data.[22] Integrity breach means unauthorised or accidental alteration of personal data and availability breach is caused when there is accidental or unauthorised loss of access to or destruction of personal data. The Committee observed that organisational measures are important for data fiduciaries to perform fair and reasonable processing. This can be ensures through asserting individual rights or through appropriate audit mechanism and regulatory actions. This framework has been incorporated based on a rights approached in the EU GDPR. The EU GDPR puts an accountability obligation on the data controllers and

[19] Article 5(1)(f) EU GDPR.

[20] OECD, OECD Guidelines on protection of privacy and trans-border flow of personal data (2013)

[21] An example cited by the Committee was Article 33(1) of EU GDPR, Section 6, News Mexico Data Breach Notification Act, 2017

[22] White paper of the Committee of Experts on Data Protection Framework for India

urges them to demonstrate the compliance through concrete organisational measures.[23]

[23] Art 29 Data Protection Working Party recommended the principle of accountability in the EU's Data Protection Law, See Article 5(2) GDPR.

CHAPTER 3

RECOMMENDATIONS-DATA PRINCIPAL'S RIGHTS & TRANSFER OF PERSONAL DATA OUTSIDE INDIA

3.1 CONFIRMATION, ACCESS AND CORRECTION

The Committee was of the view, that the rights of the Data Principal ought to be based on the 'principles of autonomy, self determination, transparency and accountability' to give the individuals control over their data which is essential for freedom in the digital economy. It noted some of these rights flow from the freedom of speech and expression and right to receive information under Article 19(1)(a) and Article 21 of the Constitution. The Committee in this chapter of the report observed that the right to object to processing, object to direct marketing and restriction of processing do not fit within the framework of lawful processing established by our Indian Legal Framework. In the EU GDPR the right to object can be enforced by an

individual even where the data is being processed lawfully under the grounds of public interest, exercise of official authority and legitimate interest. Such grounds are not found in our framework in the manner stipulated under the EU GDPR. The Committee noted that it will be difficult to mention the specific grounds that can render such objection valid and it will be ambiguous to provide a right to stop lawful processing based on unenumerated grounds. It also noted that the extent the processing is in pursuance of a law or in furtherance of a non-consensual ground, the responsibility to protect data will shift to the law which allows processing in each of these cases. For example, if Aadhar data is processed as per Aadhar Act by the Unique Identification Authority of India to maintain the integrity of the Central Identities Date Repository, processing must be in accordance with law.[1] According to the Committee's report, if the individual's circumstances change, the individual will have a remedy if the change in circumstances renders future processing illegal. According to the Committee, an overriding personal interest without describing it makes no sense.[2] As regards right to object to direct marketing the Committee concluded that the data fiduciaries can engage in direct marketing based on consent of data principal. The right to restrict processing is also unnecessary in India as the Data Principals can approach the Data Protection Authority or puts for a stay on processing in case the data is inaccurate.

[1] Sections 23(2)(j) and 23(2)(l), Aadhar Act

[2] Page 80 of the Justice Srikrishna Committee Report

The right to confirmation, access and correction were recommended to be included in the Data Protection Law.[3]

3.2 Other rights of Principal

The right to data portability was recommended to be included in the law subject to limited exceptions.[4] The right to object to processing, right to object to direct marketing, right to object to decisions based on solely automatic processing and the right to restrict processing were not provided for the above discussed reasons set out in the Report. The right to be forgotten was suggested to be adopted with the adjudication wing of Data Protection Authority to determine the applicability on the basis of five points criteria which are as follows:

(i) the sensitivity of the personal data sought to be restricted;
(ii) the scale of disclosure or degree of accessibility sought to be restricted;
(iii) the role of the data principal in public life (whether the data principal is publicly recognisable or whether they serve in public office);
(iv) the relevance of the personal data to the public (whether the passage of time or change in circumstances has modified such relevance for the public); and
(v) the nature of the disclosure and the activities of the data fiduciary (Whether the fiduciary is a credible source

[3] Section 24 & 25 of the Personal Data Protection bill
[4] Section 26 of the bill

or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not on content creation).[5]

As regards the 'Right to be forgotten', the Committee was of the view that the right shall not be available when the Adjudication Wing of the Data Protection Authority determines on conducting balancing test that the interest of Data Principal in limiting the disclosure of its personal data does not override the right to freedom of speech and right to information of any other citizen.[6] The Committee noted that the time for implementation of such rights by Data Fiduciary will be specified by the Data Protection Authority.[7] The view seems only just in view of Art 19(2) of the Constitution of India that allows placing reasonable restrictions on right to freedom of speech .Likewise, Art 21 of the Constitution of India protects right to privacy but provides an exception as it can be invaded although only by a procedure prescribed by law.

3.3 Transfer of personal data outside India:

Internet has no borders and the internet service providers freely provide their services across different countries and virtual space has become a global village. Often information collected from one country is transferred across borders for

[5] Section 27of the Personal Data Protection bill
[6] Section 27 of the bill
[7] Section 28 of the bill

provisions of services, storage or processing. This may lead to security issues and issues over violation of privacy of its users whose data is collected. Legal Scholars have advocated localisation of data can minimise the risk of security and privacy and misuse of such data also in cases of investigation, Electronic Data can found or made available more easily than in cases where data is stored across borders. This issue was discussed at length and deliberated by the Committee in chapter 6 of the Report. The Committee also considered the substantial costs that may be involved in setting up of digital infrastructure to store the data locally and observed that in the interest of free digital economy the impact of such policy may be considered. The provisional view adopted involved an adequacy test which gave the discretion to Data Protection Authority to consider if a country possesses sufficient level of protection for personal data as it would allow two way flow of personal data essential for a digital economy.[8] If such certification was missing that data fiduciary would bear the responsibility to ensure that personal data once transferred would have the same level of protection as provided for in India. Majority of commentators to the white paper proposed the adequacy test can be adopted which will facilitate greater access to markets interoperability and data protection to citizens. Certain commentators opposed the adequacy tests on the basis that the determination by Data Protection Authority would be expensive and time consuming

[8] White paper of the Committee of experts on data protection framework for India

as many countries are yet to develop the Data Protection Law. It suggested accountability of the transferor entity to ensure data protection where data is transferred abroad.[9]In my personal view, I advocate this approach for the reason that responsibility has to be taken by transferor entity in India before sharing or disclosing personal data of Indian subjects. Majority of commentators (which included major technology companies) were of the view that mandatory data localization would hamper the progress of the industry. The Committee was of the view that US can support open digital economy due to its technological advancements. It was felt that the need for local enforcement is also achieved owing to personal jurisdiction that US exercises over large number of technology companies and data stored in its territory. In European Union transfer of data from one jurisdiction to another is based on the adequacy of protection and the transfer of data is subject to approved contractual clauses and the risk of harm is minimized. Only 12 countries had received such certification from EU and data shared with the US was limited to the EU US Privacy Shield Framework.[10] The European Commission has issued two sets of standard contractual clauses. First, for transfer of data from one data controller to another data controller and second, for transfer

[9] Comments in response to white paper submitted by Cody Ankeny on 30th Jan.,2018

[10] EU US Privacy Shield Framework protects data when it is transferred from EU to US for commercial reasons it became operational on 1st August, 2016.

to data processors outside EU[11]. The binding corporate rules apply to multinational companies who need to transfer data within its group requiring approval from the Data Protection Authority of its country and that of the transferee country outside the EU. The Committee recommended that the cross border data transfer of personal data apart from sensitive personal data will be through model contract clauses which contain main obligations of the transferor and liability in case any harm is caused to the principal due to any violations of the transferee.[12] As regards cross border transfers within group entity it was suggested to formulate intra group schemes.[13] The Central Government would have the option to green light transfers to certain jurisdiction in consultation with the Data Protection Authority .[14] The Committee was of the view that sensitive personal information shall only be processed in India and not transferable abroad. The Committee recommended that the Central Government would determine the categories of such sensitive data which is critical keeping in mind the strategic interest of the nation and law enforcement.[15] In cases of medical emergency, personal data such as medical records could be permitted to be transferred for necessary

[11] Model Contracts for transfer of personal data to third country available at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-country_en (last accessed on 7th August,2018)
[12] Section 41(1)(a) of the Bill
[13] Section 41(1)(a) of the Bill
[14] Section 41(1)(b) of the Bill
[15] Section 40(2) of the bill

action or attending to emergency. Any other such data can be transferred on the basis of Central Government's approval.[16] Moreover, other types of personal data which is noncritical will be required to be stored in at least one server copy in India.[17] In my view this will be beneficial and serve interests of law enforcement as many cybercrimes fail to be properly investigated and prosecutions may not lead to convictions owing to non availability of electronic evidence from internet service providers. In many cases, such companies donot subject to jurisdiction of Indian courts and demand subpoena to be obtained from courts in U.S for seeking any electronic data from their servers.

The Committee suggested that when personal data of subjects is transferred abroad for storage or processing, the model contract should contain main obligations on the transferee entities in accordance with Indian Laws including security, purpose limitation clause, storage limitation amongst other clauses. A self certification by such entity that the contract is as per the model contract and it undertakes to bear liability for any breach by transferee will be required. These records will be audited and periodic reporting to the Data Protection Authority will also be necessary. The Committee considered that there are many cases where entities outside a particular jurisdiction do not submit to the jurisdiction of the forum or court outside India. In India MLAT requests

[16] Section 41(3) of the bill
[17] Section 40(1) of the bill

are sent.[18] This process is very time consuming and requires amendments to prove itself effective. Seeking legal assistance from abroad also entails costs. The Committee noted that between January and June, 2017 Google received 3843 user's data disclosure requests by Indian Government Agencies out of which 54% of cases some data was provided. Many internet service providers store data in the US and requests for providing such data for law enforcement purposes does not yield positive results. Thus, localisation of data will assist domestic enforcement of law enforcement purposes. Data localisation is also beneficial to create new jobs attract foreign direct investment in digital infrastructure. Creation of digital industry will prove beneficial for research and development in artificial intelligence and other emerging technologies. If data is processed in India, particularly, sensitive data it will negate the possibility of foreign surveillance. On the other hand, limiting the processing of personal data only in India will hamper free and fair digital economy. This reasoning to my mind is also fair, transparent and reasonable. In present day and age of google drives and cloud computing, demarcating national borders and limiting processing services of data only within India may not be feasible, efficient or even beneficial to the nation and its data subjects. Productivity and leverages of economies of scale and security both could be compromised until robust framework of laws and technical infrastructure forms a basis of a reliable support system.

[18] Mutual Legal Assistance Treaty signed by India with other country to request legal assistance for law enforcement purposes

CHAPTER 4

SUGGESTED AMENDMENTS TO EXTANT INDIAN LAWS & NON-CONSENSUAL PROCESSING

4.1 ALLIED LAWS

The Committee identified a list of 50 statutes and regulations which may overlap with the data protection framework. It identifies three Acts which require simultaneous amendments with the data protection framework. Firstly, the Aadhar Act was suggested to be amended to ensure privacy protections and autonomy of the UIDAI, secondly, the RTI Act prescribes exemption to transparency requirements under Section 8(1)(j). Many RTI requests have been denied based on this exemption which need to be aligned with the data protection framework. Thirdly, the data protection statute replaces Section 43A of the IT Act and the rules framed thereunder[1]. This provision may be repealed with other

[1] IT (Reasonable Security practices and procedures and Sensitive personal Data Protection Rules), 2011('SPD rules')

minor amendments. The Committee was of the view that in case of any inconsistency between the data protection law and the extant legislation, the data protection law will have overriding effect.

As regards Aadhar, the Committee suggested some amendments to strengthen the privacy rights to the individual and it was proposed that the entities could be divided into two categories: (1) those who can request for authentication and (2) those who are limited to verifying the identity of individuals offline. In the first category fall those entities which perform a public function and require verifiable identification in order to perform its public function. In the same manner as the Parliament can ask for authentication of an individual when it feels it is necessary, a public authority performing a public function which is approved by UIDAI can also seek authentication. The UIDAI can classify entities which seek Aadhar number and those which can only access the virtual ID which is a sixteen digits random number. In case of authentication failure for bonafide reasons such as disability of technical failure, offline verification should be made available. The Committee was of the view that in order to make Aadhar mandatory for several benefits and subsidies the UIDAI must be autonomous in its functioning independent of the user agencies in the government which make use of Aadhar. Secondly, the UIDAI should be equipped with the powers like a traditional regulator to carry out effective enforcement. It should also have consumer protection and

redressal of privacy breaches and be empowered to issue directions and cease and desist orders to state and private contractors discharging the function under the Aadhar Act. The Committee was also of the view that the RTI Act must provide for circumstances in which disclosure of personal information will be proportionate restriction on privacy as RTI Act promotes transparency and accountability in public administration. It took the view that in addition to likelihood of harm disclosures should be restricted only where the likely harm outweighs the common good of transparency in the functioning of Public Authorities. With the Supreme Court of India verdict on the Aadhar Act 's constitutionality, the legal regime for Aadhar has become clearer. Banks and private institutions are not entitled to seek Aadhar details anymore for authentication purposes. A citizen can choose and grant his consent to sharing Aadhar details, and it is mandatory only to claim certain government subsidies.

4.2 Non-consensual processing:

In Chapter 8 of the report the Committee on data protection dealt with the aspect of non-consensual processing. The Committee elucidates the circumstances where the consent is either not appropriate, necessary or relevant for processing. In the *Putta Swamy Judgment*, the Hon'ble Justice Chandrachud identified 4 legitimate state interests in the context of privacy. These were 'national security', 'prevention and investigation

of crime', 'protection of revenue' and 'allocation of resources for human development' out of which the first three are state functions and the fourth pertains to allocation of resources with the objective of preventing wastage of public resources. In the view of the Committee two other interests are equally important namely; ensuring compliance with judicial order. It dealt with two categories of processing; one grounds other than consent for processing and number two exemptions from the law. Such framework has also been adopted by the EUGDPR. The Committee while discussing non-consensual processing for public functions relied on the observations made by the Supreme Court in *Putty Swamy case*.[2]

> '*In a social welfare state, the government embarks upon programmes which provide benefits to impoverished and marginalised sections of society. There is a vital state interest in ensuring that scarce public resources are not dissipated by the diversion of resources to persons who do not qualify as recipients. Allocation of resources for human development is coupled with a legitimate concern that the utilisation of resources should not be siphoned away for extraneous purposes. Data mining with the object of ensuring that resources are properly deployed to legitimate beneficiaries is a valid ground for the state to insist on the collection of authentic data. But the data which the state has collected has to be utilised for legitimate purposes of the state and ought not to be utilised unauthorisedly for extraneous purposes. This will ensure that the legitimate concerns of the*

[2] Putty Swamy, 2017(10) SCALE 1 AT PARA 181

state are duly safeguarded while, at the same time, protecting privacy concerns. Prevention and investigation of crime and protection of the revenue are among the legitimate aims of the state. Digital platforms are a vital tool of ensuring good governance in a social welfare state. Information technology – legitimately deployed is a powerful enabler in the spread of innovation and knowledge.'

The Committee observed that the personal data should be collected only to the extent necessary for the provision of any subsidies or services and that the state should be allowed to collect personal data to the extent necessary to perform its regulatory functions. Such functions would include issuance of licenses by the government agencies. The Committee made a clear observation that while processing personal data the state should not be collecting personal data more than is necessary to achieve its legitimate purpose. The processing of sensitive personal data can be permitted only if it has been expressly mandated under any law made by the Parliament or Legislature of any state or by an order passed by a court in India. Further, the Committee noted that to process data such as health data may be in an emergency health situation where seeking consent before processing would be onerous or impossible. Number of countries have recognised the processing which is necessary for humanitarian emergencies including protection of data principal's life or health.[3] The Committee recommended

[3] Article 6(d) of EUGDPR, Article 9(2)(c) r/w recital 112, EUGDPR the UK Data Protection Bill has a provision similar to EUGDPR

that the welfare functions of the state should be recognised as a separate ground for processing. However, only bodies covered under Article 12 of the Constitution can rely on this ground.[4] Further, compliance with law or orders of court will be restricted to Indian Laws and Indian Codes. Obligations arising out of a contract, foreign law and foreign court orders shall not be permitted to be processed under this ground.[5] In case where prompt action is required a separate ground for processing will be available but subject to strict interpretation in cases where individual is not able to provide consent and processing is necessary to meet an emergency.[6] Another ground for non-consensual processing recognised by the Committee for employment purposes. This ground will be available where processing with consent will involve disproportionate effort or where employment relation makes consent inappropriate and will permit processing where employment related activities are not authorised under any other grounds of processing like compliance with law.[7] Reasonable purpose was recognized as a residuary ground for processing activities which are not covered by other grounds like consent, compliance with law, prompt action, public function but are nevertheless useful to society. This provision will cover those purposes which are white listed by the data protection authority to guide the data fiduciary.[8]

[4] Section 13, 19 of the bill
[5] Section 4,20 of the bill
[6] Section 15 and 21 of the bill
[7] Section 16 of the bill
[8] Section 17 of the bill

4.3 Exemptions to processing of personal data:

The Committee has recommended few exemptions to the processing of personal or sensitive personal data such as when it concerns security of a state and have suggested that the Central Government should enact a law for oversight of intelligence gathering activities.[9] According to the Committee, the prevention, detection, investigation and prosecution of contravention of law should also be one of the exemptions to processing of personal data which would however be exercised in accordance with law.[10] Thirdly, disclosures made for the purposes of legal proceedings would be exempt from the application of data protection law.[11] In the view of the Committee, the research exemption is also available but not as a blanket exemption. Those obligations which are necessary to fulfil the object of research will be exempted by the Data Protection Authority.[12] The Committee recommends a carefully tailored exemption for purely personal or domestic processing of data which would provide a blanket exemption from the application of Data Protection Law.[13] The Committee also recommended certain journalistic activities should also be exempted to maintain a balance between

[9] Section 42 of the bill
[10] Section 43 of the bill
[11] Section 44 of the bill
[12] Section 45 of the bill
[13] Section 46 of the bill

freedom of expression and right to informational privacy. The Data Protection Law should provide a clear definition of these journalistic purposes and the ethical standards for the same.[14] Another exemption proposed by the Committee is in case of manual processing by small entities. Such processing is exempted which is unlikely to cause significant harm and would have significant burdens from the obligations outlined under the Data Protection Law.

Citing various examples where the law enforcement should be exempt from the obligations related to notice, consent, use and disclosure the Committee explained that seeking consent of an individual before conducting search and seizure under Income Tax Act to determine if there has been a tax evasion can destroy the objective of conducting a raid. One of the interesting questions that the Committee considered was what is meant by personal. According to the court of justice of EU's decision in *Bodil Lindqvist*[15] if a personal data circulated on the internet is accessible to indefinite number of people then such dissemination will not qualify as personal or domestic processing as the purpose stops does not remain purely personal. The important factor is whether the views expressed by a person have any commercial nexus or are purely for personal reason which depends on the facts of every case. For example, a blogger writing a blog post cannot be considered purely personal where it may have some commercial aspects too considering the frequency

[14] Section 47 of the bill
[15] Case No.C-101/01

and scale at which the content is disseminated. As regards journalistic exemptions the Supreme Court of India in the case of *R. Rajagopal Versus State of Tamil Nadu*[16] held that the citizens have the right to protect privacy and the publication of personal information without consent irrespective of the nature of content may violate the privacy of the person. The Committee considered the journalistic exemption will balance out freedom of speech and right to privacy and where there is overriding public interest. The public interest may be upheld where disclosure of personal data is overriding. In *R. K. Jain Versus Union of India*[17], the Supreme Court considered the factors that could determine the public interest such as where the contents of documents are relied upon and interests are affected, the seriousness of issues with regard to which production is sought, likelihood of injustice if documents are not produced etc.

[16] R. Rajagopal Versus State of Tamil Nadu 194(6) SCC 632
[17] **1993 AIR 1769**

CHAPTER 5

RECOMMENDATIONS-LAW ENFORCEMENT

The Committee was of the view that legal enforcement for violation of data protection requires a Data Protection Authority which has the necessary powers to invoke compliance and enforce the data protection laws. In chapter 9, the Committee sets out the framework by proposing the structure, functions of the regulator and the tools used for regulation. Secondly, the classification of data fiduciary which will be regulated and the remedies available in case of violations. The Committee recommended that the Data Protection Law will establish Data Protection Authority as an Independent Regulatory Body to enforce and implement the law.

The Data Protection Authority's primary function will be: *(i) monitoring and enforcement; (ii) legal affairs, policy and standard setting; (iii) research and awareness; (vi) enquiry, grievance handling and adjudication*[1]. The DPA will have the power to categorise certain fiduciaries as significant data fiduciaries based on their

[1] Chapter X of the bill

ability to cause greater harm to data principles as a result of their processing activities. Such categorisation would be based on multiple factors such as assessment of volume of personal data being processed, type of personal data, type of processing activity, turn over of data fiduciary, risk of harm and the type of technology used to undertake processing.[2] The Committee further recommended that the significant fiduciary shall register with the DPA and carry out impact assessments, undertake record keeping and data audits and appointment of data protection officer. The DPA is in power to and has a discretion to require other data fiduciaries to comply with this obligations.[3] In order to ensure compliance enforcement tools shall be made available to the Data Protection Authority including the power to issue directions, power to call for information, publication of guidance, issuance of public statements, code of practice, conducting enquiry, injunctive relief, inter sectoral coordination.[4] Since the DPA would be empowered to carry out enquiries, it is proposed to wide powers including issuing warnings, reprimands, ordering data fiduciaries to seize and desist, modify or temporarily suspend businesses who violate the law.[5] It is envisaged that the DPA will have an Adjudication Bill to hear and decide the complaints between data principal and data fiduciaries.[6] After data fiduciaries the Central Government would establish an

[2] Section 38 of the bill
[3] Section 33,34,35,36,38 of the bill
[4] Chapter X of the bill
[5] Section 66 of the bill
[6] Section 68 of the bill

Appellate Tribunal or confer powers on any existing Appellate Tribunal to hear and decide appeals against an order of the Data Protection Authority. Appeals against the order of the Appellate Tribunal will be filed before the Supreme Court of India.[7] The Committee has recommended imposition of penalty and grand of compensation to Data Principals in case of breach of personal data. The penalty would have a fixed upper limit or percentage of total world wide turn over of the preceding financial year which ever is higher. This provision is also reflected in the GDPR which imposes penalties of Euro 20000 million or 4% of the global annual turn over of the company. The offences under the law were suggested should cover only intentional or reckless behaviour or damage caused with the knowledge to the concerned data principal.[8] The Committee suggested the Data Protection Authority shall be a body corporate having perpetual succession and a common seal with power to acquire, hold or dispose of property and have the capacity to contract, to sue or be sued. It would be a single institution with appropriate regional offices to fulfil its statutory functions. It is proposed to be governed by a board consisting of six whole time members and a chair person appointed by the Central Government on recommendation of Selection Committee comprising of the Chief Justice of India or her nominee who is a judge of the Supreme Court of India, the Cabinet Secretary Government of India and one Expert of repute with knowledge special knowledge of and professional

[7] Section 84,87 of the bill

[8] Sections 69,70,71,72,73,75 and Chapter XIII of the Bill

experience in Data Protection, Information Technology, Data Management, Data Science, Cyber and related areas. Similar provisions exists in Section 9 of the Competition Act, Section 4 Sub clause 4 of the SEBI Act, Section 4, TRAI Act, Section 3 of IRDA Act the members of DPA shall have a fixed term of five years subject to appropriate retirement age. It is also proposed that the members of the DPA shall not accept employment under Central or State Government or under significant data fiduciary in the course of their tenure or for a period of two years thereafter. It is also proposed that the Adjudication Wing would function at arm's length from the remaining wings of the Data Protection Authority which deal with legislative and executive enforcement. The Committee has proposed joint and several liability to pay compensation for a data fiduciary and its processors. The factors to decide quantum of compensation is similar to the factors under penalties, inter alia, nature and duration and extent of non-compliance, extent and nature of harm suffered by the data principal due to the default, intentional character of violation, the transparency adopted by the data fiduciary in its data processing activity, any mitigation efforts, unfair advantage to the data fiduciary, repetitive nature of default, nature of personal data involved etc. As regards the offences the Committee was of the view that this should be linked to any intentional or reckless behaviour or to damage caused with knowledge to the data principal. For example, obtaining transfer, disclosure and sale of personal and sensitive data in breach of the data protection law which

harms the data principal and re-identification processing of previously de-identified personal data. The Committee proposes such offences shall be made cognizable and non-bail able and may be tried by relevant jurisdictional court. In case of offences committed by a company, the person in-charge of the conduct of the business of the company and in case of offence by a Government Department the head of the department should be liable unless they can prove that such offence was committed without his consent or they took reasonable measures to prevent commission of such offence.

CONCLUSIONS

Justice Srikrishna Committee report has made many valuable recommendations to carve out the personal data and privacy law of India. The Personal data protection bill will be discussed in the parliament before it becomes a law. While there are certain recommendations which were widely accepted by common man such as purpose limitation, storage limitation, there were others such as need to localise all data within India and restrictions on its transfer to foreign countries that met with resistance. This would entail spending huge sums of money by foreign entities who serve Indian users such as facebook or WhatsApp. Security experts have also expressed concerns over the current security regime in the country. I do endorse as these concerns are genuine. There should be better security paradigms and robust security before data localisation is introduced in India. Certain groups have resisted the

independence of Adjudicating authority while others have opposed the broad permissions available to the government to seek personal data of its citizens. Whereas the bill would improve accountability and transparency in collection and processing of personal data , it is being questioned if the adjudicating authority would remain autonomous. Section 98 of the bill not only states that the Central government can issue directions to the authority, but also that the authority shall be bound by directions on questions of policy in which the decision of the Central government is final[9]. Setting clear parameters for exercise of independent discretion based on sound legal grounds & transparency can alone balance competing paradigms. Any scope of arbitrariness in discretion in exercise of powers or rather division of powers can render such provision unconstitutional.

In many ways, the proposed law is similar to the General Data protection Directive of the European Union. India has proposed that any company that fails to comply with the law will be fined Rs5 crore ($727,450) or 2% of its turnover, whichever is higher. The severity of this punishment is similar to that of the GDPR, which fines companies €20 million ($23 million) or 4% of turnover. However, there are several differences, too. For instance, it does not allow Indians to compel companies complete erasure of data they may have shared, which is commonly found in the EU. The "right to

[9] Ananya Bhattacharya, India's first data protection bill is riddled with problems, Quartz India, 30 July 2918, https://qz.com/india/1343154/justice-srikrishnas-data-protection-bill-for-india-is-full-of-holes/

be forgotten" suggested in the bill only allows individuals to restrict companies from using their data but does not confer a right on them to ask for its erasure from their storage.

Thus, there are mixed views regarding various recommendations made by the data protection Committee. These will of course have to be tested on the anvil of law and reasonableness till it crystallises into a transparent and fair law in due course of time!

Notes:

1 Roe versus Wade 410 US 113 (1973), Griswold Versus Connecticut 381 US 479 (1965)

2 Sections 5 and 6 of the Bill.

THE PERSONAL DATA PROTECTION BILL, 2018

WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data as an essential facet of informational privacy;

WHEREAS the growth of the digital economy has meant the use of data as a critical means of communication between persons;

WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation;

AND WHEREAS it is expedient to make provision: toprotect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data, to specify the rights of individuals whose personal data are processed, to create a framework for implementing organisational and technical measures in processing personal data, to lay down norms for cross-border transfer of personal data, to ensure the accountability of entities processing personal data, to provide remedies for unauthorised and harmful processing, and to establish a Data Protection Authority for overseeing processing activities;

BE IT ENACTED by Parliament in the Sixty-Ninth Year of the Republic of India as follows:–

CHAPTER I

PRELIMINARY

1. Short title, extentand commencement.–

(1) This Act may be called the Personal Data Protection Act, 2018.

(2) It extends to the whole of India.

(3) The provisions of Chapter XIV of this Act shall come into force on such date, as the Central Government may by notification appointand the remaining provisions of the Act shall come into force in accordance with the provisions in that Chapter.

2. Application of the Act to processing of personal data.–

(1) This Act applies to the following –

(a) processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and

(b) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.

(2). Notwithstanding anything contained insub-section (1), the Act shall apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, only if such processing is –

(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or

(b) in connection with any activity which involves profiling of data principals within the territory of India.

(3) Notwithstanding anything contained in sub-sections (1) and (2), the Act shall not apply to processing of anonymised data.

3. Definitions.—In this Act, unless the context otherwise requires,–

(1) **"Aadhaar number"**shall have the meaning assigned to it under clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016);

(2) **"Adjudicating Officer"** means an officer of the adjudication wing under section 68;

(3) **"Anonymisation"**in relation to personal data, means the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, meeting the standards specified by the Authority.

(4) "**Anonymised data**" means data which has undergone the process of anonymisation under sub-clause (3) of this section;

(5) **"Appellate Tribunal"**means the tribunal notified under Chapter XIIof this Act;

(6) **"Authority"** means the Data Protection Authority of India established under Chapter X of this Act;

(7) **"Automated means"** means any equipment capable of operating automatically in response to instructions given for the purpose of processing data;

(8) **"Biometric data"**means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioural

characteristics of a data principal, which allow or confirm the unique identification of that natural person;

(9) **"Child"** means a data principal below the age of eighteen years;

(10) **"Code of Practice"** means a code of practice issued by the Authority under section 61;

(11) **"Consent"** means consent under section 12;

(12) **"Data"**means and includes a representation of information, facts, concepts, opinions, or instructions in a manner suitable for communication, interpretation, or processing by humans or by automated means;

(13) **"Data fiduciary"** means any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;

(14) **"Data principal"** means the natural person to whom the personal data referred to in sub-clause (28) relates;

(15) **"Data processor"** means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary;

(16) **"De-identification"** meansthe process by which a data fiduciary or data processor may remove, or mask identifiers from personal data, or replace them with such other fictitious name or code that is unique to an individual but does not, on its own, directly identify the data principal;

(17) **"Disaster"** shall have the same meaning assigned to it underclause (d) of section 2 of the Disaster Management Act, 2005 (53 of 2005);

(18) **"Explicit consent"** means consent under section 18;

(19) **"Financial data"** means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the

relationship between a financial institution and a data principal including financial status and credit history;

(20) **"Genetic data"** means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the behavioural characteristics, physiology or the health of that natural person and which result,in particular, from an analysis of a biological sample from the natural person in question;

(21) **"Harm"** includes –

(i) bodily or mental injury;
(ii) loss, distortion or theft of identity;
(iii) financial loss or loss of property,
(iv) loss of reputation, or humiliation;
(v) loss of employment;
(vi) any discriminatory treatment;
(vii) any subjection to blackmail or extortion;
(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;
(ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or
(x) any observation or surveillance that is not reasonably expected by the data principal.

(22) **"Health data"** means data related to the state of physical or mental health of the data principal and includes records regarding the past, present or future state of the health of such data principal, data collected in the course of registration for, or provision of health services, data associating the data principal to the provision of specific health services.

(23) **"Intersex status"** means the condition of a data principal who is –

(i) a combination of female or male;
(ii) neither wholly female nor wholly male; or
(iii) neither female nor male.

(24) **"Intra-group schemes"** means schemes approved by the Authority under section 41;

(25) **"Journalistic purpose"** means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding –

(i) news, recent or current events; or
(ii) any other information which the data fiduciary believes the public, or any significantly discernible class of the public, to have an interest in;

(26) **"Notification"** means a notification published in the Official Gazette and the term "notify" shall be construed accordingly; –

(27) **"Official identifier"** means any number, code, or other identifier, including Aadhaar number, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal;

(28) **"Person"**means –

(i) an individual,
(ii) a Hindu undivided family,
(iii) a company,
(iv) a firm,
(v) an association of persons or a body of individuals, whether incorporated or not,
(vi) the State, and

(vii) every artificial juridical person, not falling within any of the preceding sub-clauses;

(29) **"Personal data"**means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information;

(30) **"Personal data breach"** means any unauthorised or accidental disclosure, acquisition, sharing, use, alteration, destruction, loss of access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;

(31) **"Prescribed"**means prescribed by rules made by the Central Government under this Act;

(32) **"Processing"**in relation to personal data, means an operation or set of operations performed on personal data, and may include operations such as collection, recording,organisation, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination or otherwise making available, restriction, erasure or destruction;

(33) **"Profiling"**means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interest of a data principal;

(32) **"Re-identification"**meansthe process by which a data fiduciary or data processor may reverse a process of de-identification;

(35) **"Sensitive Personal Data"** means personal data revealing, related to, or constituting, as may be applicable

(i) passwords;
(ii) financial data;
(iii) health data;

(iv) official identifier;
(v) sex life;
(vi) sexual orientation;
(vii) biometric data;
(viii) genetic data;
(ix) transgender status;
(x) intersex status;
(xi) caste or tribe;
(xii) religiousor political belief or affiliation; or
(xiii) any other category of data specified by the Authority under section 22.

(36) **"Significant data fiduciary"**means a data fiduciary notified by the Authority under section 38;

(37) **"Significant harm"**means harm that has an aggravated effect having regard to the nature of the personal data being processed,the impact, continuity, persistence or irreversibility of the harm;

(38) **"Specified"** means specified by regulations made by the Authority under this Act and the term "specify" shall be construed accordingly;

(39) **"State"** shall, unless the context otherwise requires, have the same meaning assigned to itunder Article 12 of the Constitution;

(40) **"Systematic activity"** means any structured or organised activity that involves an element of planning, method, continuity or persistence;

(41) **"Transgender status"**means the condition of a data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any other similar medical procedure.

CHAPTER II

DATA PROTECTION OBLIGATIONS

4. Fair and reasonable processing.—Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal.

5. Purpose limitation.–

(1) Personal data shall be processed only for purposes that are clear, specific and lawful.

(2) Personal data shall be processed only for purposes specified or for any other incidental purpose that the data principal would reasonably expect the personal data to be used for, having regard to the specified purposes, and the context and circumstances in which the personal data was collected.

6. Collection limitation. —Collection of personal data shall be limited to such data that is necessary for the purposes of processing.

7. Lawful processing. –

(1) Personal data shall be processed only on the basis of one or a combination of grounds of processing in Chapter III.

(2) Sensitive personal data shall be processed only on the basis of one or a combination of grounds of processing in Chapter IV.

8. Notice. –

(1) Thedata fiduciary shall provide the data principal with the following information, no later than at the time

of collection of the personal data or, if the data is not collected from the data principal, as soon as is reasonably practicable –

(a) the purposes for which the personal data is to be processed;
(b) the categories of personal data being collected;
(c) the identity and contact details of the data fiduciary and the contact details of the data protection officer, if applicable;
(d) the right of the data principal to withdraw such consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;
(e) the basis for such processing, and the consequences of the failure to provide such personal data, if the processing of the personal data is based on the grounds in section 12 to section 17, and section 18 to section 22;
(f) the source of such collection, if the personal data is not collected from the data principal;
(g) theindividuals or entities including other data fiduzciaries or data processors, with whom such personal data may be shared, if applicable;
(h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
(i) the period for which the personal data will be retained in terms of section 10 or where such period is not known, the criteria for determining such period;
(j) the existence of and procedure for the exercise of data principal rights mentioned in Chapter VI and any related contact details for the same;

(k) the procedure for grievance redressal under section 39;
(l) the existence of a right to file complaints to the Authority;
(m) where applicable, any rating in the form of a data trust score that may be assignedto the data fiduciary under section 35; and
(n) any other information as may be specified by the Authority.

(2) Thedata fiduciary shall provide the information as required under this section to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.
(3) Sub-section (1) shall not apply where the provision of notice under this section would substantially prejudice the purpose of processing of personal data under sections15or 21of this Act.

9. Data quality.–

(1) Thedata fiduciary shall take reasonable steps to ensure that personal data processed is complete, accurate, not misleading and updated, having regard to the purposes for which it is processed.
(2) In considering whether any reasonable step is necessaryunder sub-section (1), the data fiduciary shall have regard to whether the personal data –

(a) is likely to be used to make a decision about the data principal;
(b) is likely to be disclosed to other individuals or entities including other data fiduciaries or processors; or
(c) is kept in a form that distinguishes personal data based on facts from personal data based on opinions or personal assessments.

(3) Where personal data is disclosed to other individuals or entities, including other data fiduciaries or processors, and the data fiduciary subsequently finds that such data does not comply with sub-section (1), the data fiduciary shall take reasonable steps to notify suchindividuals or entities of thisfact.

10. Data storage limitation. –

(1) Thedata fiduciary shall retain personal data only as long as may be reasonably necessary to satisfy the purpose for which it is processed.

(2) Notwithstanding sub-section (1), personal data may be retained for a longer period of time if such retention is explicitly mandated, or necessary to comply with any obligation, under a law.

(3) The data fiduciary must undertake periodic review in order to determine whether it is necessary to retain the personal data in its possession.

(4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-sections (1) and (2), then such personal data must be deleted in a manner as may be specified.

11. Accountability. –

(1) The data fiduciary shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf.

(2) The data fiduciary should be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA

12. Processing of personal data on the basis of consent. –

(1) Personal data may be processed on the basis of the consent of the data principal, given no later than at the commencement of the processing.

(2) For the consent of the data principal to be valid, it must be

(a) free, having regard to whether it meets the standard under section 14 of the Indian Contract Act, 1872 (9 of 1872);

(b) informed, having regard to whether the data principal has been provided with the information required under section 8;

(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purposes of processing;

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and

(e) capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

(3) The data fiduciary shall not make the provision of any goods or services or the quality thereof, the performance of any contract, or the enjoyment of any legal right or claim, conditional on consent to processing of any personal data not necessary for that purpose.

(4) The data fiduciaryshall bear the burden of proof to establish that consent has been given by the data principal for processing of personal data in accordance with sub-section (2).

(5) Where the data principal withdraws consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, all legal consequences for the effects of such withdrawal shall be borne by the data principal.

13. Processing of personal data for functions of the State. –

(1) Personal data may be processed if such processing is necessary for any function of Parliament or any State Legislature.

(2) Personal data may be processed if such processing isnecessary forthe exercise of any function of the State authorised by law for:

(a) the provision of any service or benefit to the data principal from the State; or

(b) the issuance of any certification, license or permit for any action or activity of the data principal by the State.

14. Processing of personal data in compliance with law or any order of any court or tribunal. –

Personal data may be processed if such processing is –

(a) explicitly mandated under any law made by Parliament or any State Legislature; or

(b) for compliance with any order or judgment of any Court or Tribunal in India.

15. Processing of personal data necessary for prompt action. –

Personal data may be processed if such processing is necessary –

(a) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal or any other individual;
(b) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or
(c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

16. Processing of personal data necessary for purposes related to employment.

(1) Personal data may be processed if such processing is necessary for

(a) recruitmentor termination of employment of a data principal by the data fiduciary;
(b) provision of any service to, or benefit sought by,the data principal who is an employee of the data fiduciary;
(c) verifying the attendance of the data principal who is an employee of the data fiduciary; or
(d) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.

(2) Sub-section (1) shall apply only where processing on the basis of consent of the data principal is not appropriate

having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing activities under this section.

17. Processing of data for reasonable purposes. –

(1) In addition to the grounds for processing contained in section12 to section 16, personal data may be processed if such processing is necessary for such reasonable purposes as may be specified after taking into consideration –

(a) the interest of the data fiduciary in processing for that purpose;
(b) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;
(c) any public interest in processing for that purpose;
(d) the effect of the processing activity on the rights of the data principal; and
(e) the reasonable expectations of the data principal having regard to the context of the processing.

(2) For the purpose of sub-section (1), the Authority may specify reasonable purposes related to the following activities, including

(a) prevention and detection of any unlawful activity including fraud;
(b) whistle blowing;
(c) mergers and acquisitions;
(d) network and information security;
(e) credit scoring;
(f) recovery of debt;
(g) processing of publicly available personal data;

(3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall:

(a) lay down such safeguards as may be appropriate to ensure the protection of the rights of data principals; and

(b) determine where the provision of notice under section 8 would not apply having regard to whether such provision would substantially prejudice the relevant reasonable purpose.

CHAPTER IV

GROUNDS FOR PROCESSING OF SENSITIVE PERSONAL DATA

18. Processing of sensitive personal data based on explicit consent.–

(1) Sensitive personal data may be processed on the basis of explicit consent.

(2) For the purposes of sub-section (1), consent shall be considered explicit only if it isvalid as per section 12 and is additionally:

(a) informed, having regard to whether the attention of the data principal has been drawn to purposes ofor operations in processing that may have significant consequences for the data principal;

(b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and

(c) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different

categories of sensitive personal data relevant to processing.

19. Processing of sensitive personal data for certain functions of the State. – Sensitive

personal data may be processed if such processing is strictly necessary for:

(a) any function of Parliament or any State Legislature.
(b) the exercise of any function of the State authorised by law forthe provision of any service or benefit to the data principal.

20. Processing of sensitive personal data in compliance with law or any order of any court or tribunal.

Sensitive personal data may be processed if such processing is –

(a) explicitly mandated under any law made by Parliament or any State Legislature; or
(b) necessaryfor compliance with any order or judgment of any Court or Tribunal in India.

21. Processing of certain categories of sensitive personal data for prompt action.

Passwords,financial data, health data, official identifiers, genetic data, and biometric data may be processed where such processing is strictly necessary –

(a) to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal;
(b) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health; or

(c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order.

22. Further categories of sensitive personal data. –

(1) Such further categories of personal data as may be specified by the Authority shall be sensitive personal data and, where such categories of personal data have been specified, the Authority may also specify any further grounds on which such specified categories of personal data may be processed.

(2) The Authority shall specify categories of personal data under sub-section (1) having regard to –

(a) theriskof significant harm that may be caused to the data principal by the processing of such category of personal data;

(b) the expectation of confidentiality attached to such category of personal data;

(c) whether a significantly discernible class of data principals may suffer significant harm from the processing of such category of personal data; and

(d) the adequacy of protection afforded by ordinary provisions applicable to personal data.

(3) The Authority may also specify categories of personal data, which require additional safeguards or restrictions where repeated, continuous or systematic collection for the purposes of profiling takes place and, where such categories of personal data have been specified, the Authority may also specify such additional safeguards or restrictions applicable to such processing.

CHAPTER V

PERSONAL AND SENSITIVE PERSONAL DATA OF CHILDREN

23. Processing of personal data and sensitive personal data of children. –

(1) Every data fiduciary shall process personal data of children in a manner that protects and advances the rights and best interests of the child.

(2) Appropriate mechanisms for age verification and parental consent shall be incorporated by data fiduciaries in order to process personal data of children.

(3) Appropriateness of an age verification mechanism incorporated by a data fiduciary shall be determined on the basis of –

(a) volume of personal data processed;
(b) proportion of such personal data likely to be that of children;
(c) possibility of harm to children arising out of processing of personal data; and
(d) such other factors as may be specified by the Authority.

(4) The Authority shall notify the following as guardian data fiduciaries –

(a) data fiduciaries who operate commercial websites or online services directed at children; or
(b) data fiduciaries who process large volumes of personal data of children.

(5) Guardian data fiduciaries shall be barred from profiling, tracking, or behavioural monitoring of, or targeted

advertising directed at, children and undertaking any other processing of personal data that can cause significant harm to the child.

(6) Sub-section (5) may apply in such modified form, to data fiduciaries offering counseling or child protection services to a child, as the Authority may specify.

(7) Where a guardian data fiduciary notified under sub-section (4)exclusively provides counseling or child protection services to a child, as under sub-section (6), then such guardian data fiduciary will not be required to obtain parental consent as set out under sub-section (2).

CHAPTER VI

DATA PRINCIPAL RIGHTS

24. Right to confirmation and access. –

(1) The data principal shall have the right to obtain from the data fiduciary –

(a) confirmation whether the data fiduciary is processing or has processed personal data of the data principal;

(b) a brief summary ofthe personal data of the data principal being processed or that has been processed by the data fiduciary;

(c) abrief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 8 in relation to such processing activities.

(2) The data fiduciary shall provide the information as required under this section to the data principal in a

clear and concise manner that is easily comprehensible to a reasonable person.

25. Right to correction, etc.

(1) Where necessary, having regard to the purposes for which personal data is being processed, the data principal shall have the right to obtain from the data fiduciary processing personal data of the data principal –

(a) the correction of inaccurate or misleading personal data;
(b) the completion of incomplete personal data; and
(c) the updating of personal data that is out of date.

(2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with the need for such correction, completion or updatinghaving regard to the purposes of processing, the data fiduciary shall provide the data principal with adequate justificationin writing for rejecting the application.

(3) Where the data principal is not satisfied with thejustification provided by the data fiduciary under sub-section (2), the data principalmay require that the data fiduciary take reasonable steps to indicate,alongside the relevant personal data, that the same is disputed by the data principal.

(4) Where the data fiduciary corrects, completes, or updates personal data in accordance with sub-section (1), the data fiduciary shall also take reasonable steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion or updating, particularly where such action would have an impact on the rights and interests of the data principal or on decisions made regarding them.

26. Right to Data Portability. –

(1) The data principal shall have the right to –

(a) receivethe following personal data related to the data principal in a structured, commonly used and machine-readable format –

(i) whichsuch data principal has provided to the data fiduciary;

(ii) which has been generated in the course of provision of services or use of goods by the data fiduciary;or

(iii) which forms part of any profile on the data principal, or which the data fiduciaryhas otherwise obtained.

(b) have the personal data referred to in clause (a) transferred to any other data fiduciary in the format referred to in that clause.

(2) Sub-section (1) shall only apply where the processing has been carried out through automated means, and shall not apply where –

(a) processing is necessary for functions of the State undersection 13;

(b) processing is in compliance of law as referred to in section 14; or

(c) compliance with the request in sub-section (1) would reveal a trade secret of any data fiduciaryor would not be technically feasible.

27. Right to Be Forgotten. –

(1) The data principal shall have the right to restrict or prevent continuing disclosure of personal data by a data fiduciaryrelated to the data principalwhere such disclosure –

(a) has served the purpose for which it was made or is no longer necessary;
(b) was made on the basis of consent under section 12 and such consent has since been withdrawn;or
(c) was made contrary to the provisions of this Act or any other law made by Parliament or any State Legislature.

(2) Sub-section (1) shall only apply where the Adjudicating Officer under section 68determines the applicability of clause (a), (b) or (c) of sub-section (1) and that the rights and interests of the data principal in preventing or restricting the continued disclosure of personal data override the right to freedom of speech and expression and the right to information of any citizen.

(3) In determining whether the condition in sub-section (2) is satisfied, the Adjudicating Officer shall have regard to –

(a) the sensitivity of the personal data;
(b) the scale of disclosure and the degree of accessibility sought to be restricted or prevented;
(c) the role of the data principal in public life;
(d) the relevance of the personal data to the public; and
(e) the nature of the disclosure and of the activities of the data fiduciary, particularly whether the data fiduciarysystematically facilitates access to personal data and whether the activities would be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

(4) The right under sub-section (1) shall be exercised by filing an application in such form and manner as may be prescribed.

(5) Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating Officerunder sub-section (2) does

not satisfy the conditions referred to in that sub-section any longer, they may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and such Adjudicating Officer shall review her order on the basis of the considerations referred to in sub-section (3).

28. General conditions for the exercise of rights in this Chapter. –

(1) The exercise of any right under this Chapter, except the right undersection 27,shall only be on the basis of a request made in writing to the data fiduciarywith reasonable information to satisfy the data fiduciaryof the identity of the data principal making the request and the data fiduciary shall acknowledge receipt of such request within such period of time as may be specified.

(2) Thedata fiduciary may chargea reasonable fee to be paid for complying with requests made under this Chapter, except for requestsmade under clauses (a) and (b) of sub-section (1) of section 24 and section 25 which shall be complied with by the data fiduciary without charging any fee.

(3) The Authority may specify a reasonable time period within which the data fiduciaryshall comply with the requests under this Chapter, and such time period shall be communicated to the data principal along with the acknowledgement referred to in sub-section (1).

(4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal making such request with adequate reasons for suchrefusal as per the provisions of this Chapter in writing,and shall inform the data principal regarding the right to file a complaint with the Authority against the refusal within such period and in such manner as may be specified.

(5) The data fiduciary is not obliged to comply with any request made under this Chapter where such compliance would harm the rights of any other data principal under this Act.

(6) The manner of exercise of rights under this Chapter shall be in such form as may be provided by law or in the absence of such law, in a reasonable format to be followed by each data fiduciary.

CHAPTER VII

TRANSPARENCY AND ACCOUNTABILITY MEASURES

29. Privacy by Design. –

Every data fiduciary shall implement policies and measures to ensure that –

(a) managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data principal;

(b) theobligations mentioned in Chapter II are embedded in organisational and business practices;

(c) technology used in the processing of personal data is in accordance with commercially accepted or certified standards;

(d) legitimate interests of businesses including any innovation is achieved without compromising privacy interests;

(e) privacy is protected throughout processing from the point of collection to deletion of personal data;

(f) processing of personal data is carried out in a transparent manner; and

(g) the interest of the data principal is accounted for at every stage of processing of personal data.

30. Transparency. –

(1) The data fiduciary shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data and shall make the following information available in an easily accessible form as may be specified –

(a) the categories of personal data generally collected and the manner of such collection;
(b) the purposes for which personal data is generally processed;
(c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
(d) the existence of and procedure for the exercise of data principal rights mentioned in Chapter VI, and any related contact details for the same;
(e) the existence of a right to file complaints to the Authority;
(f) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under section 35;
(g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out;and
(h) any other information as may be specified by the Authority.

(2) The data fiduciary shall notify the data principal of important operations in the processing of personal data related to the data principal through periodic notifications in such manner as may be specified.

31. Security Safeguards. –

(1) Having regard to the nature, scope and purpose of processing personal data undertaken, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, the data fiduciaryand the data processor shall implement appropriate security safeguards including –

(a) use of methods such as de-identification and encryption;
(b) steps necessary to protect the integrity of personal data; and
(c) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(2) Every data fiduciary and data processor shall undertake a review of its security safeguards periodicallyas may be specified and may take appropriate measures accordingly.

32. Personal Data Breach. –

(1) The data fiduciary shall notify the Authority of any personal data breach relating to any personal data processed by the data fiduciarywhere such breach is likely to causeharm to any data principal.
(2) The notification referred to in sub-section (1) shall include the following particulars

(a) nature of personal data which is the subject matter of the breach;
(b) number of data principals affected by the breach;
(c) possible consequences of the breach; and
(d) measures being taken by the data fiduciary to remedy the breach.

(3) The notification referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and not later than the time period specified by the Authority, following the breach after accounting for any time that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

(4) Where it is not possible to provide all the information as set out in sub-section (2) at the same time, the data fiduciary shall provide such information to the Authority in phases without undue delay.

(5) Upon receipt of notification, the Authority shall determine whether such breach should be reported by the data fiduciary to the data principal, taking into account the severity of the harm that may be caused to such data principal or whether some action is required on the part of the data principal to mitigate such harm.

(6) The Authority, may in addition to requiring the data fiduciary to report the personal data breach to the data principal under sub-section (5), direct the data fiduciary to take appropriate remedial action as soon as possible andto conspicuously post the details of the personal data breach on its website.

(7) The Authority may, in addition, also post the details of the personal data breach on its own website.

33. Data Protection Impact Assessment. –

(1) Where the data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data principals, such processing shall not be commenced unless the data fiduciary has undertaken a data protection impact assessment in accordance with the provisions of this section.

(2) The Authority may, in addition, specify those circumstances, or classes of data fiduciaries, or processing operations where such data protection impact assessment shall be mandatory, and may also specify those instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment.

(3) A data protection impact assessment shall contain, at a minimum –

(a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;

(b) assessment of the potential harm that may be caused to the data principals whose personal data is proposed to be processed; and

(c) measures for managing, minimising, mitigating or removing such risk of harm.

(4) Upon completion of the data protection impact assessment, the data protection officer shall review the assessment prepared and shall submit the same to the Authorityin such manner as may be specified.

(5) On receipt of the assessment, if the Authority has reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processingor direct that such processing shall be subject to such conditions as may be issued by the Authority.

34. Record-Keeping. –

(1) The data fiduciary shall maintain accurate and up-to-date records of the following –

(a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 11;

(b) periodic review of security safeguards under section 31;
(c) dataprotection impact assessments under section 33; and
(d) any other aspect of processing as may be specified by the Authority.

(2) The records in sub-section (1) shall be maintained in such form as specified by the Authority.
(3) Notwithstanding anything contained in this Act, this section shall apply to the Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority which is "the State" under Article 12 of the Constitution.

35. Data Audits. –

(1) The data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.
(2) The data auditor will evaluate the compliance of the data fiduciary with the provisions of this Act, including –

(a) clarity and effectiveness of notices under section 8;
(b) effectiveness of measures adopted under section 29;
(c) transparency in relation to processing activities under section 30;
(d) security safeguards adopted pursuant to section 31;
(e) instances of personal data breach and response of the data fiduciary, including the promptness of notification to the Authority under section 32; and
(f) any other matter as may be specified.

(3) The Authority shall specify the form, manner and procedure for conducting audits under this section

including any civil penalties on data auditors for negligence.

(4) The Authority shall register persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, with such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may specify, as data auditors under this Act.

(5) A data auditor may assign a rating in the form of a data trust score to the data fiduciary pursuant to a data audit conducted under this section.

(6) The Authority shall specify the criteria for assigning a rating in the form of a data trust score having regard to the factors mentioned in sub-section (2).

(7) Notwithstanding sub-section (1) where the Authority is of the view that the data fiduciary is processing personal data in a manner that is likely to cause harm to a data principal, the Authority may order the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

36. Data Protection Officer. –

(1) The data fiduciary shall appoint a data protection officer for carrying out the following functions –

(a) providing information and advice to the data fiduciary on matters relating to fulfilling its obligations under this Act;

(b) monitoring personal data processing activities of the data fiduciary to ensure that such processing does not violate the provisions of this Act;

(c) providing advice to the data fiduciary where required on the manner in which data protection impact assessments must be carried out, and carry

out the review of such assessment as under sub-section (4) of section 33;

(d) providing advice to the data fiduciary, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under section 29;

(e) providing assistance to and cooperating with the Authority on matters of compliance of the data fiduciary with provisions under this Act;

(f) act as the point of contact for the data principal for the purpose of raising grievances to the data fiduciary pursuant to section 39 of this Act; and

(g) maintaining an inventory of all records maintained by the data fiduciary pursuant to section 34.

(2) Nothing shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary, in addition to the functions provided in sub-section (1) above.

(3) The data protection officer shall meet the eligibility and qualification requirements to carry out its functions under sub-section (1) as may be specified.

(4) Where any data fiduciary not present within the territory of India carries on processing to which the Act applies under section 2(2), and the data fiduciary is required to appoint a data protection officer under this Act, the data fiduciary shall appoint such officer who shall be basedin India and shall represent the data fiduciary in compliance of obligations under this Act.

37. Processing by entities other than data fiduciaries. –

(1) The data fiduciary shall only engage, appoint, use or involve a data processor to processpersonal data on its behalf through avalid contract.

(2) The data processor referred to in sub-section (1) shall not further engage, appoint, use, or involve another data processor in the relevant processing on its behalf except with the authorisation of the data fiduciary, unless permitted through the contract referred to in sub-section (1).

(3) The data processor, and any employee of the data fiduciary or the data processor, shall only process personal data in accordance with the instructions of the data fiduciary unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as confidential.

38. Classification of data fiduciaries as significant data fiduciaries. –

(1) The Authority shall, having regard to the following factors, notify certain data fiduciaries or classes of data fiduciaries as significant data fiduciaries –

(a) volume of personal data processed;
(b) sensitivity of personal data processed;
(c) turnover of the data fiduciary;
(d) risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary;
(e) use of new technologies for processing; and
(f) any other factor relevant in causing harm to any data principal as a consequence of such processing.

(2) The notification of a data fiduciary or classes of data fiduciaries as significant data fiduciaries by the Authority under sub-section (1) shall require such data fiduciary or class of data fiduciaries to register with the Authority in such manner as may be specified.

(3) All or any ofthe following obligations in this Chapter, as determined by the Authority, shall apply only to significant data fiduciaries –

(a) data protection impact assessments under section 33;
(b) record-keeping under section 34;
(c) data audits under section 35; and
(d) data protection officer under section 36.

(4). Notwithstanding sub-section (3), the Authority may notify the application of all or any of the obligations in sub-section (3) to such data fiduciary or class of data fiduciaries, not being a significant data fiduciary, if it is of the view that any processing activity undertaken by such data fiduciary or class of data fiduciaries carries a risk of significant harm to data principals.

39. Grievance Redressal. –

(1) Every data fiduciary shall have in place proper procedures and effective mechanisms to address grievances of data principals efficiently and in a speedy manner.

(2) A data principal may raise a grievance in case of a violation of any of the provisions of this Act, or rules prescribed, or regulations specified thereunder, which has caused or is likely to cause harm to such data principal, to –

(a) the data protection officer, in case of a significant data fiduciary; or
(b) an officer designated for this purpose, in case of any other data fiduciary.

(3) A grievance raised under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and no later than thirty days from the date of receipt of grievance by such data fiduciary.

(4) Where, a grievance under sub-section (2) is not resolved within the time period mentioned under sub-section (3), or where the data principal is not satisfied with the manner in which the grievance is resolved, or the data fiduciary has rejected the grievance raised, the data

principal shall have the right to file a complaint with the adjudication wing under section 68 of the Act in the manner prescribed.

(5) Any person aggrieved by an order made under this section by an Adjudicating Officerin accordance with the procedure prescribed in this regard, may prefer an appeal to the Appellate Tribunal.

CHAPTER VIII

TRANSFER OF PERSONAL DATA OUTSIDE INDIA

40. Restrictions on Cross-Border Transfer of Personal Data.

(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.

(2) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

(3) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.

(4) Nothing contained in sub-section (3) shall apply to sensitive personal data.

41. Conditions for Cross-Border Transfer of Personal Data.

(1) Personal data other than those categories of sensitive personal data notified under sub-section (2) of section 40 may be transferred outside the territory of Indiawhere –

(a) the transfer is made subject to standard contractual clauses or intra-group schemes that have been approved by the Authority; or

(b) the Central Government, after consultation with the Authority, has prescribed that transfers to a particular country, or to a sector within a country or to a particular international organisation is permissible; or

(c) the Authority approves a particular transfer or set of transfers as permissible due to a situation of necessity; or

(d) in addition to clause (a) or (b) being satisfied, the data principal has consented to such transfer of personal data; or

(e) in addition to clause (a) or (b) being satisfied, the data principal has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data notified under sub-section (2) of section 40.

(2) The Central Government may only prescribe the permissibility of transfers under clause (b) of sub-section (1) where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section.

(3) Notwithstanding sub-section (2) of Section 40,sensitive personal data notified by the Central Government may betransferred outside the territory of India –

(a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and

(b) to a particular country, a prescribed sector within a country or to a particular international organisation that has beenprescribed under clause (b) of sub-section (1), wherethe Central Government is satisfied that such transfer or class of transfersis necessary for any class of data fiduciaries or data principals anddoesnot hamper the effective enforcement of this Act.

(4) Any transfer under clause (a) ofsub-section (3) shall be notified to the Authority within such time period as may be prescribed.

(5) The Authority may only approve standard contractual clauses or intra-group schemes under clause (a) of sub-section (1) where such clauses or schemes effectively protect the rights of data principals under this Act, including in relation with further transfers from the transferees of personal data under this sub-section to any other person or entity.

(6) Where a data fiduciary seeks to transfer personal data subject to standard contractual clauses or intra-group schemes under clause (a) of sub-section (1), it shall certify and periodically report to the Authority as may be specified, that the transfer is made under a contract that adheres to such standard contractual clauses or intra-group schemes and that it shall bear any liability for the harm caused due to any non-compliance with the standard contractual clauses or intra-group schemes by the transferee.

CHAPTER IX

EXEMPTIONS

42. Security of the State.

(1) Processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law,andis in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved.

(2) Any processing authorised by a lawreferred to in sub-section (1) shall be exempted from the following provisions of the Act

(a) Chapter II, except section 4;
(b) Chapter III;
(c) Chapter IV;
(d) Chapter V;
(e) Chapter VI;
(f) Chapter VII, except section 31; and
(g) Chapter VIII.

43. Prevention, detection, investigation and prosecution of contraventions of law.

(1) Processing of personal data in the interests of prevention, detection,investigation and prosecution of any offence or any other contravention of law shall not be permitted unless it is authorised by a law made by Parliament and State Legislatureand is necessary for, and proportionate to, such interests being achieved.

(2) Any processing authorised by law referred to in sub-section (1) shall be exempted from the following provisions of the Act –

(a) Chapter II, except section 4;
(b) Chapter III;
(c) Chapter IV;
(d) Chapter V;
(e) Chapter VI;
(f) Chapter VII except section 31; and
(g) Chapter VIII.

(3) Sub-section (1) shall apply in relation to processing of personal data of a data principal who is a victim, witness, or any person with information about the relevant offence or contravention only if processing in compliance with the provisions of this law would be prejudicial to the prevention, detection, investigation or prosecution of any offence or other contravention of law.

(4) Personal data processed under sub-section (1) shall not be retained once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete except where such personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence or class of offences in future.

44. Processing for the purpose of legal proceedings. –

(1) Where disclosure of personal data is necessary for enforcing any legal right or claim, seeking any relief, defending any charge,opposing any claim, or obtaining any legal advice from an advocate in any impending legal proceeding such processing shall be exempted from the following provisions of this Act –

(a) Chapter II, except section 4;
(b) Chapter III;

(c) Chapter IV;
(d) Chapter V;
(e) Chapter VI; and
(f) Chapter VII, except section 31.

(2) Where processing of personal data by any Court or Tribunal in India is necessary for the exercise of any judicial function, such processing shall be exempted from the following provisions of this Act –

(a) Chapter II, except section 4;
(b) Chapter III;
(c) Chapter IV;
(d) Chapter V;
(e) Chapter VI; and
(f) Chapter VII, except section 31.

45. Research, archiving or statisticalpurposes. –

(1) Where processing of personal data is necessary for research, archiving, or statistical purposes, such processing may be exempted from such provisions of this Act as the Authority may specify except section 4, section 31 and section 33.

(2) For the purpose of sub-section (1), the Authority may exempt different categories of research, archiving, or statistical purposes from different provisions of the Act.

(3) Sub-section (1) shall apply only where –

(a) compliance with the provisions of this Act will disproportionately divert resources from the purpose referred to in sub-section (1);
(b) the purposes of processing cannot be achieved if the personal data is anonymised;
(c) the data fiduciary has carried out de-identification meeting the standard contained in any code of practice under section 61, where the purpose of

processing can be achieved if the personal data is in a de-identified form;

(d) personal data will not be used to take any decision specific to or action directed specifically towards the data principal; and

(e) personal data will not be processed in a manner that gives rise to a risk of significant harm to the data principal.

46. Personal or domestic purposes. –

(1) Personal data processed by a natural person in the course of a purely personal or domestic purpose, shall be exempted from the following provisions of this Act –

(a) Chapter II, except section 4;
(b) Chapter III;
(c) Chapter IV;
(d) Chapter V;
(e) Chapter VI;
(f) Chapter VII; and
(g) Chapter VIII.

(2) Sub-section (1) shall not apply where the relevant processing –

(a) involvesdisclosure to the public; or
(b) is undertaken in connection with any professional or commercial activity.

47. Journalistic purposes.

(1) Where the processing – of personal data is necessary for or relevant to a journalistic purpose, the following provisions of the Act shall not apply –

(a) Chapter II, except section 4;
(b) Chapter III;
(c) Chapter IV;

(d) Chapter V;
(e) Chapter VI;
(f) Chapter VII except section 31; and
(g) Chapter VIII.

(2) Sub-section (1) shall apply only where itcan be demonstrated that the processing is in compliance with any code of ethics issued by –

(a) the Press Council of India, or
(b) any media self-regulatory organisation

48. Manual processing by small entities. –

(1) Subject to any law for the time being in force, where personal data is processed through means other than automated means by a small entity, the following provisions of the Act shall not apply

(a) Sections 8, 9 and 10 in Chapter II;
(b) Clause (c) of sub-section (1) of section 24, and sections 26 and 27 in Chapter VI; and
(c) Section 29 to section 36, and sections 38 and 39 in Chapter VII.

(2) For the purposes of sub-section (1), a small entity shall be any data fiduciary which –

(a) did not have a turnover of more than twenty lakh rupees or such other lower amount as may be prescribed by the Central Government in the preceding financial year;
(b) does not collect personal data for the purpose of disclosure to any other individuals or entities, including other data fiduciaries or processors; and
(c) did not process personal data of more than one hundred data principals in any one day in the preceding twelve calendar months.

Explanation: For the purpose of sub-section (2), "turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, by the data fiduciary in the preceding financial year.

CHAPTER X

DATA PROTECTION AUTHORITY OF INDIA

49. Establishment and incorporation of Authority.

(1) The Central Government shall, by notification, establish for the purposes of this Act, an Authority to be called the Data Protection Authority of India.

(2) The Authority shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

(3) The head office of the Authority shall be at such place as may be prescribed.

(4) The Authority may, with the prior approval of the Central Government, establish its offices at other places in India.

50. Composition and qualifications for appointment of members. –

(1) The Authority shall consist of a chairpersonand sixwhole-time members.

(2) The chairperson and the members of the Authority shall be appointed by the Central Government on

the recommendation made by a selection committee consisting of –

(a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, who shall be the chairperson of the selection committee;
(b) theCabinet Secretary; and
(c) oneexpert of repute as mentioned in sub-section (6), to be nominated by the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India,in consultation with the Cabinet Secretary.

(3) The procedure to be followed by the selection committee for recommending the names under sub-section (2) shall be such as may be prescribed.
(4) The chairperson and the members of the Authority shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than ten years professional experience in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, and related subjects.
(5) A vacancy caused to the office of the chairperson or any other member shall be filled up within a period of three months from the date on which such vacancy occurs.
(6) The Central Government shall maintain a list of at least five experts who have specialised knowledge of, and professional experience in the field of data protection, information technology, data management, data science, cyber and internet laws, and related subjects.

51. Terms and conditions of appointment. –

(1) The chairperson and the members shall be appointed for a term of five years or till they attain the age of sixty-five

years, whichever is earlier, and they shall not be eligible for re-appointment.

(2) The salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members shall be such as may be prescribed and shall not be varied to their disadvantage during their term.

(3) The chairperson and the members shall not, during their term and for a period of two years from the date on which they cease to hold office, accept –

(a) any employment either under the Central Government or under any State Government; or

(b) any appointment, in any capacity whatsoever, with a significant data fiduciary.

(4) Notwithstanding anything contained in sub-section (1), the chairperson or a member may –

(a) relinquish his office by giving in writing to the Central Government a notice of not less than three months; or

(b) be removed from his office in accordance with the provisions of this Act.

52. Removal of members. –

(1) The Central Government may remove from office, the chairperson or any member who –

(a) has been adjudged an insolvent;

(b) has become physically or mentally incapable of acting as a chairperson or member;

(c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;

(d) has so abused her position as to render her continuation in office detrimental to the public interest; or

(e) has acquired such financial or other interest as is likely to affect prejudicially her functions as a chairperson or a member.

(2) No chairperson or any member shall be removed under clause (d) or (e) of sub-section (1) unless she has been given a reasonable opportunity of being heard.

53. Powers of the chairperson. –

The chairperson shall have powers of general superintendence and direction of the affairs of the Authority and shall also exercise all powers and do all such acts and things which may be exercised or done by the Authority under the Act.

54. Meetings of the Authority. –

(1) The chairperson and members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.

(2) If, for any reason, the chairperson is unable to attend any meeting of the Authority, any other member chosen by the members present at the meeting, shall preside at the meeting.

(3) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the members present and voting, and in the event of an equality of votes, the chairperson or in her absence, the member presiding, shall have a casting or a second vote.

(4) Any member who has any direct or indirect pecuniary interest in any matter coming up for consideration at a meeting of the Authority shall disclose the nature of her interest at such meeting, which shall be recorded in the proceedings of the Authority and such member shall not

take part in any deliberation or decision of the Authority with respect to that matter.

55. Vacancies, etc. not to invalidate proceedings of the Authority. –

No act or proceeding of the Authority shall be invalid merely by reason of –

(a) any vacancy or defect in the constitution of the Authority;
(b) any defect in the appointment of a person as a chairperson or member; or,
(c) any irregularity in the procedure of the Authority not affecting the merits of the case.

56. Officers and Employees of the Authority. –

(1) The Authority may appoint such officers, employees, consultants and experts as it may consider necessary for effectively discharging its functions under this Act.
(2) Any remuneration, salary or allowances, and other terms and conditions of service of such officers, employees, consultants and experts shall be such as may be specified.

57. Grants by Central Government. –

The Central Government may, after due appropriation made by Parliament by law in this behalf, make to the Authority grants of such sums of money as it may think fit for the purposes of this Act.

58. Accounts and Audit –

(1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of

accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor-General of India.

(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by her in connection with such audit shall be reimbursed to her by the Authority.

(3) The Comptroller and Auditor-General of India and any other person appointed by her in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor-General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.

(4) The accounts of the Authority as certified by the Comptroller and Auditor-General of India or any other person appointed by the Comptroller and Auditor-General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.

59. Furnishing of returns, etc. to Central Government. –

(1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require.

(2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government.

(3) A copy of the report received under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament.

60. Powers and Functions of the Authority. –

(1) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness of data protection.

(2) Without prejudice to the generality of the foregoing and other functions set out under this Act, the functions of the Authority shall include –

(a) monitoring and enforcing application of the provisions of this Act;

(b) specifying reasonable purposes for which personal data may be processed under section 17 of this Act;

(c) specifying residuary categories of sensitive personal data under section 22 of this Act;

(d) taking prompt and appropriate action in response to a data security breach in accordance with the provisions of this Act;

(e) specifying the circumstances where a data protection impact assessment may be required to be undertaken in accordance with section 33 of this Act;

(f) maintaining a database on its website containing names of significant data fiduciaries along with a rating in the form of a data trust score indicating

compliance with the obligations of this Act by such fiduciaries;

(g) specifying the criteria for assigning a rating in the form of a data trust score by a data auditor having regard to the factors mentioned in sub-section (2) of section 35;

(h) examination of any data audit reports submitted under section 35 of this Act and taking any action pursuant thereto in accordance with the provisions of this Act;

(i) issuance of a certificate of registration to data auditors and renewal, modification, withdrawal, suspension or cancellation thereof and maintaining a database on its website of such registered data auditors and specifying the requisite qualifications, code of conduct, practical training and functions to be performed by such data auditors;

(j) categorisation and issuance of certificate of registration to significant data fiduciaries and renewal, modification, withdrawal, suspension or cancellation thereof under section 38;

(k) monitoring cross-border transfer of personal data undersection 41 of this Act;

(l) issuing codes of practice in accordance with section 61 of this Act and publishing such codes on its website;

(m) promoting public awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data, including issuance of any public statement setting out trends in, or specific instances of, contravention of the provisions of this Act by a data fiduciary or a class of data fiduciaries, as the case may be;

(n) promoting awareness among data fiduciaries of their obligations and duties under this Act;

(o) monitoring technological developments and commercial practices that may affect protection of personal data;
(p) promoting measures and undertaking research for innovation in the field of protection of personal data;
(q) advising Parliament, Central Government, State Government and any regulatory or statutory authority on measures that must be undertaken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;
(r) issuing guidance on any provision under this Act either on its own or in response to any query received from a data fiduciary where the Authority considers it necessary, subject always to the provisions of this Act;
(s) advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;
(t) specifying fees and other charges for carrying out the purposes of this Act;
(u) receiving and handling complaints under the provisions of this Act;
(v) calling for information from, conducting inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of this Act;
(w) preparation and publication of reports setting out the result of any inspection or inquiry and any other comments that the Authority deems to be in public interest; and
(x) performing such other functions, including maintaining, updating and submitting any records, documents,books, registers or any other data, as may be prescribed.

(3) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under clause (v) of sub-section (2), the Authority shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908) while trying a suit, in respect of the following matters, namely –

(a) the discovery and production of books of account and other documents, at such place and at such time as may be specified;
(b) summoning and enforcing the attendance of persons and examining them on oath;
(c) inspection of any book, document, register or record of any data fiduciary;
(d) issuing commissions for the examination of witnesses or documents;
(e) any other matter which may be prescribed.

(4) Where, pursuant to the provisions of this Act, the Authority processes personal data,it shall be construed as the data fiduciary or the data processor in relation to such personal data as applicable, and where the Authority comes into possession of any information that is treated as confidential by the data fiduciary or data processor, it shall not disclose such information unless required as per law, or where it is required to carry out its function under clause (w) of sub-section (2).

61. Codes of Practice. –

(1) The Authority shall issue codes of practice in accordance with this section to promote good practices of data protection and facilitate compliance with the obligations under this Act.

(2) Notwithstanding sub-section (1), the Authority may also approve,and issue codes of practice submittedby an industry or trade association, an association representing

the interest of data principals, any sectoral regulator or statutory authority, or any departments or ministries of the Central or State Government.

(3) The Authority shall ensure transparency while approving or issuing any code of practice under this section in accordance with sub-section (4).

(4) A code of practice, whether under sub-section (1) or sub-section (2), shall not be issued unless the Authority has undertaken a requisite consultation process with relevant sectoral regulators and stakeholders including the public and has followed the procedure for issuance of such code of practice, as may be prescribed.

(5) A code of practice issued under this section shall not derogate fromthe provisions of this Actor any applicable law.

(6) Without prejudice to sub-sections (1) or (2), or any other provision of this Act, the Authority may issue codes of practice in respect of the following matters –

(a) requirements for notice undersection 8 of this Act including any model forms or guidance relating to notice;

(b) measures for ensuring quality of personal data processed under section 9 of this Act;

(c) measures pertaining to the retention of personal data under section 10 of this Act;

(d) conditions for valid consent under section 12 of this Act;

(e) processing of personal data under section 15 of this Act;

(f) activities where processing of personal data may be undertaken undersection 17;

(g) processing of sensitive personal data under Chapter IV of this Act;

(h) processing of personal data under any other ground for processing, including processing of personal data of children and development of appropriate age-verification mechanisms under section 23 and mechanisms for processing personal data on the basis of consent of users incapable of providing valid consent under this Act;
(i) exercise of any right by data principals under Chapter VI of this Act;
(j) the standards and means by which a data principal may avail the right to data portability under section 26 of this Act;
(k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VII of this Act;
(l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 31 of this Act;
(m) methods of de-identification and anonymisation;
(n) methods of destruction, deletion, or erasure of personal data where required under this Act;
(o) appropriate action to be taken by the data fiduciary or data processor in response to a personal data breach under section 32 of this Act;
(p) manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 33 of this Act;
(q) cross-border transfer of personal data pursuant to section 41 of this Act;
(r) processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 45 of this Act; and

(s) any other matter which, in the view of the Authority, may require issuance of a code of practice.

(7) Non-compliance by the data fiduciary or data processor with any code of practice issued under this section and applicable to it may be considered by the Authority, or any court, tribunal or statutory body, while determining whether such data fiduciary or data processor has violated the provisions of this Act.

(8) Nothing contained in sub-section (7) shall prevent a data fiduciary or data processor from demonstrating before the Authority, or any court, tribunal or statutory body, that it has adopted an equivalent or a higher standard than that stipulated under the relevant code of practice.

(9) The Authority may review, modify or revoke a code of practice issued under this section in the manner prescribed.

(10) The Authority shall maintain a register in the manner prescribed containing details of the codes of practice, which are currently in force and shall make such codes of practice publicly available on its website.

62. Power of Authority to issue directions. –

(1) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to data fiduciaries or data processors generally, or to any data fiduciaryor data processor in particular, and such data fiduciaries or data processors, as the case may be, shall be bound to comply with such directions.

(2) No such direction shall be issued under sub-section (1) unless the Authority has given a reasonable opportunity of being heard to the data fiduciaries or data processors concerned.

(3) The Authority may, on a representation made to it or on its own motion, modify, suspend, withdraw or cancel any direction issued under sub-section (1) and in doing so, may impose such conditions as it thinks fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.

63. Power of Authority to call for information. –

(1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciaryor data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.

(2) If the Authority requires a data fiduciary or a data processor to provide information as per sub-section (1), it must provide a written notice to the data fiduciaryor the data processor stating the reasons for such requisition.

(3) The Authority shall specify the manner in which the data fiduciaryor data processor shall provide the information sought in sub-section (1), including the designation of the officer or employee of the Authority who may seek such information, time frame within which such information is required to be furnished and the form in which such information may be provided.

64. Power of Authority to conduct inquiry. –

(1) The Authority may conduct an inquiry where it has reasonable grounds to believe that –

(a) the activities of the data fiduciaryor data processor being conducted in a manner which is detrimental to the interest of data principals; or

(b) anydata fiduciaryor data processor has violated any of the provisions of this Act or the rules prescribed, or the regulations specified, or directions issued by the Authority thereunder.

(2) For the purpose of sub-section (1), the Authority shall, by an order in writing, appoint one of its officers as an Inquiry Officer to inquire into the affairs of such data fiduciaryor data processor and to report to the Authority on any inquiry made.

(3) An Inquiry Officer, may wherever necessary, appoint any other person for the purpose of assisting in any inquiry under this section.

(4) The order referred to in sub-section (2) shall also set out the reasons for commencing the inquiry and the scope of the inquiry and may be modified from time to time.

(5) Every officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor, where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, shall be bound to produce before the Inquiry Officer directed to make the inquiry, all such books, registers, documents, records and any data in their custody or power and to furnish to the Inquiry Officer any statement and information relating to the affairs of the data fiduciary or data processor as the Inquiry Officer may require within such time as the said Inquiry Officer may specify.

(6) The Inquiry Officer shall undertake the inquiry only after providing a written notice to the persons referred to in sub-section (5) stating the reasons for the inquiry and the relationship between the data fiduciary and the scope of the inquiry.

(7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, record and data are produced, unless an approval to retain such

books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority.

(8) Without prejudice to any other power set out in this Act or under any other law, any Inquiry Officer directed to make an inquiry may examine on oath, any officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, in relation to the business or activity of the data fiduciary or data processor.

65. Action to be taken by Authority pursuant to an inquiry. –

(1) On receipt of a report under sub-section (2) of section 64, the Authority may, after giving such opportunity to the data fiduciaryor data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing –

(a) issue a warning to the data fiduciary or data processor where the business or activity is likely to violate the provisions of this Act;

(b) issue a reprimand to the data fiduciary or data processor where the business or activity has violated the provisions of this Act;

(c) require the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act;

(d) require the data fiduciaryor data processor to modify its business or activity to bring it in compliance with the provisions of this Act;

(e) temporarily suspend or discontinue business or activity of the data fiduciary or data processor which is in contravention of the provisions of this Act;
(f) vary, suspend or cancel any registration granted by the Authority in case of a significantdata fiduciary;
(g) suspend or discontinue any cross-border flow of personal data; or
(h) require the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may think fit.

(2) A data fiduciaryor data processor aggrieved by an order made under this section by the Authority may prefer an appeal to the Appellate Tribunal.

66. Search and Seizure.

(1) Where the Authority has reasonable grounds to believe that –

(a) any person who has been required under sub-section (5) of section 64to produce, or cause to be produced, any books, registers, documents, records or data in her custody or power is likely to omit or fail, or has omitted or failed, to do so; or
(b) any books, registers, documents, records or data belonging to any person as mentioned in clause(a) of sub-section (1) are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed; or
(c) a contravention of any provision of this Act has been committed or is likely to be committed by a data fiduciary,

it may authorise any officer of the Authority not below the rank equivalent to that of a Gazetted Officer of the

Central Government (hereinafter referred to as "Authorised Officer") to –

(i) enter and search any building or place where she has reason to suspect that such books, registers, documents, records or data are kept;
(ii) break open the lock of any box, locker, safe, almirah or other receptacle for exercising the powers conferred by clause (i) where the keys thereof are not available;
(iii) access any computer, computer resource, or any other device containing or suspected to be containing data;
(iv) seize all or any such books, registers, documents, records or data found as a result of such search;
(v) place marks of identification on such books, registers, documents, records or databases or make extracts or copies of the same.

(2) The Authorised Officer may requisition the services of any police officer or of any officer of the Central Government, or of both, as the case may be, for assistance related to any of the purposes specified in sub-section (1) and it shall be the duty of every such police officer or officer to comply with such requisition.

(3) The Authorised Officer may, where it is not practicable to seize any such book, register, document, record or data specified in sub-section (1), serve an order on the person who is in immediate possession or control thereof that such person shall not remove, part with or otherwise deal with it except with the previous permission of such officer and such officer may take such steps as may be necessary for ensuring compliance with this sub-section.

(4) The Authorised Officer may, during the course of the search or seizure, examine on oath any person who is found to be in possession or control of any books,

registers, documents, records or data, and any statement made by such person during such examination may thereafter be used in evidence in any proceeding under this Act.

(5) The books, registers, documents, records or data seized under sub-section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the reasons for retaining the same are recorded by her in writing and the approval of the Authority for such retention is obtained.

(6) The Authority shall not authorise the retention of the books, registers, documents, records or data for a period exceeding thirty days after all the proceedings under this Act, for which the said books, registers, documents, records or data are relevant, are completed.

(7) The person from whose custody the books, registers, documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer or any other person appointed by her in this behalf at such place and time as the Authorised Officer may designate in this behalf.

(8) If a person legally entitled to the books, registers, documents, records or data seized under sub-section (1) objects for any reason to the approval given by the Authority under sub-section (5), such person may make an application to the Appellate Tribunal stating therein the reason for such objection and requesting for the return of the books, registers, documents, records or data.

(9) On receipt of the application under sub-section (8), the Appellate Tribunal may, after giving the parties an opportunity of being heard, pass such order as it thinks fit including any order prohibiting the destruction or

alteration of such books, registers, documents, records or data.

(10) The provisions of the Code of Criminal Procedure, 1973 (2 of 1974) relating to searches and seizures shall apply, so far as may be, to every search and seizure made under sub-section (1).

(11) Without prejudice to the generality of the foregoing, rules may be prescribed in relation to the process for search and seizure under this section and in particular may provide for –

(a) obtaining ingress into such building or place to be searched where free ingress thereto is not available;

(b) obtaining access to a computer, computer resource, or any other device containing or suspected to be containing data, where such access is not available;

(c) ensuring safe custody of any books, registers, documents, records or data seized under this section.

67. Coordination between the Authority and other regulators or authorities. –

Where any action proposed to be taken by the Authority under this Act is such that any other regulator or authority constituted under a law made by Parliament or the State legislature may also have concurrent jurisdiction, the Authority shall consult such other regulator or authority before taking such action and may also enter into a memorandum of understanding with such other regulator or authority governing the coordination of such actions.

68. Appointment of Adjudicating Officer. –

(1) Without prejudice to any other provision of this Act and for the purpose of imposing of penalties under section69to section 73or awarding compensation under section 75, the Authority shall have a separate adjudication wing.

(2) The Central Government shall,having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication wing,prescribe –

(a) number of Adjudicating Officers;
(b) qualification of Adjudicating Officers;
(c) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;
(d) jurisdiction of Adjudicating Officers;
(e) procedure for carrying out an adjudication under this Act; and
(f) other such requirements as the Central Government may deem fit.

(3) The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects.

CHAPTER XI

PENALTIES AND REMEDIES

69. Penalties. –

(1) Where thedata fiduciary contravenes any of the following provisions, it shall be liable to a penalty which may extend up to five crore rupeesor two per cent of its total worldwide turnover of the preceding financial year, whichever is higher, as applicable –

(a) obligation to take prompt and appropriate action in response to a data security breach under section 32 of this Act;
(b) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 33 of this Act;
(c) obligation to conduct a data audit by a significant data fiduciary under section 35 of this Act;
(d) appointment of a data protection officer by a significantdata fiduciaryundersection 36 of this Act;
(e) failure to register with the Authority under sub-section (2) of section 38.

(2) Where a data fiduciary contravenes any of the following provisions, it shall be liable to a penalty which may extend up to fifteen crore rupees or four per cent of its total worldwide turnover of the preceding financial year, whichever is higher, as applicable –

(a) processing of personal data in violation of the provisions of Chapter II;
(b) processing of personal data in violation of the provisions of Chapter III;
(c) processing of sensitive personal data in violation of the provisions of Chapter IV of this Act;

(d) processing of personal data of children in violation of the provisions of Chapter V;
(e) failure to adhere to security safeguards as per section 31 of this Act;
(f) transfer of personal data outside India in violation of section 41 of this Act.

Explanation I. For the purposes of this section, "total worldwide turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.

Explanation II. For the purposes of this section, it is hereby clarified thattotal worldwide turnover in relation to a data fiduciaryis the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including –

(i) thealignment of the overall economic interests of the data fiduciary and the group entity;
(ii) therelationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and
(iii) thedegree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be.

70. Penalty for failure to comply with data principal requests under Chapter VI. –

Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter VI of this Act, such data fiduciary shall be liable to a

penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

71. Penalty for failure to furnish report, returns, information, etc.

If any data fiduciary, who is required under this Act, or rules prescribed or regulations specified thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to penalty which shall be ten thousand rupees for each day during which such default continues, subject to a maximum of twenty lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

72. Penalty for failure to comply with direction or order issued by the Authority. –

If any data fiduciaryor data processor fails to comply with any direction issued by the Authority under section 62or order issued by the Authority under section 65,as applicable, such data fiduciaryor data processor shall be liable to a penalty which, in case of a data fiduciary may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore rupees, and in case of a data processor may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.

73. Penalty for contravention where no separate penalty has been provided. –

Where any person fails to comply with any provision of this Act, or rules prescribed or regulations specified thereunder

as applicable to such person, for which no separate penalty has been provided, then such person shall be liable to a penalty subject to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in all other cases.

74. Adjudication by Adjudicating Officer. –

(1) No penalty shall be imposed under this Chapter except after conducting an inquiry in such manner as may be prescribed, and the data fiduciary or data processoror any person, as the case may be, has been given a reasonable opportunity of being heard.

(2) While holding an inquiry, the Adjudicating Officer shall have the power to summon and enforce the attendance of any person acquainted with the facts and circumstances of the case to give evidence or to produce any document which, in the opinion of the Adjudicating Officer, may be useful for or relevant to the subject matter of the inquiry.

(3) If, on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal as a result of any violation of the provisions of this Act, which a penalty may be imposed under section 69to section 73, the Adjudicating Officer may impose a penalty in accordance with the provisions of the appropriate section.

(4) While deciding whether to impose a penalty under sub-section (3) of this section and in determining the quantum of penalty under section69to section 73, the Adjudicating Officer shall have due regard to the following factors, as may be applicable –

(a) nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned;

(b) number of data principals affected, and the level of harm suffered by them;
(c) intentional or negligent character of the violation;
(d) nature of personal data impacted by the violation;
(e) repetitive nature of the default;
(f) transparency and accountability measures implemented by the data fiduciary or data processor including adherence to any relevant code of practice relating to security safeguards;
(g) action taken by the data fiduciary or data processor to mitigate the harm suffered by data principals; and
(h) any other aggravating or mitigating factors relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

(5) Any person aggrieved by an order under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

75. Compensation. –

(1) Any data principal who has suffered harm as a result of any violation of any provision under this Act, or rules prescribed or regulations specified hereunder, by a data fiduciary or a data processor, shall have the right to seek compensation from the data fiduciary or the data processor, as the case may be.

Explanation.- For the removal of doubts, it is hereby clarified that a data processor shall be liable only where it has acted outside or contrary to the instructions of the data fiduciary pursuant to section37, or where the data processor is found to have acted in a negligent manner, or where the data processor has not incorporated adequate security safeguards under

section 31, or where it has violated any provisions of this Act expressly applicable to it.

(2) The data principal may seek compensation under this section pursuant to a complaint instituted in such form and manner as may be prescribed before an Adjudicating Officer.

(3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any violation by the same data fiduciary or data processor, one complaint may be instituted on behalf of all such principals seeking compensation for the harm suffered.

(4) While deciding whether to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have due regard to the following factors, namely –

(a) nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified thereunder;
(b) nature and extent of harm suffered by the data principal;
(c) intentional or negligent character of the violation;
(d) transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;
(e) action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal;
(f) previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be;

(g) whether the arrangement between the data fiduciary and data processor contains adequate transparency and accountability measures to safeguard the personal data being processed by the data processor on behalf of the data fiduciary;

(h) any other aggravating or mitigating factor relevant to the circumstances of the case, such as, the amount of disproportionate gain or unfair advantage, wherever quantifiable, made as a result of the default.

(5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal as per this section, then each data fiduciary or data processor may be ordered to pay the entire compensation for the harm in order to ensure effective and speedy compensation to the data principal.

(6) Where a data fiduciary or a data processor has, in accordance with sub-section (5), paid the entire amount of compensation for the harm suffered by the data principal, such data fiduciary or data processor shall be entitled to claim from the other data fiduciaries or data processors, as the case may be, that amount of compensation corresponding to their part of responsibility for the harm caused.

(7) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal.

(8) The Central Government may prescribe the procedure for hearing of a complaint under this section.

76. Compensation or penalties not to interfere with other punishment. –

No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under any other law for the time being in force.

77. Data ProtectionFunds. –

(1) There shall be constituted a fund to be called the Data Protection Authority Fundto which the following shall be credited –

(a) all Government grants, fees and charges received by the Authority under this Act; and

(b) all sums received by the Authority from such other source as may be decided upon by the Central Government, but which shall not include the sums mentioned in sub-section (3).

(c) The Data Protection Authority Fund shall be applied for meeting –

(i) the salaries, allowances and other remuneration of the chairperson, members, officers, employees, consultants and experts appointed by the Authority; and

(ii) the other expenses of the Authority in connection with the discharge of its functions and for the purposes of this Act.

(2) Without prejudice to the foregoing, there shall also be constituted a fund to be called the Data Protection Awareness Fundto which all sums realised by way of penalties by the Authority under this Act shall be credited.

(3) The Data Protection Awareness Fund shall be applied solely for the purpose of generating awareness regarding data protection including for the purposes set out in clauses (m), (o) and (p) of sub-section (2) of section 61 and for no other purpose whatsoever.

78. Recovery of Amounts. –

(1) The Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer for the purpose of this Act.

(2) Where any person fails to comply with –

(a) an order of the Adjudicating Officer imposing a penalty under the provisions of this Act; or

(b) an order of the Adjudicating Officer directing payment of compensation under the provisions of this Act,

the Recovery Officer may recover from such person the aforesaid amount in any of the following ways, in descending order of priority, namely –

(i) attachment and sale of the person"s movable property;

(ii) attachment of the person"s bank accounts;

(iii) attachment and sale of the person"s immovable property;

(iv) arrest and detention of the person in prison;

(v) appointing a receiver for the management of the person"s movable and immovable properties.

(3) For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income

Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the said provisions and rules –

(a) were the provisions of this Act; and
(b) referred to the amount due under this Act instead of to income tax under the Income Tax Act, 1961 (43 of 1961).

(4) In this section, the movable or immovable property or monies held in a bank account shall include property or monies which meet all the following conditions –

(a) property or monies transferred by the person without adequate consideration;
(b) such transfer is made:

(i) on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and
(ii) to the person"s spouse, minor child, son"s wife or son"s minor child.

(c) such property or monies are held by, or stand in the name of, any of the persons referred to in sub-clause (b), including where they are so held or stand in the name of such persons after they have attained the age of majority.

(5) The Recovery Officer shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.

CHAPTER XII

APPELLATE TRIBUNAL

79. Establishment of Appellate Tribunal. –

(1) The Central Government shall, by notification, establish an Appellate Tribunal to –

(a) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 39;
(b) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 65;
(c) hear and dispose of an application under sub-section (9) of section 66;
(d) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 74; and
(e) hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 75.

(2) The Appellate Tribunal shall consist of a chairperson and such number of members as may be notified by the Central Government.

(3) The Appellate Tribunal shall be set up at such place or places, as the Central Government may, in consultation with the chairperson of the Appellate Tribunal, notify.

(4) Where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal as envisaged under this Act, then the Central Government may notify such existing body to act as the Appellate Tribunal under this Act.

80. Qualifications, appointment, term, conditions of service of members. –

(1) The Central Government may prescribe the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal.

(2) Neither the salary and allowances nor the other terms and conditions of service of the chairperson or member of the Appellate Tribunal may be varied to her disadvantage after her appointment.

81. Vacancies. –

If, for reason other than temporary absence, any vacancy occurs in the office of the chairperson or a member of the Appellate Tribunal, the Central Government shall appoint another person in accordance with the provisions of this Act and the rules prescribed to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.

82. Staff of Appellate Tribunal. –

(1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit.

(2) The officers and employees of the Appellate Tribunal shall discharge their functions under the general superintendence of its chairperson.

(3) The salaries and allowances and other conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.

83. Distribution of business amongst benches. –

(1) Subject to the provisions of this Act, the jurisdiction of the Appellate Tribunal may be exercised by benches thereof, which shall be constituted by the chairperson.

(2) Where benches of the Appellate Tribunal are constituted under sub-section (1), the chairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the benches, transfer of members between benches, and also provide for the matters which may be dealt with by each bench.

(3) On the application of any of the parties and after notice to the parties, and after hearing such of them as the chairperson may desire to be heard, or on the chairperson"s own motion without such notice, the chairperson of the Appellate Tribunal may transfer any case pending before one bench, for disposal, to any other bench.

84. Appeals to Appellate Tribunal. –

(1) Any person may file an appealor application, as the case may be, with the Appellate Tribunal in such form, verified in such manner and be accompanied by such fee, as may be prescribed.

(2) Any appeal or application to the Appellate Tribunal, as the case may beshall be preferred within a period of thirty days from the date on which a copy of the decision or order made by the Authority or the Adjudicating Officer, as the case may be, is received by the appellant or applicant and it shall be in such form, verified in such manner and be accompanied by such fee as may be prescribed.

(3) Notwithstanding sub-section (2), the Appellate Tribunal may entertain any appeal or application, as the case may be, after the expiry of the said period of thirty days if it

is satisfied that there was sufficient cause for not filing it within that period.

(4) On receipt of an appealor application, as the case may be, under this section, the Appellate Tribunal may, after providing the parties to the dispute or appeal, an opportunity of being heard, pass such orders thereon as it thinks fit.

(5) The Appellate Tribunal shall send a copy of every order made by it to the parties to the dispute or the appeal and to the Authority, as the case may be.

(6) The Appellate Tribunal may, for the purpose of examining the legality or propriety or correctness, of any decision, or order of the Authority or Adjudicating Officer referred to in the appeal or application preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.

85. Procedure and powers of Appellate Tribunal. –

(1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 (5 of 1908), but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.

(2) The Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying a suit, in respect of the following matters, namely –

(a) summoning and enforcing the attendance of any person and examining her on oath;

(b) requiring the discovery and production of documents;

(c) receiving evidence on affidavits;
(d) subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872 (1 of 1872), requisitioning any public record or document or a copy of such record or document, from any office;
(e) issuing commissions for the examination of witnesses or documents;
(f) reviewing its decisions;
(g) dismissing an application for default or deciding it, ex parte;
(h) setting aside any order of dismissal of any application for default or any order passed by it, *ex parte;* and
(i) any other matter which may be prescribed.

(3) Every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860) and the Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 (2 of 1974).

86. Orders passed by Appellate Tribunal to be executable as a decree.

(1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.
(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

87. Appeal to Supreme Court of India. –

(1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 (5 of 1908) or in any other law, an appeal shall lie against any order of the Appellate Tribunal to the Supreme Court of India.

(2) No appeal shall lie against any decision or order made by the Appellate Tribunal with the consent of the parties.

(3) Every appeal under this section shall be preferred within a period of ninety days from the date of the decision or order appealed against.

(4) Notwithstanding sub-section (3), the Supreme Court of India may entertain the appeal after the expiry of the said period of ninety days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.

88. Right to legal representation. –

The applicant or appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present her or its case before the Appellate Tribunal.

Explanation.- For the purposes of this section, "legal practitioner" includes an advocate, or an attorney and includes a pleader in practice.

89. Civil court not to have jurisdiction. –

No civil court shall have jurisdiction to entertain any suit or proceeding in respect of any matter which the Appellate Tribunal is empowered by or under this Act to determine and no injunction shall be granted by any court or other authority in respect of any action taken or to be taken in pursuance of any power conferred by or under this Act.

CHAPTER XIII

OFFENCES

90. Obtaining, transferring or selling of personal data contrary to the Act. –

Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act –

(a) obtains personal data; or
(b) discloses personal data; or
(c) transfers personal data to another person; or
(d) sells or offers to sell personal data to another person,

which results in significant harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both.

91. Obtaining, transferring or selling of sensitive personal data contrary to the Act. –

Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act –

(a) obtains sensitive personal data; or
(b) discloses sensitive personal data; or
(c) transfers sensitive personal data to another person; or
(d) sells or offers to sell sensitive personal data to another person,

which results in harm to a data principal, then such person shall be punishable with imprisonment for a term not exceeding five years or shall be liable to a fine which may extend up to rupees three lakhs or both.

92. Re-identification and processing of de-identified personal data. –

(1) Any person who, knowingly or intentionally or recklessly –

(a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or

(b) re-identifies and processes such personal data as mentioned in clause (a)

without the consent of such data fiduciary or data processor, then such person shall be punishable with imprisonment for a term not exceeding three years or shall be liable to a fine which may extend up to rupees two lakh or both.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided under this section, if she proves that –

(a) the personal data belongs to the person charged with the offence under sub-section (1); or

(b) the data principal whose personal data is in question has explicitly consented to such re-identification or processing as per the provisions of this Act.

93. Offences to be cognizable and non-bailable. –

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), an offence punishable under this Act shall be cognizable and non-bailable.

94. Power to investigate offences. –

Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector shall investigate any offence under this Act.

95. Offences by companies. –

(1) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if she proves that the offence was committed without her knowledge or that she had exercised all due diligence to prevent the commission of such offence.

(3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a company and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any director, manager, secretary or other officer of the company, such director, manager, secretary or other officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

Explanation.- For the purpose of this section –

(a) "company" means any body corporate, and includes –

(i) a firm; and
(ii) an association of persons or a body of individuals whether incorporated or not.

(b) "director" in relation to –

(i) a firm, means a partner in the firm;
(ii) an association of persons or a body of individuals, means any member controlling affairs there of.

96. Offences by Central or State Government departments. –

(1) Where an offence under this Act has been committed by any department of the Central or State Government,or any authority of the State, the head of the department or authority shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if she proves that the offence was committed without her knowledge or that she had exercised all due diligence to prevent the commission of such offence.

(3) Notwithstanding anything contained in sub-section (1), where an offence under this Act has been committed by a department of the Central or State Government, or any authority of the State and it is proved that the offence has been committed with the consent or connivance of, or is attributable to any neglect on the part of, any officer, other than the head of the department or authority, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

CHAPTER XIV

TRANSITIONAL PROVISIONS

97. Transitional provisions and commencement. –

(1) For the purposes of this Chapter, the term „notified date" refers to the date notified by the Central Government under sub-section (3) of section 1.

(2) The notified date shall be any date within twelve months from the date of enactment of this Act.

(3) The following provisions shall come into force on the notified date –

(a) Chapter X;
(b) Section 107; and
(c) Section 108.

(4) The Central Government shall, no later than threemonths from the notified date establish the Authority.

(5) The Authority, shall, no later than twelve months from the notified date, notify the grounds of processing personal data in respect of the activities listed in sub-section (2) of section 17.

(6) The Authority, shall, no later than twelve months from the notified date issue codes of practice on the following matters –

(a) notice under section 8;
(b) data quality under section 9;
(c) storage limitation under section 10;
(d) processing of personal data under Chapter III;
(e) processing of sensitive personal data under Chapter IV;
(f) security safeguards under section 31;
(g) research purposes under section 45;
(h) exercise of data principal rights under Chapter VI;
(i) methods of de-identification and anonymisation; and
(j) transparency and accountability measures under chapter VII.

(7) Section 40 shall come into force on such date as is notified by the Central Government for the purpose of that section.

(8) The remaining provisions of the Act shall come into force eighteen months from the notified date.

CHAPTER XV

MISCELLANEOUS

98. Power of Central Government to issue directions in certain circumstances. –

(1) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order.

(2) Without prejudice to the foregoing provisions of this Act, the Authority shall, in exercise of its powers or the performance of its functions under this Act, be bound by such directions on questions of policy as the Central Government may give in writing to it from time to time:

(3) Any direction issued by the Central Government shall, as far as practicable, be given, after providing an opportunity to the Authority to express its views in this regard.

(4) The decision of the Central Government on whether a question is one of policy or not, shall be final.

99. Members, etc., to be public servants. –

The chairperson, members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

100 . Protection of action taken in good faith. –

No suit, prosecution or other legal proceedings shall lie against the Authority or its chairperson, member, employee or officer for anything which is done in good faith or intended to be done under this Act, or the rules prescribed, or the regulations specified thereunder.

101. Exemption from tax on income. –

Notwithstanding anything contained in the Income Tax Act, 1961 (43 of 1961) or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.

102. Delegation. –

The chairperson of the Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act except the powers under section 108 as it may deem necessary.

103. Power to remove difficulties. –

(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty.

(2) No such order shall be made under this section after the expiry of five years from the commencement of this Act.

(3) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.

104. Power to exempt certain data processors. –

The Central Government may, by notification, exempt from the application of this Act or any provisions of this Act, processing of personal data of data principals not within the territory of India, pursuant to any contract entered into with any person outside the territory of India, including any company incorporated outside the territory of India, by any data processor or any class of data processors incorporated under Indian law.

105. No application to non-personal data

Nothing contained in this Act shall affect the power of the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse,insofar as such policies do not govern personal data.

106. Bar on processing certain forms of biometric data

No data fiduciary shall process such biometric data as may be notified by the Central Government, unless such processing is permitted by law.

107. Power to make rules. –

(1) The Central Government may, by notification, make rules to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely –

(a) the form and manner in which an application to exercise the right under sub-section (4) of Section 27;

(b) the manner of review of the order passed by the Adjudicating Officer under sub-section (5) of section 27;

(c) the manner in which a complaint with the adjudication wing may be filed under sub-section (4) of section 39;
(d) the countries, sectors within a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 41;
(e) the time period of notification to the Authority under sub-section (4) of section 41 of the transfer of personal data to a particular country as permitted under clause (b) of sub-section (3) of section 41;
(f) the amount of turnover for a data fiduciary to qualify as a small entity under clause (a) of sub-section (2) of section 48;
(g) the place of establishment and incorporation of the head office of the Authority as under sub-section (3) of section 49;
(h) procedure to be followed by the selection committeeunder sub-section (3) of section 50;
(i) the salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members of the Authority under sub-section (2) of section 51;
(j) the times and places for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 54;
(k) the form of accounts, other relevant records and annual statement of accounts under sub-section (1) of section 58;
(l) the intervals at which the accounts of the Authority will be audited under sub-section (2) of section 58;
(m) the time in which, and the form and manner in whichthe returns, statements, and particulars are to be furnished to the Central Government under sub-section (1) of section 59;

(n) the time in which, and the form in which an annual report is to be prepared by the Authority and forwarded to the Central Government under sub-section (2) of section 59;
(o) other functions of the Authority under clause (x) of sub-section (2) of section 60;
(p) other matters under clause (e) of sub-section (3) of section 60 in respect of which the Authority shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit;
(q) the procedure of issuance of a code of practice under sub-section (4) of section 61;
(r) the manner in which the Authority may review, modify or revoke a code of practice under sub-section (9) of section 61;
(s) the manner in which the Authority shall maintain a register containing details of the codes of practice under sub-section (10) of section 61;
(t) the process for search and seizure under sub-section (11) of section 66;
(u) the number of Adjudicating Officers that the adjudication wing will consist of under sub-section (2) of section 68;
(v) the qualification, manner and terms of appointment, and jurisdiction of Adjudicating Officers to ensure their independence, and the procedure for carrying out adjudication under this Act and other such requirements as deemed fit by the Central Government under sub-section (2) of section 68;
(w) the manner in which the Adjudicating Officer will conduct an inquiry under sub-section (1) of section 74;
(x) the form and manner of instituting a complaint under sub-section (2) of section 75;

(y) the procedure for hearing of a complaint and the limit on the amount of compensation under sub-section (8) of section 75;

(z) the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal under sub-section (1) of section 80;

(aa) the procedure of filling of vacancies in the Appellate Tribunal under section 81;

(bb) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 82;

(cc) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 84; and

(dd) other matters under clause (i) of sub-section (2) of section 85 in respect of which the Appellate Tribunal shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit.

108. Power to make regulations. –

(1) The Authority may, by notification, make regulations consistent with this Act and the rules prescribed thereunder to carry out the purposes of this Act.

(2) In particular and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:

(a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 8;

(b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 10;
(c) reasonable purposes for which personal data may be processed in accordance with sub-section (2) of section17;
(d) safeguards as may be appropriate for protecting the rights of data principals under sub-section (3) of section17;
(e) any further categories of sensitive personal data and further grounds on which such data may be processed under sub-section (1) of section 22;
(f) such additional safeguards or restrictions applicable to processing of sensitive personal data and any further categories of personal data where there is repeated, continuous, systematic collection for the purposes of profiling and such additional safeguards required under sub-section (3) of section 22;
(g) theadditional factors necessary for determining the appropriateness of age verification mechanisms to be incorporated by a data fiduciary processing the personal data and sensitive personal data of children under sub-section (3) of section 23;
(h) practices that may be undertaken by data fiduciaries offering counseling or child protection services under sub-section (6) of section 23;
(i) the time period within which a data fiduciary must comply with a request made under sub-section (3) of section 28;
(j) the time period within which a data principal may file a complaint under sub-section (4) of section 28;
(k) the form in which the data fiduciary is required to make available to the data principal information under sub-section (1) of section 30;

(l) the manner by which a data fiduciary shall notify the data principal regarding important operations in the processing of personal data under sub-section (2) of section 30;

(m) the manner of periodic review of security safeguards to be undertaken by the data fiduciary and the data processor under sub-section (2) of section 31;

(n) the circumstances or classes of data fiduciaries or processing operations where it is mandatory to carry out data protection impact assessments under sub-section (2) of section 33;

(o) the instances where a data auditor under this Act shall be engaged by the data fiduciary to undertake a data protection impact assessment under sub-section (2) of section 33;

(p) the manner in which the data fiduciary shall submit the data protection impact assessment to the Authority under sub-section (4) of section 33;

(q) any aspect of processing for which records shall be maintained under clause (d) of sub-section (1) of section 34;

(r) the form in which records shall be maintained under sub-section (2) of section 34;

(s) the factors to be taken into consideration while evaluating the compliance of data fiduciaries with the provisions of this Act under sub-section (2) of section 35;

(t) the form, manner and procedure by which data audits shall be conducted under sub-section (3) of section 35;

(u) criteria on the basis of which rating in the form of a data trust score may be assigned to a data fiduciary under sub-section (6) of section 35;

(v) theeligibility, qualifications and functions to be performed by data auditors under sub-section (4) of section 35;

(w) the eligibility and qualification of a data protection officer under sub-section (3) of section 36;
(x) the registration requirements of significant data fiduciaries under sub-section (2) of section 38;
(y) themanner of certification and time period within which transfer of personal data shall be notified to the Authority under sub-section (6) of section 41;
(z) the provisions of the Act which may be exempted for different categories of research, archival or statistical purposes under sub-section (1) of section 45;
(aa) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (2) of section 56;
(bb) any other fees and charges for carrying out purposes of this Act under clause (t) of sub-section (2) of Section 60;
(cc) the manner in which information shall be provided to the authority by the data fiduciary under sub-section (3) of Section 63; and
(dd) any other matter which is required to be, or may be specified,or in respect of which provision is to be or may be made by regulations.

109. Rules and Regulations to be laid before Parliament. –

Every rule and regulation made under this Act shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both Houses agree in making any modification in the rule or regulation or, both Houses agree that the rule or regulation should not be made, the rule or regulation shall thereafter have effect only in such modified form or be of

no effect, as the case may be;so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under that rule or regulation.

110. Overriding effect of this Act. –

Save as otherwise expressly provided under this Act, the provisions of this Act shall have an overriding effect to the extent that such provisions are inconsistent with any other law for the time being in force or any instrument having effect by virtue of any such law.

111. Amendment of Act 21 of 2000. –

The Information Technology Act, 2000 (21 of 2000) shall be amended in the manner set out in the FirstSchedule to this Act.

112. Amendment of Act 22 of 2005. –

The Right to Information Act, 2005 (22 of 2005) shall be in the manner set out in the SecondSchedule to this Act.

THE FIRST SCHEDULE

(See Section 111)

AMENDMENT TO THE INFORMATION TECHNOLOGY ACT, 2000

(21 of 2000)

1. **Deletion of section 43A. —** Section 43A of the Information Technology Act, 2000 (hereinafter referred to as the principal Act) shall be omitted.

2. **Amendment of section 87. —** In section 87 of the principal Act, in sub-section (2), clause (ob) shall be omitted.

THE SECONDSCHEDULE

(SEE SECTION 112)

AMENDMENT TO THE RIGHT TO INFORMATION ACT, 2005

(22 OF 2005)

1. **Amendment of section 8. —** In place of the current clause (j) of sub-section (1) of section 8 of the Right to Information Act, 2005 the following clause (j) of sub-section (1) of section 8 shall be substituted, namely: –

"(j) information which relates to personal data which is likely to cause harm to a data principal, where such harm outweighs the public interest in accessing such information having due regard to the common good of promoting transparency and accountability in the functioning of the public authority;

Provided, disclosure of information under this clause shall be notwithstanding anything contained in the Personal Data Protection Act, 2018;

Provided further, that the information, which cannot be denied to the Parliament or a State Legislature shall not be denied to any person.

Explanation. —For the purpose of this section, the terms „personal data", „data principal", and „harm" shall have the meaning assigned to these terms in the Personal Data Protection Act, 2018."