LOK SABHA

DRAFT REPORT OF THE JOINT COMMITTEE ON THE PERSONAL DATA PROTECTION BILL, 2019

(SEVENTEENTH LOK SABHA)

LOK SABHA SECRETARIAT
NEW DELHI

Recommendations are at para nos.1.15.7.2.,1.15.8.4., 1.15.9.6., 1.15.10.2., 1.15.11.3., 1.15.12.7., 1.15.13.8., 1.15.14.3., 1.15.15.2., 1.15.16.3., 1.15.17.5., 1.15.17.6., 2.4, 2.13, 2.15, 2.25, 2.28, 2.29, 2.30, 2.32, 2.33, 2.34, 2.36, 2.37, 2.38, 2.39, 2.41, 2.43, 2.47, 2.48, 2.50, 2.54, 2.55, 2.56, 2.61, 2.65, 2.76, 2.80, 2.85, 2.90, 2.93, 2.96, 2.99, 2.100, 2.114, 2.123, 2.128, 2.131, 2.138, 2.142, 2.151, 2.152, 2.154, 2.155, 2.172, 2.176, 2.177, 2.181, 2.186, 2.187, 2.189, 2.191, 2.193, 2.200, 2.201, 2.206, 2.207, 2.209, 2.213, 2.215, 2.217, 2.219, 2.222, 2.226, 2.228, 2.233, 2.241, 2.244, 2.246, 2.249, 2.254, 2.56, 2.257, 2.262, 2.266, 2.271, 2.273, 2.275, 2.277, 2.279, 2.81, 2.282.

INDEX

REPORT

PART-I
DATA PROTECTION AND PRIVACY

1.1 Introduction

We are heading towards a data and technology driven "Web of the World" where mobile communications and social media are connecting people in hitherto unforeseen ways. Curated datasets are recorded and then fed into algorithms, which predict who we are, who and what we know, where we are, where we have been and where we plan to go. Processing this data gives us the ability to understand and even predict where humans focus their attention and activity at the individual, group and global level. With around 4.66 billion internet users, the size of the internet is now estimated to be 44 zettabytes (one zettabyte is 10^{21}bytes or one billion terabytes) and new data is being added at the rate of 2.5 quintillion bytes per day. By June 2019, the indexed web was estimated to host 5.85 billion pages, which was only the activity reached via search engines. Moreover, the internet has almost doubled in size every year since 2012. The internet and data have given rise to some of the largest corporations in the world. The spread of data driven technologies around the world has led to several citizen and consumer centric innovations including means of communication and access to goods and services through e-governance and online commerce and transactions. This has resulted in an eruption of online marketplaces where more and more social and economic activities now take place online. Therefore, data is the new oil which has the potential to unleash the true power of an economy. Countries are striving for accelerating socio-economic transformation through the use of smart and secure data.

1.2 Transforming India Through Data

1.2.1. With the world's second largest population, the fifth largest economy with GDP of $3.0 trillion, over 700 million internet users and over 400 million smart phone users, India is generating mammoth amounts of data on a daily basis. India generates about 150 exabytes of data annually and is amongst the fastest growing data generating nations in the world. Data is a new resource that is vital for the internet economy, supporting innovation and building new age businesses. By integrating datasets from various sources and domains and applying data analytics and artificial intelligence technologies, powerful new insights can be generated to build new and innovative products and services. Exploiting data effectively can help accelerate economic growth and development and provide better services to people and businesses. Data can be a significant enabler towards achieving the

vision of an "AatmaNirbhar Bharat" by powering technology driven innovation in almost all sectors of the economy and all domains of governance.

1.2.2. The data, an intangible asset, can be consumed and exploited by various organisations for multiple purposes including for better and more efficient utilization of resources, real-time delivery of services, effective management of disasters, etc. The value chain of data can be described as below:

Data → Information→ Knowledge → Effective Usage

1.2.3. Powerful data analytics and artificial intelligence technologies are moving the world towards predictive and prescriptive analytics thus bringing in disruptive innovations which result in transformation of the society for a better tomorrow. Data can substantially improve socio-economic indicators across sectors- be it health, education, tax collection, poverty, public safety, etc.

1.2.4. There is a plethora of latest data technologies ranging from Cloud, Deep Vision, Artificial Intelligence, Machine Learning, Data Lakes, etc. which enable hyper capabilities - real time access and processing of large volumes of data at extremely high speed. These technologies can be broadly classified into two categories – those that capture and store data, and those that help generate insights from data. The predictive power of data can enhance decision making capabilities for the present and better prepare us for the future.

1.2.5. India already has many data assets of national importance including Aadhar, Passport Seva, Open Data Stack (data.gov.in), MCA21, GSTN, Unified Payment Interface (UPI), WRIS (Jalshakti), DISHA (rural development), Bhuvan (ISRO), etc. These platforms are very efficient and can address specific requirements in their domains and are also cross-cutting in nature as they can also be used as building blocks for providing integrated services in a wide range of domains.

1.2.6. The time has come now to broaden our data vision to solve complex inter-connected social and economic development challenges, connecting various islands of data and move from data collected and used for a specific purpose to create cross-sectoral data sets. There is a need to move from 'siloed' view across different data platforms to truly unleash the power of data for India.

1.2.7. For this purpose, there is need to design and setup processes to unify data sets across public sector, private sector, and academic and research institutions. The data from these sources can be integrated on need basis and can be utilized for applying advanced digital technologies for generating new insights and supporting innovation for improving products and services in various domains. Data management policies would need to be defined to address access, accuracy, privacy, residency and security related aspects of data.

1.2.8. Hence, there is a requirement to formulate robust data management policies, standards and best practices with accurate data, appropriate data access, strong data security, privacy and ownership rights. Deploying advanced digital infrastructure for connecting and aggregating data and making them available for various stakeholders, developing new insights from cross-platform data, and developing a data ecosystem across public and private sectors to spur data led innovation are extremely important. A large and well-organised data ecosystem would also encourage innovation, entrepreneurship and job creation.

1.2.9. In this journey of transforming India through data, there are few data specific challenges like data latency, data duplicity, accuracy and insufficient data, which also need to be addressed.

1.2.10. Data is an asset of national importance which is waiting to be tapped comprehensively. By deploying the right data infrastructure and governance mechanism, unleashing the power of data for India can become a reality.

1.3 Data Protection as a Global Concern

1.3.1.The explosive growth of online transactions for delivery of a wide variety of goods and services has led to generation of huge amounts of data. This has also led to issues in collection, storage, processing and usage of data, particularly personal data. Of equal concern is the sharing of personal information to third parties without notice or consent of individuals and the violation of sovereign laws. Consequently, out of 194 countries, 132 have put in place regulations and legislations to secure the protection of personal data and privacy. About 55% of countries in Asia and Africa have adopted such legislations, out of which 23 are least developed countries. The rise of computer technologies and the internet have given birth to a variety of new online domains of economic and social activities and a host of new stakeholders. These include those dealing with collection, storage, and processing of personal information, directly or as a part of their business models.

1.4 Data: A New Asset Class

1.4.1.At its heart, data is the fuel for a new economy. It represents unprecedented opportunity, complexity, velocity and global reach. Utilizing a humongous communications infrastructure, this will be our gateway to a world where nearly everyone and everything are connected in real time. For this, highly reliable, secure and readily available infrastructure on the back of innovation is imperative. To unlock the full potential of this valuable resource, a balanced and trustworthy ecosystem needs to be deployed amongst individuals, Government and the private sector. The data ecosystem encompasses the following:

- Defining Data Sets: The types, quantity and value of personal data is diverse and deep, including our profiles and demographic data from bank accounts to medical records to employment data.
- Behaviour: Web searches and sites visited, preferences and purchase histories.
- Network: Tweets, posts, texts, emails, phone calls, photos and videos as well as the coordinates of our real-time locations.
- Spending Pattern: Online purchases, transactions, mode of transaction, gateways used, etc.

1.4.2.Personal data is used by big corporations to support personalised service-delivery businesses. The Government uses it to provide various public services in an efficient manner. The data scientists deploy it to design and develop new protocols and algorithms. Users also benefit via personalized consumer experiences which include better internet search suggestions, buying recommendations and social networking experience.

1.5 Dwindling Consumer Trust

1.5.1.The rapid commercial use of personal data has resulted in undermining the end user trust and confidence. Concerns and tensions about misuse of sensitive and critical personal data is rising exponentially. On top of that, there is a sense of unease in the general public regarding what "they" know about them. This "us" vs "they" situation has resulted in a trust deficit on the part of the citizens and consumers.

1.5.2.Dominant uncertainties include privacy, property, global governance, human rights and information asymmetry. It is important to build the legal, cultural, technological and economic infrastructure for development of a secure and user-friendly personal data ecosystem. Big Tech companies have put in perspective the role of data economy. These Big Tech giants are built on the economics of personal data. Several governments across the globe have now started to shift to e-governance initiatives in order to improve the effectiveness and efficiency of communication among public organisations and citizens.

1.5.3. While insufficient protection dwindles consumer confidence, an overly stringent protection is restrictive. Ensuring the laws in consideration are globally compatible is also important with increasing reliance of trade on data economies. Cross-border compatible data protection regimes will go a long way in creating a more predictable future for all stakeholders. For example, while underlying privacy principles are constant, interpretations and applications are diverse.

Privacy is a fundamental right only in some jurisdictions, but protected by all societies across the spectrum. Moreover, there is still an ongoing debate on the implementation of data protection regimes. Ranging from one regime for all to a sector specific bespoke approach to complete exemption for some or a combination, jurisdictions are yet to converge on the basic principles of implementation.

1.6 Impact of Data Breaches on Health and Well-Being

1.6.1. Role of data has increased at an exponential rate in our lives. From banking to education to healthcare, insurance, recreation, travel to even our grocery cart - every moment of our lives even remotely related to online presence, which itself has become ubiquitous, is being captured in the form of digital footprint by multiple applications simultaneously. This has increased our vulnerability towards privacy violations which in turn has led to dwindling trust and confidence and fears of misuse of personal data. We are under constant fear of facing personal data breachesincluding financial and identity data and thereby incurring huge financial and personal losses through cybercrimes. It is true that sometimes the data breaches occur at the organisationallevel.However, while the organisational reputation is adversely affected, for individual persons, it could be psychologically and socially detrimental. It can also lead to adverse life events such as change of location, loss of employment, adverse effects on social and personal relationships, etc. Serious lasting implications in the psychological sphere are often not discussed by organisations and regulators. However, the "knock-on" effects of a data breach cannot be ignored. The fact that the victim is not even aware of the extent of the breach puts the victim in a state of anxiety and fear which can impact her decisions for a long time in the future.

1.6.2. According to a survey by Identity Theft Resource Center, among the individuals who faced data breach:-

- 86% felt worried, angry and frustrated
- 85% experienced disturbances in their sleep habits
- 77% felt increase in stress levels
- 70% felt unsafe and were unable to trust
- 67% felt powerlessness or helplessness
- 64% faced trouble concentrating
- 59% felt sad or depressed
- 57% experienced symptoms of aches, pains, headaches and cramps
- 50% lost interest in activities or hobbies they once enjoyed

1.6.3. Medico-legal dimension of data security needs to be an integral piece of the data protection and security regime. According to clinical psychologist Professor Hugh C. H. Koch, Visiting Professor in Psychology and Law at Birmingham City University School of Law, victims of data breach face anxiety even in generalized situations like correspondence, telephone and digital communication and payment for services. Post-Traumatic Stress Disorder, commonly known as PTSD is a severe after effect of data breach, increasingly observed in victims who wrestle with feelings of helplessness and vulnerability. Stanford University Psychiatry Professor Elias Aboujaoude writes, "with every exposure you have to it (data sharing), with every reminder, you (victim) get retraumatized". Moreover, the blame attribution that comes with every breach further exacerbates the psychological impact on the victim. The Ashley Madison breach gave us a glimpse on how lives can be wrecked due to breach of data. After the data was stolen from the website which catered to adults, high-profile divorces, suicides and resignations followed taking a toll on otherwise nondescript lives.

1.7 Proliferation of Bots and Fake Accounts

1.7.1. One of the biggest issues surrounding social media today is the prevalence of fake accounts. These include accounts operated by humans in the name of other people, or fake names, multiple accounts by the same person and of course, computer operated accounts called "bots". The New York Times reported that by some calculations, as many as 48 million of Twitter's reported active users — nearly 15% are automated accounts designed to simulate real people, though the company claims that the number is far lower. In fact, in a single purge on some fake accounts and bots which Twitter did on 10th-11th July 2018, many celebrities lost millions of followers as those accounts were found fake and removed. Within that one day, Twitter's own official account lost nearly 12% of its total followers - 7.7 million fake followers.

1.7.2. The saga of fake accounts prevails on almost all platforms - including Instagram, Facebook, and Linkedin. Since Facebook and Gmail are often used to authenticate on several sites - these fake accounts lead to multiple fake identities across the web. These bots and fake accounts can push a certain agenda or person, carry malicious campaigns, promote digital scams and even conduct organised phishing and blackmailing. There is a need to stop the influx of fake accounts and bots on social media - which can be achieved only by verification of accounts under standard norms through simple measures like ID verification, submission of proof of identity, etc.

1.8 Growing Importance of Data Protection

1.8.1. The history of laws on data goes back to the 1970s reflecting worries about the advent of computers and associated technologies which built the capacity to handle and process enormous volumes of information. While various public, local and worldwide activities have sought after administrative methodologies and regulatory approaches, a noteworthy level of harmonization around the central rules exists. These include principles like the permission for any data processing activity. This could be obtained either through consent or some other justification designed to acknowledge competing private and public interests. The second common factor is related to the quality of personal data being processed. The data should be up-to-date, accurate and complete. Compliance with this principle should be mutually beneficial to both the subject of the processing and the processor.

1.8.2 The role of data security is fundamental: the objective of data security is to protect against deliberate as well as any accidental loss or destruction of data. When a data protection ecosystem is being pursued, it must be noted that appropriate data security should take into account the requirements of individual data subjects, controllers and personal data itself.

1.9 Growing Importance of Data Localisation

1.9.1. Data is core to the future of our economy and is unlike any other resource. Data is now treated as an asset, deriving implicit value generated from insights, patterns and distribution of data and its amalgamation with other data. It is available nationally and internationally, providing an impetus to the economy and innovation.

1.9.2. India's information technology (IT) sector is highly integrated in global data flows. Of the 10 most-accessed websites in India, eight are owned by US based entities and most of the data collected in interactions on these websites can currently be stored, processed or transferred anywhere in the world. IT and IT-enabled services (IT/ITeS) account for around 40% of India's exports, 65% of IT/ITeS produced in India are for global clients, and another 15% are delivered through commercial presence of our IT firms in other countries. Cross border data flow management is essential to one of the most productive sectors of the Indian economy. While there are distinct benefits from data-sharing and collaboration, there is need to take a balanced approach towards data-sharing and collaboration in view of the risks that stem from cross-border access to data.

1.9.3. Data localization is related to two strategic aspects of data: geographically located data storage and data sharing. Data localization, in broad terms, implies restrictions on the cross-border movement of data. It can have the following dimensions:

i. Residency of data within the country - data is stored only within the country and is not permitted to be transferred to any other country. This is known as hard localization.
ii. Mirroring of data - data is primarily stored in one country and available for use. However, data can also be transferred to other countries. This is known as soft localization.

1.9.4. Objectives of Data Localisation

Normally, the imposition of data localization norms can be attributed to mitigation of certain risks in cross-border flow of data and address strategic objectives. These include:

i. National security and law enforcement: In a hostile country, the data can be a tool for surveillance and manipulation of consumer behavior/opinion. Timely access to personal information by law enforcement agencies is also one major requirement.
ii. Privacy: Better informational privacy can be ensured with appropriate data protection regulations within the country.
iii. Employment generation: Data localization can provide a great boost to the data economy in the domestic market with the emergence of the data centers and other associated industries, which have the potential to create significant employment opportunities.
iv. Bargaining power: With strong presence on the internet and mammoth generation of consumer data, India can be in better position to bargain with other countries for encouraging data-based innovation for providing digital services and impetus to the digital economy.

1.9.5. Stakeholders in Data Localisation

i. Government and Law enforcement Agencies: Data localization would lead to easier access to data for the Government and law enforcement agencies, thus facilitating better law enforcement.
ii. Citizens and Residents: In the absence of data localization, any compromise with the personal data of individuals in other countries may have very few remedial opportunities to individuals. Hence, data localization norms can be very helpful in personal data and privacy protection, which is the prime objective of this Bill.
iii. Domestic IT Companies: With the appropriate data localization norms in place, Indian companies can easily avail the data storage and hosting services within India, as the data centre infrastructure in India will be substantially enhanced. IT infrastructure companies will also be

encouraged to make investments in setting up hyperscale data centres and other IT infrastructure within the country.

iv. Foreign IT Companies: These companies, while complying with the regulations, will need to setup new data centers and other IT infrastructure in the country, thus increasing their investments in India.

1.9.6. India is a strong and growing economy and many multinational companies look at India as a major data market. The international policy framework on data protection and localization policy is evolving with very few accepted principles globally. In India, the envisaged data localization norms place emphasis on regulating the cross-border movement of sensitive and critical personal data. Such movement of sensitive personal data is allowed only under certain conditions like explicit consent of the individuals, approved contractual obligations or based on permissions in specific situations, etc. Similarly, the critical personal data can be transferred outside India based on certain conditions like in requirement of emergency services or government allowing certain data transfers. The cross-border flow of sensitive personal data can take place under the regulatory framework as noted above, thus enabling continued innovation and participation in data chain management globally by the IT industry.

1.10 Data Security is Key to National Security

1.10.1. There are several instances where social media has instigated people across the globe to plan, organize and execute revolutions, protests, riots and spread violence. Individuals and organisations use social media to recruit people, connect with each other, amplify their voices, coordinate and even publicize their side of the story - actions that have the potential to change the global narrative. There are several instances where social media was used to catalyze protests against respective governments which were called spontaneous, however, they turned out to be well coordinated. In one of the most significant publicly known cyber attacks on ‘critical infrastructure’, the U.S. power grid was attacked in May, 2021 which is infamously known as ‘Colonial Grid Attack’.

1.10.2. Terrorist organizations like Al-Qaeda have been using the internet to spread their ideology, recruit terrorists and plan attacks for over a decade now. They host events and discussion forums, post provocative videos and connect with possible recruits over Facebook, Twitter and even action video games like World of Warcraft. Some of the terrorist organizations have official twitter handles as well. In addition, social media can also pose a danger to internal security and create communal and civic disharmony. For example, in April 2013, the Twitter account of Associated Press shared false news, i.e., "Breaking: Two Explosions in the White House and Barack Obama is injured." Within a few minutes, the

tweet had reached the US stock traders and the stock market fell by over 143 points, resulting in a loss of about USD 136.5 billion. Few months later, Associated Press' Twitter account was hacked by the Syrian Electronic Army and shared bogus posts. The content was pulled down within minutes but the damage was done.

1.10.3. Coming to India, in August 2012, public order suffered enormous disruptions when thousands of workers and students came to streets in the southern and the western parts of the country. This was a result of circulation of fake text messages containing warnings about communal counter attacks over ethnic clashes in the state of Assam. The Government of India blamed Google, Facebook, YouTube videos and Pakistani accounts on social media. Subsequently, the Government banned over 250 websites and social networking sites for spreading hate content. It is evident that local media has become a tool in the hands of some to spread disaffection and chaos.

1.11 Biggest Data Breaches of the 21st Century

1.11.1. The world has faced major data breaches in the digital era that seem to justify the need for a legislation for personal data protection. The list of some big data breaches around the world is as under:-

Sl. No.:	Name of the Company	Accounts Impacted	Particulars
1.	Adobe	153 million	Encrypted customer credit card records and login data of an undetermined number of user accounts were stolen.
2.	Adult FriendFinder	412.2 million	When the FriendFinder Networks, which included casual hookup and adult content websites like Adult Friend Finder, Penthouse.com, Cams.com, iCams.com and Stripshow.com, was breached, the stolen data spanned 20 years on six databases and included names, email addresses and passwords.
3.	Canva	137 million	Canva suffered an attack that exposed (not stolen) email addresses,

			usernames, names, cities of residence, and salted and hashed with bcrypt passwords (for users not using social logins — around 61 million).
4.	eBay	145 million	The attack exposed its entire account list of 145 million users including names, addresses, dates of birth and encrypted passwords. Hackers used the credentials of three corporate employees to access its network and had complete access for 229 days! Financial information, such as credit card numbers, was stored separately and was not compromised.
5.	Equifax	147.9 million	The breach compromised the personal information (including Social Security numbers, birth dates, addresses, and in some cases drivers' license numbers) of 143 million consumers; 209,000 consumers also had their credit card data exposed. That number was raised to 147.9 million in October 2017.
6.	Dubsmash	162 million	In 2018 Dubsmash had 162 million email addresses, usernames, PBKDF2 password hashes, and other personal data such as dates of birth stolen, all of which was then put up for sale on the Dream Market dark web market. The information was being sold as part of a collected dump also including the likes of MyFitnessPal, MyHeritage, ShareThis, Armor Games, and dating app Coffee Meets Bagel.
7.	Heartland Payment Systems	134 million	At the time of the breach, Heartland was processing 100 million payment card transactions per month for 175,000 merchants — mostly small- to mid-sized retailers. The attackers exploited a known vulnerability to perform a SQL injection attack.

			Security analysts had warned retailers about the vulnerability for several years, and it made SQL injection the most common form of attack against websites at the time.
8.	LinkedIn	165 million	In 2012, the company announced that 6.5 million unassociated passwords (unsalted SHA-1 hashes) were stolen by attackers and posted onto a Russian hacker forum. In 2016, it was discovered that the same hacker selling MySpace's data was found to be offering the email addresses and passwords of around 165 million LinkedIn users for just 5 bitcoins (around USD 2,000 at the time).
9.	Marriott International	500 million	Marriott International announced in November 2018 that attackers had stolen data on approximately 500 million customers. The attackers were able to take some combination of contact information, passport number, Starwood Preferred Guest numbers, travel information, and other personal information. The credit card numbers and expiration dates of more than 100 million customers were believed to be stolen.
10.	My FitnessPal	150 million	MyFitnessPal was among the massive information dump of 16 compromised sites that saw some 617 million customers' accounts leaked and offered for sale on Dream Market. In February 2018, the usernames, email addresses, IP addresses, SHA-1 and bcrypt hashed passwords of around 150 million customers were stolen and then put up for sale a year later at the same time as Dubsmash et

			al.
11.	Myspace	360 million	In 2016, 360 million user accounts were leaked onto both LeakedSource (a searchable database of stolen accounts) and put up for sale on dark web market The Real Deal with an asking price of 6 bitcoins (around USD 3,000 at the time).
12.	NetEase	235 million	It was reported that email addresses and plaintext passwords of some 235 million accounts from NetEase customers were being sold by a dark web marketplace vendor known as DoubleFlag. The same vendor was also selling information taken from other Chinese giants such as Tencent's QQ.com, Sina Corporation and Sohu, Inc.
13.	Sina Weibo	538 million	In March 2020, it was reported that the real names, site usernames, gender, location, phone numbers had been posted for sale on dark web markets. Passwords were not included, which may indicate why the data was available for just 1,799 Yuan (USD 250).
14.	Yahoo	3 billion	Yahoo announced in September 2016 that in 2014, it had been the victim of the biggest data breach in history. The attackers compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users. Yahoo claimed that most of the compromised passwords were hashed. In December 2016, Yahoo disclosed another breach from 2013 by a different attacker that compromised the names, dates of birth, email addresses and passwords, and security

			questions and answers of all of its 3 billion user accounts. The breaches eroded an estimated USD 350 million off the value of the company.
15.	Zynga	218 million	In September 2019, a Pakistani hacker by the name Gnosticplayers claimed to have hacked into Zynga's database of Draw Something and Words with Friends players and gained access to the 218 million accounts registered there. Zynga later confirmed that email addresses, salted SHA-1 hashed passwords, phone numbers, and user IDs for Facebook and Zynga accounts were stolen.

Source:https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

1.12 Proposed Framework by the World Economic Forum (WEF)

1.12.1. The Report titled "Personal Data: The Emergence of a New Asset Class"(WEF, 2011) suggests multiple frameworks to organise user-centric data protection frameworks. Some of the contours that it impresses on across frameworks are:

- User centric framework
- Culture of collaborative exchange of knowledge
- Global principles for a balanced personal data ecosystem
- Economics of personal data: Companies dealing with Big Data depend heavily on individual data of the "empowered individual".
- End user-centricity, i.e., to integrate multiple types of personal data by putting the end user around the following four key principles:
    - Transparency
    - Trust
    - Control
    - Value

1.13 Global Legal Frameworks in Data Protection:General Data ProtectionRegulation (GDPR) of the European Union (EU)

1.13.1. The global conversation on data protection and privacy is expanding, and the impact on non-EU countries is evident. This seems valid both inside Europe (Norway, Iceland, Switzerland and Liechtenstein) and outside Europe considering California's upcoming Consumer Privacy Actand South Korea's updating of its Personal Information Protection Act.

1.13.2. Advent of General Data Protection Regulation (GDPR) was a watershed moment for the European Union as it was the first formal recognition of data as an economic driver and asset class. Moreover, it has sought to inform citizens about the role of consent and its significance in data economies dominated by Big Tech and Big Data.

1.13.3. GDPR came into effect on May 25, 2018. With the intent to synchronise and establish a closely compatible data protection and privacy regime, GDPR aimed to create awareness on significance of data among the common populace of the EU. GDPR ensured that any Europeans' personal data is qualified for protection, even outside non-EU organizations. By putting the citizens at the centre of the regulatory framework, GDPR assumed significant global attention and political support.

- **Significant Features of GDPR**
    a. **Informed consent:** Most users indiscriminately click "I Agree" due to the sheer verbosity, complexity and lengthy agreement text. Commonly known as "consent fatigue", where consent form is treated as a point of friction, GDPR enforces meaningful consent by simplification of language, and deters storage of any data that is not necessary for operations.
    b. **Breach notification:** In the event of a breach, the "supervisory authority" is required to be notified within 72 hours. The overarching goal is to notify the affected users so that they can take adequate steps to protect their information. This has succeeded in increasing the rate of reporting of breaches. According to the International Association of Privacy Professionals (IAPP), the rate has more than doubled. This provision once again puts the interests of citizens at the core of GDPR framework.
    c. **Automated decision making:** Citizens now have the choice to keep their data out of automated decision making which bears legal or other significant impacts, such as profiling. Considering this will impact all algorithmic media, it also explains how algorithms profile, aggregate,

and predict using vast data sets of user profiles without any user consent.

d. **Citizen awareness:** The ultimate objective of any citizen-friendly data regime is to create awareness. With increase in reporting of cases, it is imperative that sustained efforts are to be carried out to reform the attitude of concerned citizens. According to an EU survey, Eurobarometer, 73% of Europeans have heard about at least one of their new rights. Unfortunately, seven in ten Europeans are not even aware of all of their rights.

1.14 Genesis of the Legal Mechanism to Deal with Data Protection in India

1.14.1. At present, India doesn't have a comprehensive and specific legislation on data protection, but certain guidelines on data protection can be inferred from the Information Technology Act, 2000, as amended, and rules issued thereunder, namely, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. However, given the rapid changes in the domain of internet, it was felt that the existing legislative framework for data protection is inadequate, ineffective and results in unregulated space where data companies interplay compromising the privacy of individuals and security of the country.

1.14.2. The genesis of a legal mechanism to deal with data protection in India stems from the judgment of the nine Judge Constitutional Bench of the Supreme Court, in the matter of Justice K.S. Puttaswami and another Vs. Union of India (Writ Petition No.: 494 of 2012). While delivering its judgment on 24thAugust, 2017, the Court declared "privacy" as a fundamental right under Article 21 of the Constitution. The Court further noted that the right to privacy lies at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution (Para 126) and it is not open to a citizen to waive the fundamental rights conferred by Part III of the Constitution [para 32, BashesharNath v. CIT, (1959) Supp. (1) SCR 528]. Subsequently, on 26 September, 2018, a five Judge Constitutional Bench of the Supreme Court, while delivering its final judgment in the above case, impressed upon the Government to bring out a robust data protection regime.

1.14.3. The Government of India on 31 July, 2017 constituted a "Committee of Experts on Data Protection" chaired by Justice Shri B.N. Srikrishna to examine the issues relating to data protection in the country. The aforesaid Committee examined the issues on data protection and submitted its Report to the Government on 27 July, 2018. On the basis of the recommendations made in the said Report and the suggestions received from various stakeholders, Government of India proposed to enact an appropriate legislation, namely, The Personal Data

Protection Bill, 2019 which was later introduced in the Lok Sabha on 11 December, 2019.

1.15 An Overview of The Personal Data Protection Bill, 2019 and General Discussion Thereon

1.15.1. It has been mentioned in Statement of Objects and Reasons of the Bill that the proposed legislation seeks to bring a strong and robust data protection framework for India and to set up an Authority for protecting data and empowering the citizens with rights relating to their personal data ensuring their fundamental right to privacy and protection of personal data. It would also improve ease of doing business, and facilitate more investments leading to higher economic growth, development and more job opportunities.

1.15.2. The objective of The Personal Data Protection (PDP) Bill, 2019 reads as under:

> "to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto."

1.15.3. The PDP Bill is a horizontal legislation covering both state as well as non-state entities with various obligations on the data fiduciaries and rights bestowed to individuals. The core principles of the draft legislation are as follows:

i) The two principal constituents of the Bill – data principal (natural persons or individuals providing the personal data) and the data fiduciaries (entities who collect and process the data) are in symbiotic relationship.

ii) The individuals are provided rights to confirm, correct, access, erase, and port their personal data along with the right to be forgotten.

iii) The Bill lays down guiding principles, defining contours of the compliance framework and setting up of an adjudicating mechanism for enforcement of individual's privacy rights and grievance redressal. The setting up of a Data Protection Authority, an Appellate Tribunal

and appointment of Adjudicating Officers paves the way for the implementation of the regulatory framework envisaged under the Bill.

iv) The Bill acts as an enabler for the promotion of digital growth, innovation and enterprising spirit in the economy.

1.15.4. Scheme of the Proposed Bill

The scheme of the Bill, as set out in its various provisions categorized under different chapters, is as follows:

i) The statement of Scope and Key Objects of the Act is captured in the Preamble. It identifies protection of 'personal data' for individual and informational privacy and fostering of digital economy along with the digital products and services.

ii) Chapter-I lays down the key terms and definitions along with the schedule of implementation of Act. This is followed by Chapter-II that lays down the basic principles that govern the processing of the personal data by data fiduciaries: that it should be done in a fair and reasonable manner while ensuring the privacy of the data principal, and processing should be based on free, informed and, in certain cases, explicit consent. Data minimization is another guiding principle that the Act provides for. This is followed by provisions on requirements of adequate notice and restriction on retention of data beyond the period necessary.

iii) Chapter-III carves out some categories of exceptions to the consent rule. Chapter-IV makes special provisions for processing of personal data for children.

iv) Chapter-V empowers the data principals with various rights like right to confirmation and access, correction and erasure, data portability and right to be forgotten.

v) Chapter-VI prescribes detailed provisions on transparency, accountability and security measures as also audit requirements and grievance redressal that need to be complied with by the data fiduciaries. It also covers the aspects related to Data Protection Officer and Data Protection Impact Assessment related to the significant data fiduciaries.

vi) Chapter-VII deals with the restrictions on transfer of personal data for processing outside India, especially related to sensitive and critical personal data.

vii) Chapter-VIII provides for exemptions to government and law enforcement agencies from application of various provisions of the law in certain cases. The creation of sandbox for data processing for the purposes of innovation is another feature.

viii) The other chapters in the Bill on the regulation and enforcement framework such as creation of the Data Protection Authority, penalties and compensation, adjudication framework, setting up of Appellate Tribunal and provision for appeal to the Supreme Court complete the personal data protection architecture in the Bill.

1.15.5. Salient Features of the Draft Legislation

1.15.5.1. The salient features of the Data Protection Bill, 2019 enumerated in the Statement of Objects and Reasons are as under:

(i) to promote the concepts such as consent framework, purpose limitation, storage limitation and data minimization;

(ii) to lay down obligations on entities collecting personal data (data fiduciary) to collect only that data which is required for a specific purpose and with the express consent of the individual (data principal);

(iii) to confer rights on the individual to obtain personal data, correct inaccurate data, erase data, update the data, port the data to other fiduciaries and the right to restrict or prevent the disclosure of personal data;

(iv) to establish an Authority to be called the "Data Protection Authority of India" (the Authority) which shall consist of a Chairperson and not more than six whole-time Members to be appointed by the Central Government;

(v) to provide that the Authority shall protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the proposed legislation and promote awareness about the data protection;

(vi) to specify a provision relating to "social media intermediary" whose actions have significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India and to empower the Central Government, in consultation with the Authority, to notify the said intermediary as a significant data fiduciary;

(vii) to confer a "right of grievance" on data principal to make a complaint against the grievance to the data fiduciary and if aggrieved by the decision of such data fiduciary, he may approach the Authority;

(viii) to empower the Central Government to exempt any agency of Government from application of the proposed Legislation;

(ix) to empower the Authority to specify the "code of practice" to

promote good practices of data protection and facilitate compliance with the obligations under this legislation;

(x) to appoint "Adjudicating Officers" for the purpose of adjudging the penalties to be imposed and the compensation to be awarded under the provisions of this legislation;

(xi) to establish an "Appellate Tribunal" to hear and dispose of any appeal from an order of the Authority under Clause 54 and the Adjudicating Officer under Clauses 63 and 64; and

(xii) to impose "fines and penalties" for contravention of the provisions of the proposed legislation.

1.15.6. Legislative Competence of The Personal Data Protection Bill, 2019

1.15.6.1. Article 51(c) of the Constitution, which forms part of the Directive Principles, requires the State to endeavor to "foster respect for international law and treaty obligations in the dealings of organized peoples with one another". India is a signatory to both the Universal Declaration of Human Rights and International Covenant on Civil and Political Rights which recognizes the right to privacy under Article 12 and Article 17, respectively. Further, in terms of Article 73 (1) (b) of the Constitution, the executive powers of the Union extend to the exercise of such rights, authority and jurisdiction as are exercisable by the government of India by virtue of any treaty or agreement. Thus, the Union Government has exclusive power to enact any law in accordance with its international obligations. Such power has previously been exercised by enacting the Information Technology Act, 2000 in accordance with United Nations General Assembly Resolution A/RES/51/162 and by adopting Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law.

1.15.6.2. Further, the Seventh Schedule of the Constitution provides for different entries in three Lists which separate fields of legislation into the realm of the Union Government (List I), the State Government (List II) and concurrent jurisdiction of both sets of Government (List III). The Union Government has exclusive power to make laws on "Posts and telegraphs; telephones, wireless, broadcasting and other like forms of communication" under Entry 31 of the List 1 of Seventh Schedule of the Constitution. Given the objectives, The Personal Data Protection Bill, 2019 intends to achieve, it falls within the meaning of Entry 31 of List I.

1.15.6.3. Additionally, Entry 97 of List I vests the Union Government with the power to legislate on "Any other matter not enumerated in List I or List III including any tax not mentioned in either of those Lists". These factors,

coupled with the absence of any specific Entry under List II and List III (with respect to data protection), tend to indicate that States in India do not have legislative competence over the subject of data protection and, even otherwise, the subject would fall in the residuary powers of the Union Government to legislate (Article 248).

1.15.6.4. Taking into consideration all of the above, it appears to be clear that the Union Government has the exclusive legislative competence in relation to data protection in India. Further, the Bill, drawing its intent and meaning from the fundamental right to privacy drawn out in the Puttaswamy judgement, confers certain rights on data principals which they cannot waive. Moreover, the foundation of the 2019 Bill stems from the right to privacy under Article 21 of the Constitution.

1.15.7. Overriding Effect of The Personal Data Protection Bill, 2019

1.15.7.1. It is a settled position of law that a special law shall prevail over a general and prior law (para 32, SharatBabuDigumarti vs Govt. of NCT of Delhi, AIR 2017 SC 150 – hereinafter "SharatBabuDigumarti"). The 2019 Bill, being a special law exclusively dealing with data protection, will prevail over all other general laws incidentally governing the data protection regime. Moreover, Clause 97 of the Bill provides for the overriding effect by way of a non-obstante clause. Further, the court in SharatBabuDigumarti (at para 37) has relied on prior decisions to rule that even where two statutes contain non-obstante clauses, if the legislative intendment is discernible that a latter enactment shall prevail, the same is to be interpreted in accordance with the said intention.

1.15.7.2. The Committee find that the objectives of The Personal Data Protection Bill are covered under a broad and liberal interpretation of Entry 31 of the List I of Seventh Schedule of the Constitution. As such, the Act falls within the exclusive legislative domain of the Union Government vis-a-vis the data protection regime in India. Moreover, the provisions of the 2019 Bill (once brought into force) would apply irrespective of any other law governing contractual relations between a data fiduciary and a data principal in so far as they relate to the contours of the Bill. Additionally, the Bill, being a special law containing a non-obstante clause on its applicability over other laws, would appear to govern the field of data protection in India irrespective of other pre-existing laws that may govern the subject incidentally. The Committee approve the Objects and Reasons of the Bill as these are in the nature of public policy as these suitably address the concerns that emerge out of the

Puttaswami judgment on privacy as a fundamental right and the broad recommendations of Justice B.N. Srikrishna Committee and desire that the contractual provisions must adhere to the same accordingly.

(Recommendation No. 1)

1.15.8. Regulation of Personal and Non-Personal Data

1.15.8.1. On their 37th sitting held on 24th November 2020, the Committee observed that we cannot keep non-personal data above or beyond the law or regulation. Instead, there should be different layers of protection or security on these two types of data. Besides, when we are creating Data Protection Authority, the Authority necessarily has to deal with all disputes pertaining to data protection, whether personal or non-personal. Thus, a larger umbrella of Data Protection Authority has been created in which non-personal data will also be governed by rules and regulations. Further, the Committee noted that a large volume of non-personal data is essentially derived from one of the three sets of data- personal data, sensitive personal data, and critical personal data -which has been either anonymized or has been in some way converted into non-re-identifiable data.

1.15.8.2. The Committee while considering the nature of data collection and data storage feel that there is a mass movement of data without any distinction of personal or non-personal. It is not possible to differentiate between personal or non-personal data not just in the initial stage but at later stages also. Besides, sometimes, it is the application of data that determines whether it is personal or non-personal and it is the processing that determines how data is going to be extracted or used. The Committee also feel that it is actually simpler to enact a single law and a single regulator to oversee all the data that originates from any data principal and is in the custody of any data fiduciary. This will restrict the grey area in terms of anonymisation and re-identification.

1.15.8.3. The Committee observe that to define and restrict the new legislation only to personal data protection or to name it as Personal Data Protection Bill is detrimental to privacy. The Bill is dealing with various kinds of data at various levels of security and it is impossible to distinguish between personal data and non-personal data, when mass data is collected or transported. So, the Committee opine that if privacy is the concern, non-personal data has also to be dealt with in the Bill. To avert contradiction, confusion and mis-management, single administration and regulatory body is necessitated. In Committee's view, all the data has to be dealt with by one Data Protection Authority (DPA). Since the Bill provides for the establishment of one Data

Protection Authority, we cannot have two DPAs one dealing with privacy and personal data and the other dealing with non-personal data.

1.15.8.4. **The Committee, therefore, recommend that since the DPA will handle both personal and non-personal data, any further policy / legal framework on non-personal data may be made a part of the same enactment instead of any separate legislation. As soon as the provisions to regulate non-personal data are finalized, there may be a separate regulation on non-personal data in the Data Protection Act to be regulated by the Data Protection Authority.**

(Recommendation No. 2)

1.15.9. Timeline for Implementation of the Act

1.15.9.1. With regard to the date of commencement of the Act and implementation of various provisions therein, the Committee examined the provisions of Clause 1(2) of the Bill and observed that different dates may be appointed for implementation of different provisions of the Act, but neither any specific timeline for each implementation process has been pronounced nor any time limit fixed for the implementation of the Act and its provisions.

1.15.9.2. In this regard, the Committee received various suggestions from the different stakeholders/experts, regarding incorporation of a specific timeline in the Bill for implementation of the provisions. Gist of the important/relevant points raised in the Memoranda received in this regard is as under:-

(i) A period of two years may be allowed from the notification of rules for compliance. This period should not include the time taken for the consultation process with stakeholders.

(ii) Time period may also be taken into consideration for data processors that work with foreign national data since renegotiation of international contracts may be required.

(iii) The Bill may specify a minimum period before which any provisions of the Bill become applicable and mandatory.

(iv) A gestation period of approximately two years from the date of notification of the Data Protection Act is essential to ensure collaboration amongst relevant stakeholders, having funds/manpower/processes/technologies in places and above all, for the Bill to be a success. A comprehensive analysis should be undertaken by the Government prior to notifying any portion of the Bill as regards capacity building. Also, elaborate awareness plans need to be undertaken.

(v) Implementation may be in phases, or suitable transition period may be provided where the Data Protection Bill is in force, but penalties are

not; or implementation of regulations and suitable notice period be provided.

(vi) The absence of transitional provisions in the Bill creates sizeable uncertainty for data processors and data fiduciaries about when all the provisions will come into force.

(vii) It has been global best practice to provide a transition period in comprehensive data protection bills. For instance, the European Union provided a 2 (Two) year transition period for the provisions of the General Data Protection Regulation ("GDPR") to take effect.

1.15.9.3. Many of the non-official witnesses who deposed before the Committee also raised this as an issue of concern. Most of them suggested that a specific transition time should be provided for in the Bill to avoid any uncertainty. When asked about the reason for absence of any timeframe for implementation of the Act, the Ministry of Electronics and IT submitted that flexibility has been provided in the Bill regarding the date of enforcement. The Committee differed with the view of the Ministry and had an unanimous opinion that a timeline must be provided for implementation of provisions of the Bill.

1.15.9.4. In the sitting of the Committee held on 23.11.2020, when asked for clarification in this regard, the Ministry of Law and Justice (Legislative Department) suggested for transition of time as under: "Actually, if you want to insert any specific period in the commencement clause, the right thing is, it shall come into force within 24 months from the date of its enactment provided that different dates may be appointed for different provisions of the Act and rest will continue".

1.15.9.5. After a detailed deliberation, the Committee are of the considered view that the timelines must be specific and reasonable for implementing the various provisions of the Act in order to allow the data fiduciaries and data processors sufficient time for compliance with the provisions within a timeframe.

1.15.9.6. The Committee note that Clause 1(2) of the Bill does not provide for any timeline for implementation of the Act after issue of notification. The Committee also observe that the implementation of the Act will be in phases but feel that the period for implementation of various provisions may not be too short or too delayed. Data fiduciaries and data processors would also require sufficient time for transition. No specific provision for transitional phase necessarily creates uncertainty for the concerned stakeholders. The Committee, therefore, recommend that an

approximate period of 24 months may be provided for implementation of any and all the provisions of the Act so that the data fiduciaries and data processors have enough time to make the necessary changes to their policies, infrastructure, processes etc. The Committee suggest that the phased implementation may be undertaken in order to ensure that within three months, Chairperson and Members of DPA are appointed, the DPA commences its activities within six months from the date of notification of the Act, the registration of data fiduciaries should start not later than 9 months and be completed within a timeline, adjudicators and appellate tribunal commence their work not later than twelve months and provisions of the Act shall be deemed to be effective not later than 24 months from the date of notification of this Act. While appointing the timelines for different phases and processes, a comprehensive analysis and consultation with stakeholders should be undertaken by the Government to discover/understand the technical/operational and managerial requirements for compliance of the provisions of the Bill. The Government should ensure that in the process of implementation of each phase, it should keep the legitimate interests of businesses in mind, so that it does not detract, too far, from the Government's stated objective of promoting ease of doing business in India.

(Recommendation No. 3)

1.15.10. Guiding Principles to Handle Data Breach

1.15.10.1. With reference to the actions, as laid down in the Bill, to be undertaken by the data fiduciary in the event of any data breach, the Committee suggested some amendments in Clause 25 including imposing a timeline for reporting of data breach and removal of subjective discretion of the data fiduciary concerning the reporting of any data breach to the data fiduciary. At the same time, the Committee also felt that there should be a set of guiding principles to be followed by the Data Protection Authority while framing rules and regulations concerning the Clause.

1.15.10.2. The Committee express their concern over the forms and procedures provided for reporting of instances of data breach by the data fiduciary. The Committee suggest some specific amendments at appropriate places in the existing Clause 25 of the Bill. **Simultaneously, the Committee also desire that there should be specific guiding principles to be followed by DPA while framing the regulations in this regard. The Committee desire that these guiding principles should incorporate the following points:-**

(i) The Authority while posting the details of the personal data breach under Clause 25(5) should ensure that the privacy of the data principals is protected;

(ii) Where the data principal has suffered immaterial or material harm owing to the delay in reporting of the personal data breach by data fiduciary, the burden to prove that the delay was reasonable shall lie on the data fiduciary. Also, the data fiduciary shall be responsible for the harm suffered by the data principal on account of delay of reporting of personal data breach; and

(iii) The Authority should ask the data fiduciaries to maintain a log of all data breaches(both personal and non-personal data breaches), to be reviewed periodically by the Authority, irrespective of the likelihood of harm to the data principal.

(iv) Temporary reprieve to data fiduciary may also be an area of concern when data breaches occur inspite of precautions as an act of business rivalry or espionage to harm the interest of the data fiduciary.In such cases,the Data Protection Authority may use its discretion to authorize temporary order on non-disclosure of details if it doesn't compromise the interests of data principal.

(Recommendation No. 4)

1.15.11. Mechanism to be followed when the child attains the age of majority.

1.15.11.1. Chapter IV of the Bill relates to processing of personal data and sensitive personal data of children. The Committee, in this regard, observed that the obligation should be on the part of the data fiduciary till the child attains the age of majority. The Committee, however, noted that in this Chapter, no consent option is available to the child with respect to his/her personal data when he/she attains the age of majority.

1.15.11.2. The Committee deliberated, in detail, on the protection of personal data of children. The Committee feel that the consent options may not be incorporated as amendment in the Bill, rather, being procedural matter, it may be included as regulations to be framed by DPA.

1.15.11.3. The Committee observe that in Section 16 of the Bill, there are provisions about the processing of personal data and sensitive personal

data of children, however, the Committee find that there is no mention of any procedure to be followed regarding delineating the options to be made available to the child at the stage when he or she attains the age of majority. The Committee feel it necessary that there should be rules or guidelines to be followed by the data principal regarding consent when he or she attains the age of majority i.e., 18 years. Accordingly, the Committee desire that the following provisions may be incorporated in the rules:-

(i) Data fiduciaries dealing exclusively with children's data, must register themselves, with the Data Protection Authority;

(ii) With respect to any contract that may exist between a data fiduciary or data processor and a data principal who is a child, the provisions of the Majority Act may apply when he/she attains the age of 18 years;

(iii) Three months before a child attains the age of majority, the data fiduciary should inform the child for providing consent again on the date of attaining the age of majority; and

(iv) Whatever services the person was getting will continue unless and until the person is either opting out of that or giving a fresh consent so that there is no discontinuity in the services being offered.

(Recommendation No. 5)

1.15.12. Regulation of Social Media Platforms and Intermediaries

1.15.12.1. Clause 26 of the Bill deals with classification of data fiduciaries as significant data fiduciaries and special provisions for classification of social media intermediaries, fulfilling certain criteria, as significant data fiduciaries. In this regard, the Committee had detailed discussions regarding provisions pertaining to social media platforms and the Ministry of Electronics and IT (MEITY) also made a presentation before the Committee detailing the provisions under the IT Act that regulate social media intermediaries.

1.15.12.2. The key areas of concern identified by the Committee with respect to social media intermediaries are as under:-

(i) Transparency and accountability of social media platforms;
(ii) Categorisation of such platforms as intermediaries;
(iii) Profiling of personal data by such platforms;
(iv) Instances of discriminatory use of AI by such platforms;
(v) Privacy policy of such platforms;

(vi) Ongoing investigations of such platforms in countries other than India;
(vii) Privacy and content policy of such social media intermediaries;
(viii) Intermingling of social media platforms and other OTT platforms;
(ix) Ability to influence large segment of population through the use of AI;
(x) Anonymous publication of content on such platforms;
(xi) Obscene and other illegal content;
(xii) Criteria adopted by social media platforms for removal of content;
(xiii) Code of Ethics for social media platforms.

1.15.12.3. The Committee also made a comparison between the social media platforms with print and electronic media. The Committee pointed out that print and electronic media take the responsibility for the content that they disseminate and there exist mechanisms for grievance redressal whereas, the social media platforms neither take any responsibility for the content hosted on their platforms nor is there any mechanism to regulate them.

1.15.12.4. The foremost point of concern for the Committee was that the IT Act had designated social media platforms as 'intermediaries'. In this regard, the Committee were of the view that the social media platforms may not be designated as such because, in effect, they act as publishers of content, whereby, they have the ability to select the receiver of the content, as well as control the access to any content posted on their platform. The Committee, therefore, opined that they should be made accountable for the content that they allow to be posted/hosted on their platforms. For this purpose, they should allow users to officially identify themselves and voluntary verification must be made mandatory. The Committee also took note of absence of a code of ethics for such social media platforms and the inadequacies of self-regulation.

1.15.12.5. On being questioned regarding the provisions in the IT Act for the regulation of social media intermediaries, MEITY submitted as under:-

"Any intermediary including the social media platform is expected to define their terms and conditions of usage, publish a privacy policy. They are also supposed to take down or remove unlawful content as and when unlawful activities relatable to 19(2) which is how the hon. Supreme Court in Shreya Singhal case restricted the scope of the unlawful contents being reported and being taken down provided, they also are expected to provide information to law enforcement agencies such as police, etc. They are supposed to report security incidents to computer emergency response team and they are also supposed to have a grievance officer in place. Platforms can also remove the content which is violative of the platform policies as and when reported to

them. So, while it is expected most of the times the court or the appropriate Government or the law enforcement agencies along with the corresponding law which is being violated, they will inform, but in certain cases, it is also possible that if the platform policy is being violated and if they are informed, then the call is being taken by the platforms themselves."

1.15.12.6. Responding to the observations of the Committee about the inadequate provisions for regulation of social media platforms, the MEITY submitted their future plan as under: "*The plan is that we have already started working on two fronts. One, the amendment of the intermediary rules itself which is under process as of now, including specific and additional liabilities for social media platforms and the significant social media platforms. We are asking them whether it is a significant social media platform and, of course, we are also asking to have people here in India officially representing those actual organisations". It is noted subsequently that MeitY has notified the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 on 25.02.2021. The criterion for defining the significant social media platforms was also notified by MeitY on 26.02.2021.*

1.15.12.7. The Committee observe that social media platforms have been designated as intermediaries in the IT Act and the Act had not been able to regulate social media platforms adequately because the Act has not been able to keep pace with the changing nature of the social media ecosystem. The Personal Data Protection Bill, 2019 also has very general provisions regarding social media platforms and intermediaries. But, the Committee, considering the immediate need to regulate social media intermediaries have a strong view that these designated intermediaries may be working as publishers of the content in many situations, owing to the fact that they have the ability to select the receiver of the content and also exercise control over the access to any such content hosted by them.Therefore, a mechanism must be devised for their regulation. The Committee, therefore, recommend that all social media platforms,which do not act as intermediaries,should be treated as publishers and be held accountable for the content they host. A mechanism may be devised in which social media platforms, which do not act as intermediaries, will be held responsible for the content from unverified accounts on their platforms. Once application for verification is submitted with necessary documents, the social media intermediaries must mandatorily verify the account. Moreover, the Committee also recommend that no social media platform should be allowed to operate in India unless the parent company handling the technology sets up an office in India. Further, the Committee recommend that a statutory media regulatory authority, on the lines of

Press Council of India, may be setup for the regulation of the contents on all such media platforms irrespective of the platform where their content is published, whether online, print or otherwise.

(Recommendation No. 6)

1.15.13. Enforcement of Right to be Forgotten / Erasure

1.15.13.1. Clause 18 deals with the right of the data principal regarding correction and erasure of personal data. The Committee discussed in great detail the scope of Clause 18(1) and enquired about the restrictions on the scope of Clause18(1)(d). The Committee felt that the Clause had been restricted by stating that the data principal has the right to erasure of personal data but only where 'the personal data is no longer necessary for the purpose for which it was processed' and questioned why does the data principal not have the right of erasure of all personal data.

1.15.13.2. In this regard, the MEITY deposed as under:-

"Sir, I think, this is just to ensure that there is no frivolous request. Suppose today I give data with consent to some data fiduciary for processing, let us say, there may be a Government department collecting data and tomorrow just by some motive I say you erase it now, even though the purpose is not served or processed, even then I may start asking for erasure. So, to prevent that frivolous request, a safeguard has been given that if the purpose is served then you can erase it."

1.15.13.3. The Committee deliberated on the scenarios where the erasure of an individual's data may not be possible due to legal obligations/purposes. The Committee identified that there may be instances when the data may have to be stored for a period longer than required for providing that service, for the purpose of verification and record. After considering an example wherein a data principal may furnish a false declaration for availing government benefits, the Committee opined that in such cases the right of the data principal for the complete erasure of data may not be complied with.

1.15.13.4. In this regard, the MEITY clarified that the right of the data principal under Clause 18(1) have been qualified by making them subject to 'such conditions and in such manner as may be specified by regulations'. Moreover, it was also submitted that, qualification of the right under Clause 18(1)(d) would also prevent litigations.

1.15.13.5. The Committee also sought clarity regarding the possibility of misuse of the qualification provided under Clause 18(1)(d) by data fiduciaries through denial of request for erasure by stating that it is still relevant for processing.

1.15.13.6. In their reply, MEITY illustrated the safeguards available with the data principal in other Clauses of the Bill and submitted as under:-

"If we see 18(2), so, under 18(1), if some data fiduciary rejects the request of the data principal to erase, then he has to give a reason in writing and they can go in appeal against this and under Section 18(3), they say `you erase my data'. So, this right is given to data principal under Section 18(3) that if you are not satisfied with the response of the data fiduciary, you can go in appeal and get the data erased. I would like to point out one more Section. Section 9(1) puts an obligation on data fiduciary to not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete. So, the data fiduciary is required to delete the data at the end of the processing."

1.15.13.7. Examining further, the Committee took cognizance of the fact that, if the right under Clause 18, more specifically Clause 18(1)(d) remains unqualified, then in certain cases, the financial costs associated with the erasure request, of the data principal under the said subsection, might make it unfeasible for the data fiduciary to comply with. Keeping in view the two contrary positions that emerged during the deliberations, the Committee felt that the intent behind Clause 18(1)(d) was ambiguous. The Committee also note that the operational technological systems have their own limitations and the legislation must take into account those limitations to remain effective.

1.15.13.8. The Committee find that although the individual's liberty and right to privacy is of primary concern but how far the same can be achieved depends upon multiple factors such as available technology, cost, practicability, etc. The Committee, therefore, desire that the regulatory body, the DPA which would be established under the proposed Act should evolve in line with the best practices internationally and they should frame the regulations which can really ensure that the rights of data principal could be exercised in a simple manner and at the same time the data fiduciaries could discharge those obligations in the way that is practically possible. Moreover, the DPA should also take into account the interests of the Government with regard to the obligations that it has to discharge, while framing its policies.

(Recommendation No. 7)

1.15.14. Scope for an Alternative Financial System for India

1.15.14.1. Chinese Lending-App Data Breach in India: A dangerous circuit of Chinese lending applications has been unearthed in India whereby two Chinese and several Indians have been arrested for duping gullible Indian borrowers. After the "loans for nudes" scam in China in 2016, predatory lending applications from the neighboring country are duping Indians who have run in a financial crisis due to the COVID-19 pandemic. These applications get access to the contacts database and the gallery of the phone they are installed in and use sensitive information and harass the borrower. At least 60 such loan apps available on Google Play Store were not registered or recognised by the Reserve Bank of India (RBI) as a Non-Banking Financial Company (NBFC). India's Google Play Store has several such applications owned by Chinese operators or companies including those named like other legitimate fintech companies. For instance, 'Udhaar Loan' resembles 'Udhaar', a fintech focusing on micro loans, recognised by the Government of India. Chinese micro-lending app 'MoNeed' has been accused of leaking personal details of over 350 million records of Indian users. More than 150,000 IDs of Indians were leaked on the dark web including names and phone numbers, type and model of phone, list of apps in the phone, IP addresses, etc.

1.15.14.2. While considering the suggestions received from the stakeholders, the Joint Committee took cognizance to the possible chances of breach of privacy in the financial system. One of the memoranda received stated as under:

"As of 2018, around half of all high-value cross-border payments worldwide used the SWIFT network. As of 2015, SWIFT linked more than 11,000 financial institutions in more than 200 countries and territories, who were exchanging an average of over 32 million messages per day. A series of articles published on 23 June 2006 in The New York Times, The Wall Street Journal, and the Los Angeles Times revealed a program, named the Terrorist Finance Tracking Program, which the US Treasury Department, Central Intelligence Agency (CIA), and other United States governmental agencies initiated after the 11 September attacks to gain access to the SWIFT transaction database. After the publication of these articles, SWIFT quickly came under pressure for compromising the privacy of its customers by allowing governments to gain access to sensitive personal information. In September 2006, the Belgian government declared that these SWIFT dealings with American governmental authorities were a breach of Belgian and European privacy laws."

1.15.14.3. The Committee observe that data protection in the financial sector is a matter of genuine concern worldwide, particularly when through the SWIFT network, privacy has been compromised widely. Indian citizens are engaged in huge cross border payments using the same network. The Committee are of the view that an alternative to SWIFT payment system may be developed in India which will not only ensure privacy, but will also give boost to the domestic economy.The Committee, therefore strongly recommend that an alternative indigenous financial system should be developed on the lines of similar systems elsewhere such as Ripple (USA), INSTEX (EU), etc. which would not only ensure privacy but also give a boost to the digital economy.

(Recommendation No. 8)

1.15.15. Amendments for Encouraging Innovations

1.15.15.1. The Committee observed that there is a rapid growth of data driven businesses in recent years and there is an apprehension that data protection regulations may affect start up innovations. Keeping this in mind, the Committee deliberated in detail and suggested amendments in various provisions of the Bill. Simultaneously, they also considered that in view of those amendments in the data protection law, existing laws will also require amendment.

1.15.15.2. While observing the likely impact of the later protection regulations on corporate innovation, the Committee suggest several amendments in various clauses of the Bill to protect the interests of the startups. The Committee also desire that while framing the regulations also, DPA should keep in mind the interests of startups and encourage innovations and sandbox. Moreover, the Committee also recommend that in the light of the Data Protection Act which will come into effect after this Bill is passed, to unleash the innovative potential of the people for our country and to encourage more innovations,simultaneously,the Patent Act, 1970 may also be amended.

(Recommendation No. 9)

1.15.16. Obligations of Hardware Manufacturers as Data Fiduciaries

1.15.16.1. During their deliberations, the Committee observed that in recent times, the threat to informational security was no longer exclusive to the realm

of software but had expanded to a form where data is now being stolen through physical devices itself. In this regard, the Committee found that the Personal Data Protection Bill, 2019 has not made any provision for the regulation of the data fiduciaries, who being hardware manufacturers collect data through digital devices.

1.15.16.2. The Committee also noted that the vulnerability of data leakage through devices stems from the manner in which the global supply chain has transformed. The global spread of manufacturing has increased the difficulty of regulating such threats. It was also noted that there is a real danger that individual/organizations and states inimical to India may make use of such opportunities to subvert Indian interests.

1.15.16.3. The Committee note that the current Bill has no provision to keep a check on hardware manufacturers that collect the data through digital devices. In Committee's view, with the global spread of manufacturing, it has become essential to regulate hardware manufacturers who are now collecting data alongwith the software. The Committee, therefore, desire that a new sub-clause as 49(2)(o) may be inserted to enable DPA for framing the regulations to regulate hardware manufacturers and related entities. The Committee strongly recommend that the Government should make efforts to establish a mechanism for the formal certification process for all digital and IoT devices that will ensure the integrity of all such devices with respect to data security. Moreover, emerging technologies, that have the potential to train AI systems through the use of personal data of individuals, should be certified in a manner that ensures their compliance with the provisions of the Act. To achieve these objectives, the Committee stress upon the Government that it should set up a dedicated lab/testing facility, with branches spread throughout India, that will provide certification of integrity and security of all digital devices. In the same context, the Committee specifically desire that the Government should also ensure that these labs also provide services, whereby, an individual can have his/her device certified and in case, the device does not meet specified standards of data security, approach the DPA for taking action against such manufacturer.

(Recommendation No. 10)

1.15.17. Impact of Data Localisation in India

1.15.17.1. With the evolution and growth of information technology, the world has become a global village wherein there is a seamless flow of people,

goods and data. Now, data is not merely a group of letters and figures, but it is the medium for revenue generation. Individual data is being used by various entities to understand consumer behavior and to develop various products. Thus, data has a huge economic value attached to it. But when data is to be sharedbetween various countries without restrictions, various concerns emerge with respect to national security and growth of local businesses. Notwithstanding the benefits of data sharing and collaboration, a country has to balance innovation with the risks associated with cross-border transfer of data. The key focus of data localization should to achieve legitimate goals mitigating risks – whether to national security, privacy or employment.

1.15.17.2. The Committee noted that the data collected by various countries are being used in their favour to promote own businesses and this can undermine local businesses, especially in developing and least developed countries. It has been also observed that since India has become a big consumer market, there is a large collection, processing and storage of data happening daily. Moreover, the Committee put forth their concern that though India has entered into agreement with many countries under Mutual Legal Assistance Treaty (MLAT) framework for sharing of data for investigation of crimes, the country finds it difficult to get access to data stored in other countries which in turn is delaying speedy delivery of justice and settling of cases. Hence, the Committee opined that it is imperative to store data in India and to restrict access to it by categorizing them as sensitive and critical personal data, thus giving impetus to data localisation.

1.15.17.3. Taking a cue from the analysis of the market research firm MarketsandMarkets™ which says that the global cloud storage market size is projected to grow from USD 50.1 billion in 2020 to USD 137.3 billion by 2025 at a Compound Annual Growth Rate (CAGR) of 22.3% during the forecast period, the Committee desired that India should take advantage of the opportunities that may arise in the cloud storage market. Therefore, the Committee observed that during the post COVID-19 times, huge volume of data is generated due to offer of services through online platforms and India can attract investment and generate employment opportunities by making use of such emerging trends in cloud storage market by localizing data. In this regard, an organisation in their memorandum submitted to the Committee computed the potential of job creation, investment and taxes due to data localization of four top foreign companies operating in India as under:

	Based on the similar trend in USA		Between the top four data companies - Amazon, Microsoft, Facebook, Google the potential of creating Local Data Storage in India (based on US Benchmark and Table 2)	
Economic Impact of 1 data center[1] in US (using as a benchmark)	**Construction Phase**	**Operations phase**	**Construction Phase**	**Operations phase**
Jobs created[2]	1,688	157	28,696	2,669
Wages ($ Million)	78	8	1,321	133
Local Economic Activity[3] ($ Million)	244	33	4,140	553
Taxes[4] ($ Million)	10	1	200	22

Assumptions

1) The data centre is assumed to be large in size (165,141 sf)
2) Number of jobs include direct, indirect and induced jobs.
3) To calculate local economic activity US Bureau of Economic Analysis' multiplier is used.
4) Taxes are calculated based on US Tax rates.

1.15.17.4. During the deliberations, the Committee acknowledged that Reserve Bank of India (RBI) has taken commendable steps in this regard. In view of the threats attached with the transfer of payment data between various nations, RBI on 6th April 2018 notified a mandatory rule which states, "All system providers shall ensure that the entire data relating to payment systems operated by them are stored in a system only in India. This data should include the full end-to-end transaction details / information collected / carried / processed as part of the message / payment instruction. For the foreign leg of the transaction, if any, the data can also be stored in the foreign country, if required."

1.15.17.5. The Committee understand that privacy is a fundamental right of the citizen which also empowers him or her to ensure the protection of his personal data being shared. The Committee also believe that India, being a sovereign and democratic nation, is duty bound to safeguard the privacy of its citizens while making legislations and entering into treaties with various nations. In the Committee's view, India may no more leave its data to be governed by any other country. Besides, it has also been observed that national security is of paramount importance and India can't compromise it on the ground of promotion of businesses. Therefore, the Committee feel that though there are provisions under Clause 33 and 34 for cross-border transfer of data, some concrete steps must be taken by the Central Government to ensure that a mirror copy of the sensitive and critical personal data which is already in possession of the foreign entities be mandatorily brought to India in a time bound manner.

Consequent upon the building up of proper infrastructure and establishment of Data Protection Authority, the Central Government must ensure that data localisation provisions under this legislation are followed in letter and spirit by all local and foreign entities and India must move towards data localisation gradually.

(Recommendation No. 11)

1.15.17.6. In this regard, the Committee specifically recommend that the Central Government, in consultation with all the sectoral regulators, must prepare and pronounce an extensive policy on data localisation encompassing broadly the aspects like development of adequate infrastructure for the safe storage of data of Indians which may generate employment; introduction of alternative payment systems to cover higher operational costs, inclusion of the system that can support local business entities and start-ups to comply with the data localisation provisions laid down under this legislation; promote investment, innovations and fair economic practices; proper taxation of data flow and creation of local Artificial Intelligence ecosystem to attract investment and to generate capital gains. The Committee also desire that proper utilization of revenue generated out of data localisation may be used for welfare measures in the country, especially to help small businesses and start-ups to comply with data localization norms. Besides, the Committee would also like to state that the steps taken by the Central Government must guarantee ease of doing business in India and promote initiatives such as Make in India, Digital India and Start-up India. Moreover, Government's surveillance on data stored in India must be strictly based on necessity as laid down in the legislation.

(Recommendation No. 12)

PART II

CLAUSE BY CLAUSE EXAMINATION OF
'THE PERSONAL DATA PROTECTION BILL, 2019'

2.1 The Committee during the course of Clause by Clause examination, noted certain drafting errors in the Bill. Legislative Department also agreed for the correction/language improvement for thepurpose of clarity in the relevant Clauses. The Committee suggest several modifications with the purpose of drafting improvement and the same have been placed at the end of this chapter. In other Clauses, the Committee also suggest certain modifications based on the detailed discussion which are enumerated in the succeeding paragraphs. Words and figures in bold and underlined indicate the amendments and ***(asterisks) indicate the omission suggested by the Joint Committee.

TITLE OF THE BILL

2.2 The Title of the Bill is "The Personal Data Protection Bill, 2019".

2.3 The Committee examined, in detail, the Title of the Bill *vis-à-vis* the Objects and Reasons of the Bill and the Committee in their sitting held on 12 November, 2020 observed that the Bill is dealing with various kinds of data involving various levels of security and distinguishes between personal data and non-personal data. Moreover, the data is collected as mass data and movement of data is also in mass, therefore, it is almost impossible to segregate the personal and non-personal data at every stage.

2.4 **The Committee after considering the Objects and Reasons of the Bill find that The Personal Data Protection Bill cannot privilege digital economy over data Protection. Moreover in view of the impossibility of a clear cut demarcation of personal and non-personal data and to cover the protection of all kinds of data, the Committee recommend that the Title of the Bill may be amended as "**THE (***) DATA PROTECTION BILL, 20**21**" and the Act may be called as "The Data Protection Act, 2021".**

(Recommendation No. 13)

LONG TITLE AND PREAMBLE

2.5 Long Title and Preamble of The Personal Data Protection Bill, 2019 read as under:

"A

BILL

to provide for protection of the privacy of individuals relating to their personal data, specify the flow and usage of personal data, create a relationship of trust between persons and entities processing the personal data, protect the rights of individuals whose personal data are processed, to create a framework for organisational and technical measures in processing of data, laying down norms for social media intermediary, cross-border transfer, accountability of entities processing personal data, remedies for unauthorised and harmful processing, and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.

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

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

AND 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 through digital governance and inclusion and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the Seventieth Year of the Republic of India as follows:-"

2.6 Several suggestions were received in the form of memoranda from the stakeholders on The Preamble, Short Title and Long Title of the Bill seeking amendments thereon. A gist of the suggestions is as follows:

i Focus should be on data protection rather than the digital economy.

ii The norms for social media intermediaries should not be added in the Bill andthePreamble.

iii Transition period should be provided within the Bill and a minimum of two to three years should be given to comply with the provisions of the Bill.

iv Implementation of the Bill should be phased. Time should be provided for data fiduciaries to comply with the Bill after coming into effect.

2.7 On thorough examination of the Short Title, Long Title and Preamble of the Bill, the Committee felt that the Preamble must encompass all the objectives

of the Bill and must also set out the scope and purpose of the Bill. The Committee were of the view that privacy is a primordial concern and in the digital space so far, in our country, no legislation is in place to protect the privacy and data of the people.

2.8 The Committee in the sitting held on 11 November, 2020 had observed that this is a Bill regulating the digitization process and everything that leads to digitization, and non-digitized data is not governed by this enactment.

2.9 The Committee also held the view that individual's fundamental right to privacy needs to be protected along with all kinds of developments and innovations. Further, the Committee expressed their concern regarding the usage of the term 'personal data' in entirety in the Preamble and suggested that not only personal data but all kinds of data have to be covered under this Bill so as to achieve the purpose of the Bill in entirety.

2.10 Moreover, the Authority envisaged under this Bill is called as Data Protection Authority which is empowered to look into matters relating to all aspects of data, i.e., personal data, sensitive personal data, critical personal data and non-personal data. It also determines and regulates the collection, processing and storage of data whether digitized or non-digitized.

2.11 **The Committee note that since the Bill now covers data as whole, the word "personal" should be appropriately removed from "personal data" so as to read as "data" throughout the Long Title.**

2.12 **The Committee feel that the Bill basically relates to the privacy of information pertaining to a person available in digital domain and digitized data is not governed by this Bill. The Committee, therefore, recommend to add the word "digital" before "privacy of the individuals". The Committee feel that the digital privacy has to be circumscribed and limited by nation's sovereignty, integrity and state interest and security. Therefore, the Committee, suggest the addition of phrase "to ensure the interest and security of the State" in the Long Title, and inclusion of phrases such as "of an individual" and "that fosters sustainable growth of digital products and services" in the Preamble. The Committee also note that since the expression 'social media intermediaries' in the Bill has been changed to 'social media platforms', after due consideration of the significant role played by them, the same has to be reflected in the Long Title also. Therefore, the word "intermediary" should be substituted with the word "platforms" justification for which has been given in succeeding**

paragraphs. Besides, the Committee suggest to substitute "Seventy-second Year" for "Seventieth Year" in the Preamble.

2.13 **Accordingly, the Long Title and the Preamble of the Bill may be amended as under:**

"A

BILL

to provide for protection of the ***digital****privacy of individuals relating to their personal data,* ***to****specify the flow and usage of* ***(***)*** *data,* ***to*** *create a relationship of trust between persons and entities processing the* ***(***)*** *data,* ***to****protect the rights of individuals whose* ***(***)*** *data are processed,* to *create a framework for organisational and technical measures in processing of data,* ***to****lay****(***)*** *down norms for social media* ***platforms****, cross-border transfer, accountability of entities processing* ***(***)*** *data, remedies for unauthorised and harmful processing,* ***to ensure the interest and security of the State*** *and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.*

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

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

AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals **that fosters sustainable growth of digital products and services** and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.

BE it enacted by Parliament in the **Seventy-second** Year of the Republic of India as follows:—"

(Recommendation No. 14)

CLAUSE 1 – SHORT TITLE AND COMMENCEMENT

2.14 The Short Title of the Bill reads as follows: "1. (1) This Act may be called the Personal Data Protection Act, 2019.'

2.15 **Consequent to the amendment in the Long Title and Preamble of the Bill, the Committee recommend that the Short Title of the Bill may be changed as:**

"1.(1)This Act may be called the **(***)** Data Protection Act, 20**21**."

(Recommendation No. 15)

CLAUSE 2 – APPLICATION OF ACT TO PROCESSING OF PERSONAL DATA

2.16 Clause 2 of the Personal Data Protection Bill, 2019 dealing with application of Act to processing of personal data reads as under:

"The provisions of this Act,—

(A) shall apply to—

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

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

(c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—

(i) 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

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

(B) shall not apply to the processing of anonymised data, other than the anonymised data referred to in section 91".

2.17 Several suggestions were received on the above mentioned Clause from stakeholders in the form of memoranda, a gist of which is as under:

i "Any business carried outside India" should be clarified.

ii It is unclear how the law would apply to foreign citizens and residents. The Bill may not be extended to extra territorial application to businesses outside India, except when they offer services to Indian residents/ citizens.

iii The explicit mention of "anonymized data" under the Clause may be removed.

iv Non-personal data may not be included within the scope of this Bill.

v Entities covered by sectoral regulations should be exempted from this Bill and instead be covered by the sectoral regulations only.

vi The Bill should not be retrospectively applicable for data processing where data was collected prior to the effectuation of the Act.

vii Anonymised data should be redefined to limit it to data anonymized through a process of anonymisation, which at the time was irreversible.

2.18 In this regard, Recital (26) of GDPR states as under:

"The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."

2.19 Justice B.N.Srikrishna Committee has also deliberated on this aspect and their report *inter-alia* state as follows:

"Anonymisation requires the use of mathematical and technical methods to distort data to irreversibly ensure that identification is not possible. In this aspect, anonymisation is distinct from de-identification which involves the masking or removal of identifiers from data sets to make identification more difficult. Given the pace of technological advancement, it is desirable not to precisely define or prescribe standards which anonymisation must meet in the law. It is appropriate to leave it to the DPA to specify standards for anonymisation and data sets that meet these standards need not be governed by the law because they cease to be personal data." Further the Committee recommends, "Standards for anonymisation and de-identification (including pseudonymisation) may be laid down by the DPA. However, de-identified data will continue to be within the purview of this law. Anonymised data that meets the standards laid down by the DPA would be exempt from the law."

2.20 During the examination of this particular Clause, the Committee observed that the core objective of this Bill is privacy and it is quintessential to protect non-personal data as well in order to uphold privacy.

2.21 In their sitting held on 23 November, 2019, the Committee observed that, any kind of flexibility in the legislation such as exclusion of anonymized data under the Bill may encourage manipulation or commercialization of personal data under the array of anonymisation jeopardizing the privacy of data principals. Moreover, as the name of the Act has been changed, the Committee strongly held the opinion that anonymized data should be brought under the ambit of the Bill.

2.22 **Since the Bill deals with both personal and non-personal data, the marginal heading of Clause 2 may suitably be amended as** Application of Act to processing of personal data **and non-personal data.**

2.23 **The Committee also note that the word 'person' as defined in Clause 3 (27) is quite exhaustive and feel that selective usage of words "State, any Indian company, any citizen of India or body of persons incorporated" in Clause 2 (A) (b) shall be restrictive and may lead to complications. The Committee, therefore, feel that the word 'person' may be used to replace the words 'the State, any Indian company, any citizen of India or body of persons incorporated" in Clause 2 (A) (b).**

2.24 **The Committee observe that anonymization per se necessarily has to be part of this very Bill. The Committee, therefore, recommend to remove Clause 2(B) so as to add Clause 2(d) and to modify Clause 91 accordingly. The Committee also observe that the word "stored" needs to be inserted in Clause 2 (A)(a) between the words "collected" and "disclosed" to make the clause more meaningful.**

2.25 **Accordingly, the whole Clause 2 may be amended as under:**

"2. The provisions of this Act **shall apply to**,–

(A) (***)

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

(*b*) the processing of personal data by **(***)** any person **(***)** under Indian law;

(*c*) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—

(*i*) 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

(*ii*) in connection with any activity which involves profiling of data principals within the territory of India**; and**

(d) the processing of non-personal data including anonymised personal data.

(B) (***)"

(Recommendation No. 16)

CLAUSE 3-DEFINITIONS

2.26 The Committee examined, in detail, the "Definitions" in the Bill. Suggestions were also received from the stakeholders in this regard. Gist of the memoranda received from the stakeholders "Definitions" are as follows:

i The definition of personal data should not extend to "inferences drawn from such data for the purpose of profiling".

ii Definition of 'harm' is not sufficiently clear in explaining its scope. The definition may further be subject to interpretations of 'harm' under other laws and regulations currently in force.

iii The definition of children should be restricted to 13/14/16 years of age and be reduced from 18 years.

iv The scope of sensitive personal data should be made exhaustive.

v Anonymised data should not be defined based on the irreversibility of the process.

vi DNA needs to be clarified, regarding whether it needs to form part of SPD and how it should be defined.

vii Explicit consent should be defined under the Bill.

viii A distinction between machine readable and non-machine-readable biometric data processing should be made.

2.27 The Committee considered each and every "Definition" mentioned at Clause 3 of the Bill in the light of the intent of the Bill and recommend the following amendments in various provisions:

Inclusion of Clause 3(11): Consent Manager

2.28 **The Committee find that the term "ConsentManager" has been defined as an explanation under Clause 23. The Committee desire that the Consent Manager may be defined in Chapter I under 'Definitions' and therefore, recommend an exhaustive definition of "Consent Manager" may be inserted after Sub Clause 3(10). Accordingly, the Explanation after Clause 23(5) may be omitted and consequent upon the addition of the definition of "Consent Manager", the numbering of all sub-clauses**

under Clause 3 will change accordingly. Clause 3(11) may be read as under:

"(11)Consent Manager" means a data fiduciary which enables a data principal to give, withdraw, review and manage his consent through an accessible, transparent and interoperable platform;"

(Recommendation No. 17)

Clause 3(12)- Data Auditor

2.29 **Data Auditor has been defined as, "data auditor means an independent data auditor referred to in section 29;". The Committee feel that the word 'independent' is superfluous as the same has been used in Clause 29 and as such may be deleted from the clause 3 (12). Accordingly, the renumbered Clause 3 (13) may be read as under:**

"(**13**)data auditor" means a **(***)** data auditor referred to in section 29;

(Recommendation No. 18)

Inclusion of Clause 3(14)

2.30 **The Committee find that the term 'data breach' has not been defined in the Bill anywhere whereas it has appeared number of times in various contexts of the Bill. The Committee observe that the term 'data breach' may be defined in the Bill itself.The Committee, therefore, recommend for insertion of the definition of "Data Breach" after Sub Clause 3(13) and the numbering of all sub-clauses under Clause 3 may be changed accordingly. Clause 3(14) may be now read as under:**

"(14) data breach" includes personal data breach and non-personal data breach;

(Recommendation No. 19)

Clause 3 (13)-data fiduciary

2.31 GDPR under Article 4(7) defines: " 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law."

2.32 **The Committee while considering the definition of "data fiduciary" opine that in India, Non-Governmental Organisations (NGOs) also play a significant role in the**

rural areas in terms of collection of data for various purposes. Therefore, they must also be treated as data fiduciaries and should come under the purview of this Act. Hence, the Committee suggest that the word 'a non-government organisation' may be inserted after the word 'a company' and before 'juristic entity' the renumbered Clause 3(15), as amended may be read as under:

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

(Recommendation No. 20)

Clause 3 (15)-data processor

2.33 **The Committee feel that there are Non-Governmental Organisations (NGOs) who also process data on behalf of data fiduciaries for various reasons. Therefore, they must also be treated as data processors and should come under the ambit of this legislation. Accordingly, the Committee desire that word 'a non-government organisation' may be inserted after the word 'a company'. Hence, renumbered Clause 3(17) may be amended to read as under:**

"(*17*) "data processor" means any person, including **a** State, a company, **anon-government organisation,(***)** juristic entity or any individual, who processes personal data on behalf of a data fiduciary;"

(Recommendation No. 21)

Inclusion of Clause 3(18):Data Protection Officer

2.34 **Data Protection Officer as mentioned under Clause 30 plays an important role in the proper implementation of this legislation. Therefore, the Committee are of the view that definition of "data protection officer" needs to be included under Clause 3 with reference to Clause 30. The newly added sub-clause (18) may be read as follows:**

"(18) "data protection officer" means an officer who shall be appointed by the significant data fiduciary under section 30;"

(Recommendation No. 22)

Clause 3(20): Harm

2.35 GDPR under Recital (75) talks about risks as, "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy,

unauthorized reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects."

2.36 **Considering the wide impact of the definition of "harm" and taking into account the unrestricted horizon of interpretation for the word harm that may arise in the future owing to increased technological innovation, the Committee feel that the definition of "harm" needs to be widened in order to incorporate such harms as psychological manipulation which impairs the autonomy of the person. The Committee, therefore, desire to modify 3(20) so as to add sub-clause (xi) referring psychological manipulation. The Committee also feel that there may be many more considerations to identify harms in future which may empower the government to modify this sub-clause by inclusion of other kinds of harms. Therefore, an enabling sub-clause (xii) may also be added. Consequent upon these changes in Clause (20), sub-clauses (xi) and (xii) may be added as a part of renumbered Clause 3(23) to read as under:**

"(xi) psychological manipulation which impairs the autonomy of the individual; or"

(xii) such other harm as may be prescribed;

(Recommendation No. 23)

2.37 **Modification of Clause 3 (23)**

The Committee find that sub-clause 3(23) defines 'in writing' and defines communication in electronic form with reference to Information Technology Act 2000. The Committee desire that writing should also include 'information' and despite referring any specific clause of IT Act 2000, this sub-clause should use exact words of the IT Act too to define the electronic form. After amendment the sub-clause 3(23) may be renumbered as 3(26) and be read as under:

"**(*26*)** "in writing" includes any communication **or information** in electronic form**(***) generated, sent, received or stored in media, magnetic, optical,**

computer memory, micro film, computer generated micro fiche or similar device (***);"

(Recommendation No. 24)

Inclusion of Clause 3(28) and 3(29)

2.38 **The Committee find that the words 'non-personal data' and 'non-personal data breach' have appeared in the Bill at several times but have not been either defined or explained at any place. The Committee, therefore, desire that the word 'non-personal data' may be defined and included as sub-clause 3(28) and similarly, 'non-personal data breach' may also defined and inserted as sub-clause 3(29) as under:**

"28) "non-personal data" means the data other than personal data;"

(Recommendation No. 25)

"29) "non-personal data breach" means any unauthorized including accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the confidentiality, integrity or availability of such data;"

(Recommendation No. 26)

2.39 **Inclusion of Clause 3(44)**

The Committee find that the term "social media intermediary" has been defined as an explanation to sub-clause 26(4). The Committee feel that presently most of the social media intermediaries are actually working as internet based intermediaries as well as platforms where people communicate through various socializing applications and websites. The Committee also feel that the more appropriate term for the expression 'social media intermediary' would be 'social media platform'. The Committee therefore recommend that "Social Media Platform" may be defined in Chapter I under 'Definitions. The Committee further recommend that the explanation to Clause 26(4) defining the term 'social media intermediaries' excluding the categories mentioned therein may be used to define the term 'social media platform' and inserted after Clause 3(43). Accordingly, the Explanation after Clause 26(4) may be omitted. Consequent upon the addition of the definition of "social media platform", the numbering of all sub-clauses under Clause 3 will change accordingly. Clause 3(44) may be read as under:

***(44)*"social media platform" means a platform which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;**

(Recommendation No. 27)

CLAUSE 4-PROHIBITION OF PROCESSING OF PERSONAL DATA

2.40 Clause 4 of the Bill reads as "No personal data shall be processed by any person, except for any specific, clear and lawful purposes."

2.41 With respect to Clause 4, gist of the suggestions received from experts and stakeholders is that lawful, clear and specific are not defined; so they may either be defined, or removed.

This Clause relates to prohibition of processing of personal data but its language gives a negative connotation. The Committee, therefore, desire that this Clause may be reworded to convey a better and effective sense and may be amended as under:

4. (***) <u>The processing</u> of personal data (***) by any person **(***) <u>shall be subject to the provisions of this Act and the rules and regulations made thereunder.</u>**

(Recommendation No.28)

CLAUSE 5- LIMITATION ON PURPOSE OF PROCESSING OF PERSONAL DATA

2.42 Clause 5 of the Bill reads as under:

"5. Every person processing personal data of a data principal shall process such personal data—

(a) in a fair and reasonable manner and ensure the privacy of the data principal; and

(b) for the purpose consented to by the data principal or which is incidental to or connected with such purpose, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected."

2.43 **Clause 5 deals with limitation on purpose of processing of personal data and 5(b) describes various purposes in that regard. The Committee, however, find that there is no mention of grounds for processing of personal data without consent. In Committee's view, it is very essential to mention the purpose of processing of personal data under Clause 12 as only such provision can enable the state agencies to function smoothly. The Committee, therefore, desire that in addition to other purposes mentioned in sub-clause 5(b) , the expression "or which is for**

the purpose of processing or personal data under Section 12 " may be inserted in 5(b) after the words "such purpose" . The Committee feel that the purpose limitation need to be understood in the context of purpose. Accordingly, the sub-clause 5(b), as amended, is as follows:

"(b) for the purpose consented to by the data principal or which is incidental **there**to or connected with such purpose **or which isfor the purpose of processing of personal data under section 12**, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected."

(Recommendation No.29)

CLAUSE 8 – QUALITY OF PERSONAL DATA PROCESSED

2.44 Clause 8 deals with quality of personal data processed and reads as under:

"(1)The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

(2) While taking any steps under 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 any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify such individual or entity of this fact."

2.45 A gist of the memoranda received from the stakeholders on Clause 8 is as follows:

i Data fiduciary should not have the obligation to ensure the accuracy of the data.

ii The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading, and updated, having regard to the purpose for which it is processed.

iii This obligation under Clause 8 should be deleted as a right to rectification and erasure is already provided to the data principal.

iv The requirement should be limited to reasonable efforts and not necessary efforts.

2.46 **The Committee consider that Clause 8 is a protective clause that defines the mandate of the processing of personal data. Upon examination of the Clause, the Committee feel that rather than giving the data fiduciary the freedom to act upon his/her free will to take reasonable steps to notify any non compliance of sub-clause (1), the data fiduciary has to be obliged to mandatorily notify the same.**

2.47 **The Committee also find that Clause 8(3) mentions the conditions when the data fiduciary has to notify if such data does not comply with the requirements of sub-clause (1). In Committee's view, such condition may not be sync with the provisions of Section 12 and may thus create hurdles in the smooth functioning of Government agencies processing personal data. The Committee, therefore, recommend that to ensure that the functioning of the Government agencies is not compromised, the language of the Clause 8(3) may be suitably modified and a proviso may be added to sub clause 8 (3). The Committee further desire that the phrase "take reasonable steps to" may be deleted from sub-clause (3). The amended Clause 8(3) may now be read as under:**

"(3) Where personal data is disclosed to any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the requirement**s** of sub-section (1), the data fiduciary shall **(***)** notify such individual or entity of this fact."

Provided that the provisions of this sub-sectionshall not apply where such notice prejudices the purpose of processing of personal data under section 12.

(Recommendation No. 30)

2.48 **Besides, the Committee also feel that in order to curb the seamless sharing, transfer or transmission of data between various entities and individuals especially under the garb of services, a suitable provision along with the same proviso as above may be added as Clause 8(4). It may be framed as under:**

(4) **A data fiduciary may share, transfer or transmit the personal data to any person as part of any business transaction in such manner as may be prescribed:**
Provided that the provisions of this sub-section shall not apply where such sharing, transfer or transmission of personal data prejudices the purpose of processing of personal data under Section 12.

(Recommendation No.31)

CLAUSE 9- RESTRICTION ON RETENTION OF PERSONAL DATA

2.49 Clause 9 seeks to lay down restriction on retention of personal data beyond what is necessary reads as under:

"(1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of the processing.

(2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.

(3) The data fiduciary shall undertake periodic review 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-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations."

2.50 **The Clause 9(1) specifically mentions that a data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of processing. Such provision is very restrictive and may be a big hurdle in functioning of the agencies which process the collected data multiple times for various welfare purposes. The Committee, therefore, desire that in Clause 9(1) the word 'the processing' should be deleted and it should be replaced with 'such period'. Clause 9(1) may be read as under:**

"9.(1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of **(***)** **<u>such period</u>**."

(Recommendation No. 32)

CLAUSE 11 – CONSENT NECESSARY FOR PROCESSING OF PERSONAL DATA

2.51 Clause 11 which deals with the necessity of consent for processing of personal data reads as under:

"11. (1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.

(2) The consent of the data principal shall not be valid, unless such consent is—

(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;
(b) informed, having regard to whether the data principal has been provided with the information required under section 7;
(c) specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose 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) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—
(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;
(b) in clear terms without recourse to inference from conduct in a context; and
(c) after giving him the choice of separately consenting to the purposes of operations in, the use of different categories of, sensitive personal data relevant to processing.
(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose.
(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.
(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by such data principal."

2.52 Suggestions were received from stakeholders soliciting modification of the Clause. A gist of the suggestions received in the form of memoranda is as under:

i Sensitive personal data should also be permitted to be processed for employment purposes without requiring consent.
ii Data principals should be provided a notice and opt-out option instead on relying solely on consent.
iii The withdrawal of consent should not be restricted to "valid reasons", but permissible regardless.
iv The requirement of fresh consent whenever the processing methods and the purposes for which such consent was obtained change should be set out

explicitly in the Bill.

2.53 In this regard, Justice B.N. Srikrishna Committee Report states as under:-

"Consent also must be clear, having regard to whether it communicates agreement to the relevant processing through an affirmative action that is meaningful in a given context. Thus, silence and pre-ticked checkboxes would be unlawful modes of obtaining consent. However, that does not mean that in some instances that consent cannot be implied. For example, when an association's membership form requests for details such as name, address, telephone number, professional designation, and marital status, the affirmative action of entering such details can amount to a clear expression of consent. This would depend on the context in which the form has been collected, including whether the form explains the purposes of processing this data. Here, no explicit written expression of their agreement to such processing activity needs to be given separately."

2.54 **The Committee, observe that the language of Clause 11(3)(b) is quite ambiguous and needs clarity. The Committee, therefore recommend that the language of this sub-clause must reflect the idea that the consent of data principal has to be obtained by specifying the conduct and context explicitly without circumvention of law and without any kind of implicit inferences. Accordingly, the Committee recommend that Clause 11(3)(b) may be amended as under:**

(b) in clear terms without recourse to inference **to be drawn either** from conduct (***) **or** context; and"

(Recommendation No. 33)

2.55 **Besides, the Committee also recommend that the scope of the provision under Clause 11(4) shall be extended to include denial based on exercise of choice too. Hence Clause 11(4) may suitably be modified as follows:**

"(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be,-

(i) made conditional on the consent to the processing of any personal data not necessary for that purpose; **and**

(ii) **denied based on exercise of choice."**

(Recommendation No. 34)

2.56 **Further, the Committee observe that the word "legal" in Clause 11(6) is not necessary when the objective of the said provision is to ensure the**

accountability part of withdrawal of consent by data principal to process personal data without any valid reason. Therefore, the Committee recommend to delete the word "legal" from the Clause 11(6). Similarly, words 'effects, of such withdrawal' are superfluous and omitted replacing them with one word 'same' after 'consequences for the'. The sub-clause (6) of Clause 11 may be read as under:

"(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, **(***) the** consequences for the **same (***)** shall be borne by such data principal."

(Recommendation No. 35)

CLAUSE 13– PROCESSING OF PERSONAL DATA NECESSARY FOR PURPOSES RELATED TO EMPLOYMENT ETC.

2.57 Clause 13 of the Personal Data Protection Bill, 2019 deals with processing of personal data necessary for purposes related to employment, etc. The Clause reads as under:

"13. (1) Notwithstanding anything contained in section 11 and subject to sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary for—

(a) recruitment or 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) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the 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 under the said sub-section."

2.58 Various stakeholders submitted their suggestions to the Committee on the above mentioned Clause. A gist of the memoranda received from the stakeholders on Clause 13 is as follows:

i This exception should also extend to sensitive personal data.

ii The employment relationship should be explicitly defined under the Bill or referenced to the relevant law.

iii Any other activity incidental to employment should also be included within the scope of this exemption.
iv The exemption should not be included unless it is necessary, proportionate and reasonably foreseeable by the data principal.
v The meaning of employee should include contractors, secondees or agency workers.
vi Notice should nevertheless be provided to employees.

2.59 In this regard, Article 88 of GDPR states:

"1. Member States may, by law or by collective agreements, provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees' personal data in the employment context, in particular for the purposes of the recruitment, the performance of the contract of employment, including discharge of obligations laid down by law or by collective agreements, management, planning and organisation of work, equality and diversity in the workplace, health and safety at work, protection of employer's or customer's property and for the purposes of the exercise and enjoyment, on an individual or collective basis, of rights and benefits related to employment, and for the purpose of the termination of the employment relationship.

2. Those rules shall include suitable and specific measures to safeguard the data subject's human dignity, legitimate interests and fundamental rights, with particular regard to the transparency of processing, the transfer of personal data within a group of undertakings, or a group of enterprises engaged in a joint economic activity and monitoring systems at the work place."

2.60 Further Justice B.N.Srikrishna Committee Report states, "The Committee is of the view that this ground should be extended to the following situations: (i) recruitment or termination of employment of a data principal; (ii) provision of any service to or benefit sought by an employee; (iii) verifying the attendance of an employee; or (iv) any other activity relating to the assessment of the performance of the employee. This ground should be invoked only where it involves a disproportionate or unreasonable effort on the part of the employer to obtain valid consent of the data principal, or where validity of the consent is in question due to the unique nature of the relationship between the employer and employee. This ground may be used when the type of processing activity which is required to be undertaken by the employer does not fall within any of the other grounds."

2.61 **The Committee observe that the employer can't be given complete freedom to process the personal data of employee without his or her consent for the sake of employment purposes. The Committee hold the view that the relation between employee and employer is very sensitive and should be dealt with utmost care so as no harm is caused to either of them. As employer collects all the data of its employees and there is a trust relation between them which the Committee think should be respected. Therefore, there should be equilibrium in processing of data of employee by the employer and its use/misuse of data by the employer. The employee must also be given the opportunity to ensure that his or her personal data is not being processed for unreasonable purposes. Therefore, the Committee recommend that the processing may happen if such processing is necessary or can reasonably be expected by the data principal. The Committee, therefore, recommend to add a phrase "or can reasonably be expected by the data principal" after the word "necessary". After incorporating drafting changes, the amended Clause 13(1) may be read as under:**

"13.(1)Notwithstanding anything contained in section 11 and subject to **the provisions contained in** sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary **or can reasonably be expected by the data principal** for—"

(Recommendation No. 36)

CLAUSE 14 – PROCESSING OF PERSONAL DATA FOR OTHER REASONABBLE PURPOSES

2.62 Clause 14 of The Personal Data Protection Bill, 2019 seeks to provide for other reasonable purposes for which personal data may be processed and the Clause reads as below:

"14. (1) In addition to the grounds referred to under sections 12 and 13, the personal data may be processed without obtaining consent under section 11, if such processing is necessary for such reasonable purposes as may be specified by regulations, 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 expression "reasonable purposes" may include—

(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; and
(h) the operation of search engines.

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

(a) lay down, by regulations, 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 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose."

2.63 A summary of the suggestions received from the stakeholders on Clause 14 is as follows:

i Contractual necessity should be recognized as a valid ground for nonconsensual processing of personal data.
ii Data fiduciaries should be allowed to determine the reasonability of purposes, it should not be specified by the DPA.
iii The grounds of "credit scoring", "recovery of debt" and "operation of search engines" should be removed from the ambit of reasonable purposes.
iv The grounds comprising reasonable purposes exception should be exhaustively listed within this Clause .
v Legitimate interest exception as determined by the data fiduciary should be included.
vi The exception should be proportionate and linked to the legitimate interest of the data principal. Further, the determination of additional reasonable purposes by the DPA should be determined based on the effect it has on the data principal's rights.

2.64 The Committee devoted five sittings held between 25 and 27 November, 2020 to examine the Clause 14. The Committee feel that in order to explicitly state the intent of the Clause, certain clarity is required in its formulation.

2.65 **The Committee observe that there are already several sectoral laws in place and this particular provision should not affect various legislations in force. The Committee note that the Section 14 is also an exception to**

Section 11 similar to Sections 12 and 13. The Committee feel that to keep the scheme of the Section in sync with the Act and also not to diminish the powers of the Act with respect to the other laws, the Clause should be worded similarly to Sections 12 and 13. Therefore the Committee recommend that a phrase "Notwithstanding anything contained in Section 11" may be used in place of "In addition to the grounds referred to under Sections 12 and 13" and the words "without obtaining consent under Section 11" may be deleted in sub-clause (1) of Clause 14. The Committee opine that reasonableness and legitimacy must go hand-in-hand and the same should be reflected under this Clause. The Committee feel that the consent of data principal is not required under Clause 14, since the tenet of legitimacy can ensure accountability of data fiduciary and discourage any kind of dilution of law. Hence, the Committee recommend to add the word "legitimate" before "interest" in Clause 14(1)(a), thus adding thrust upon the principle of reasonableness mentioned under Clause 14(1) and keeping in check the legitimate interest of the data fiduciary. Similarly, the Committee feel that the expression "and it is practicable' needs to be inserted in clause 14 (1) (b) and the expression "degree of any adverse effect" needs to be inserted in clause 14 (1) (c) to provide a balance between the needs of the data fiduciary to process the data vis-a-vis obtaining the consent of the data principal. Similarly, the Committee observe that 'any other similar combinationsor corporate restructuring transactions in accordance with the provisions of applicable laws' need to be included under Clause 14 (2) (c) along with mergers and acquisitions as exclusion of it is narrowing down the scope of the Clause. After incorporating all the changes, the amended Clause 14(1) and 14 (2) (c) may be reproduced as under:

14.(1) (***) **Notwithstanding anything contained in section 11,** the personal data may be processed (***), if such processing is necessary for **(***)** reasonable purposes as may be specified by regulations, after taking into consideration—

(a) the **legitimate** interest of the data fiduciary in processing for that purpose;
(b)
(b)whether the data fiduciary can reasonably be expected, **and it is practicable**to obtain the consent of the data principal;
(c) any public interest in processing for that purpose;
(d) the **degree of any adverse**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 expression "reasonable purposes" may include—

(c) mergers **(***),** acquisitions, **any other similar combinationsor corporate restructuring transactions in accordance with the provisions of applicable laws**;

(Recommendation No. 37)

CLAUSE 16 – PROCESSING OF PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

2.66 Clause 16 of the Personal Data Protection Bill, 2019 seeks to provide for obligations on data fiduciaries that process personal data of children. Considering the importance of the Clause, the Committee had in depth deliberations on Clause 16 in order to protect the rights of children and to guarantee the availability of better services. Clause 16 of the Bill reads as under:

"16. (1) Every data fiduciary shall process personal data of a child in such manner that protects the rights of, and is in the best interests of, the child.

(2) The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations.

(3) The manner for verification of the age of child under sub-section (2) shall be specified by regulations, taking into consideration—

(a) the volume of personal data processed;

(b) the proportion of such personal data likely to be that of child;

(c) possibility of harm to child arising out of processing of personal data; and

(d) such other factors as may be prescribed.

(4) The Authority shall, by regulations, classify any data fiduciary, as guardian data fiduciary, who—

(a) operate commercial websites or online services directed at children; or

(b) process large volumes of personal data of children.

(5) The guardian data fiduciary 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) The provisions of sub-section (5) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may, by regulations, specify.

(7) A guardian data fiduciary providing exclusive counselling or child protection services to a child shall not require to obtain the consent of parent or guardian of the child under sub-section (2).

Explanation.—For the purposes of this section, the expression "guardian data fiduciary" means any data fiduciary classified as a guardian data fiduciary under sub-section (4).”

2.67 A Gist of the memoranda received from the stakeholders on Clause 16 is as under:

i Age of consent may be reduced to below 18. Either bring in compliance with the US standard (13 years) or GDPR standard (13-16 years).

ii Do away with age verification requirement because it causes additional privacy risks.

iii Bar on profiling, tracking etc. should be linked to harm, significant harm, and not a complete bar on all such activities. Specifically, the application of this Clause for educational institutions requires clarification.

iv Children have the right to withdraw consent from processing even where the parent has consented to such processing and require erasure of data upon attaining majority.

v The obligation of data fiduciary should be limited to obtaining age verification and processing accordingly.

2.68 GDPR under Article 8 deals with ‘Conditions applicable to child's consent in relation to information society services’ which says,

“1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

2. The controller shall make reasonable efforts to verify in such cases that consent is given or authorised by the holder of parental responsibility over the child, taking into consideration available technology.

3. Paragraph 1 shall not affect the general contract law of Member States such as the rules on the validity, formation or effect of a contract in relation to a child.”

2.69 The Justice B.N.Srikrishna Committee Report states “At present, the Committee understands that there are two categories of data fiduciaries who may be processing personal data of children: first, services offered primarily to children (e.g. YouTube Kids app, Hot Wheels, Walt Disney); second, social

media services (e.g. Facebook, Instagram). The DPA shall have the power to notify data fiduciaries who operate commercial websites or online services directed at children, or who process large volumes of personal data of children as guardian data fiduciaries".

2.70 Besides, the same Report determines who a child is and says, "In US, COPPA allows children 13 years of age and above to consent, whereas Article 8 of the EU GDPR mandates age 16 as the threshold, though allowing leeway for states to reduce the age of consent to 13. At the same time, the CRC defines a child as below 18 years of age under Article 1. This is also the age for anyone to validly enter into a contract in India as per Section 11, Contract Act. The principled considerations for determining an age for consent are clear — protecting the child from harm while ensuring that he/ she can autonomously participate in her own development.In order to determine the cut-off age, the choice should be governed by a balance of the following factors:

(i) Principled considerations;

(ii) The maximum age of 18 and the minimum age of 13 (considered as the relevant range in most literature and comparative jurisdictions);

(iii) The need to prescribe a single threshold to ensure practical implementation.

At the moment, keeping in view the fact that the age for majority in the Contract Act is 18 and the provision of consent for data sharing is often intertwined with consent to contract, the age of 18 is recommended as the age below which a person is classified as a child for the purpose of this law. We are aware that from the perspective of the full, autonomous development of the child, the age of 18 may appear too high. However, consistency with the existing legal framework demands this formulation. Were the age of consent for contract to reduce, a similar amendment may be effected here too."

2.71 Further Justice B.N.Srikrishna Committee recommended, "A data principal below the age of eighteen years will be considered a child. Data fiduciaries have a general obligation to ensure that processing is undertaken keeping the best interests of the child in mind. Further, data fiduciaries capable of causing significant harm to children will be identified as guardian data fiduciaries. All data fiduciaries (including guardian data fiduciaries) shall adopt appropriate age verification mechanism and obtain parental consent. Furthermore, guardian data fiduciaries, specifically, shall be barred from certain practices. Guardian data fiduciaries exclusively offering counselling services or other similar services will not be required to take parental consent."

2.72 During the course of further discussions, the Committee in their sitting held on 3 December, 2020 observed that below 18 years, any data fiduciary dealing

with child's data has to give protection to that child and no untoward thing should happen to them because they may think they have grown up but they are actually children".

2.73 **The Committee note that the chapter heading and marginal heading of Clause 16 is "processing of personal data and sensitive personal data of children". However, there is no reference of sensitive personal data in the entire chapter IV. Therefore, the Committee recommend to remove the usage of expression "sensitive personal data" from chapter heading and marginal heading.**

2.74 **The Committee express their concern over using the phrase "and is in the best interests of, the child" under sub-clause 16(1) and observe that "the entire Bill is about the rights of the data principal and such qualifying phrases may dilute the purpose of the provision and give a leeway to the data fiduciary for manipulation". The Committee, therefore, recommend to delete the phrase "and is in the best interests of," from sub-clause 16(1) as the modified Clause amply serves the objective.**

2.75 **Besides, on the concept of "guardian data fiduciary", the Committee observe that the difference between a child and an adult under this law is that the right to consent is exercised by the guardian on behalf of the child. So, first of all, the term 'guardian data fiduciary' needs to be defined which may be done in the form of an Explanation. Secondly, the consent from the guardian is more important and sufficient to meet the end for which personal data of children are processed by a data fiduciary. In Committee's view, the mention of guardian fiduciary will be altogether a new class of data fiduciary and there will be no advantage in creating such a separate class of data fiduciary. Moreover, the concept of guardian data fiduciary may lead to circumvention and dilution of law too. The Committee further observe that those who are not guardian data fiduciary necessarily have to be compliant to Section 16. Also, if they all are compliant to Section 16, any exclusionary Clause within Section 16 can' be given. The Committee, therefore, recommend to remove the word 'guardian data fiduciary' from Clause 16 and to delete Clause 16(4) and 16(7) in its entirety. Consequent to modifications made in Clause 16, the Committee, propose that the subsections 16(5) and 16(6) under Clause 16 may be renumbered as 16(4) and 16(5) respectively. Also, the explanation relating to guardian data fiduciary in this Clause may also be deleted being superfluous.**

2.76 **After incorporating all the changes, chapter IV, Clause (16) may be amended as under:**

"**CHAPTER IV**

PERSONAL DATA (***) OF CHILDREN

16.(1)Every data fiduciary shall process **the** personal data of a child in such manner that protects the rights of **(***)** the child.

(2)The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations;

(3) The manner for verification of the age of child under sub-section (2) shall (***) **take** into consideration—

(a) the volume of personal data processed;

(b) the proportion of such personal data likely to be that of child;

(c) **the** possibility of harm to child arising out of processing of personal data; and

(d) such other factors as may be prescribed.

(4) (***)

(4) The(***)data fiduciary 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.

(5) The provisions of sub-section (4) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.

(7) (***)

Explanation.-(***)"

(Recommendation No. 38)

CLAUSE 17- RIGHT TO CONFIRMATION AND ACCESS

2.77 Clause 17 of the Personal Data Protection Bill, 2019 which deals with rights of data principal to confirm and access reads as under:

"17. (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) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof;

(c) a brief 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 7in relation to such processing.

(2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to a reasonable person.

(3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations."

2.78 A gist of the memoranda received from the stakeholders on Clause 17 is as follows:

i Rights of Data principals should be expanded to include the right to object to automated processing, right to object to or block processing and privacy by default.

ii Period for compliance should be provided in the Bill itself.

iii Requirement for providing list of fiduciaries should be limited to categories of data fiduciaries.

iv This right should be expanded to also obligate data fiduciaries to provide information justifying the ground under which the processing is being conducted.

v There should be a limit on the number of times and the reasons for which the data principal seeks information under this Clause to ensure only genuine requests need to be considered by the data fiduciaries.

2.79 GDPR under Recital (27) states "This Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons."

2.80 **The Committee observe that there is no mention of the rights of a deceased data principal in the Bill. The Committee, therefore, recommend that a suitable provision may be added under Clause 17 which empowers the data principal to exercise his or her right to decide how his or her data has to be dealt with in case of casualty/death. Accordingly, the Committee desire that a separate sub-clause (4) should be added to Clause 17 which may be read as under:**

(4) The data principal shall have the following options, namely:-
(a) to nominate a legal heir or a legal representative as his nominee;
(b) to exercise the right to be forgotten; and
(c) to append the terms of agreement,
with regard to processing of personal data in the event of the death of such data principal.

(Recommendation No. 39)

CLAUSE 19 – RIGHT TO DATA PORTABILITY

2.81 Clause 19 of The Personal Data Protection Bill, 2019 which deals with the data principal's right to port personal data to any data fiduciary reads as follows:

"19. (1) Where the processing has been carried out through automated means, the data principal shall have the right to—

(a) receive the following personal data in a structured, commonly used and machine-readable format—

(i) the personal data provided to the data fiduciary;

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

(iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and

(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) The provisions of sub-section (1) shall not apply where—

(a) processing is necessary for functions of the State or in compliance of law or order of a court under section 12;

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

2.82 A gist of the memoranda received from the stakeholders on Clause 19 is as follows:

(i) Right to data portability should extend to all data and not be limited to automated processing and large entities.

(ii) The exceptions under Clause 19(2) should also include a clarification of state exceptions and include IPR along with trade secrets.

(iii) Portability rights should not be extended to inferred, processed, derived data (under Clause 19(1)(ii) and (iii)).

(iv) The meaning of 'machine readable' may be clarified.

(v) The meaning of 'trade secret' may be clarified.

2.83 With respect to data portability, GDPR under Article 20 states as under:

"1.The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:

the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); andthe processing is carried out by automated means.

2.In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

3.The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

4.The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

2.84 Besides, Justice B.N.Srikrishna Committee Report says "…the right to data portability is critical in making the digital economy seamless. This right allows data principals to obtain and transfer their personal data stored with a data fiduciary for the data principal's own uses, in a structured, commonly used and machine readable format. Thereby, it empowers data principals by giving them greater control over their personal data. Further, the free flow of data is facilitated easing transfer from one data fiduciary to another. This in turn improves competition between fiduciaries who are engaged in the same industry and therefore, has potential to increase consumer welfare. As the right extends to receiving personal data generated in the course of provision of services or the use of goods as well as profiles created on the data principal, it is possible that access to such information could reveal trade secrets of the data fiduciary. To the extent that it is possible to provide such data or profiles without revealing the relevant secrets, the right must still be guaranteed. However, if it is impossible to provide certain information without revealing the secrets, the request may be denied."

2.85 **The Committee observe that Clause 19(2)(b) provides scope for several data fiduciaries to conceal their actions by denying data portability under the garb of non-feasibility or trade secret. Moreover, the definition of trade secret can't be formulated under this Bill since it's a dynamic concept, differs from domain to domain and subjected to evolution of technology. The Committee, therefore, understand that trade secret cannot be a ground for anyone to deny data portability and data can only be denied on the ground of technical feasibility which has to be strictly determined by the regulations laid down in this regard. Accordingly, sub-clause (2) (b) of Clause 19 may be amended and Clause 19(2) of the Bill may be amended as under:**

"(2) The provisions of sub-section (1) shall not apply where—

(a) processing is necessary for functions of the State or in compliance (***) **with any judgement** (***) or order of (***) **any court, quasi-judicial authority or Tribunal** under section 12;

(b) compliance with the request in sub-section (1) would **(***)** not be technically feasible**,as determined by the data fiduciary in such manner as may be specified by regulations.**

(Recommendation No. 40)

CLAUSE 20– RIGHT TO BE FORGOTTEN

2.86 The Clause relating to the Rights to be Forgotten reads as under:

"20. (1) The data principal shall have the right to restrict or prevent the continuing disclosure of his personal data by a data fiduciary where such disclosure—

(a) has served the purpose for which it was collected or is no longer necessary for the purpose;

(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or

(c) was made contrary to the provisions of this Act or any other law for the time being in force."

2.87 The following suggestions were received from the stakeholders on Clause 20:

i The nature and scope of the right to be forgotten, including the enforcement measures should be specified in the Bill.

ii There should be a timeline prescribed for the Privacy Officer to decide the application for the right to be forgotten.

iii Right to be forgotten should be limited to only Personal Data shared by Data principal, subject to other legal provisions pertaining to maintaining of records. Intellectual Property Rights acquired by the Data Fiduciary should be removed from the purview of this Clause .

iv These obligations should not apply to collection of information by banks and financial institutions.

v There is an inadvertent typographical error in Clause 20(3) i.e., the phrase "having regard to" ought to be "have regard to".

vi An exception for establishing, exercising or defending legal claims may be added.

vii The language should include an exception of the data that is in anonymised or deidentified form.

2.88 In this regard, Justice B.N.Srikrishna Committee Report had recommended as under: -

"The right to be forgotten may be adopted, with the Adjudication Wing of the DPA determining its applicability on the basis of the five-point criteria 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 or whether the disclosure is a matter of public record; further, the right should focus on restricting accessibility and not content creation)..
The right to be forgotten shall not be available when the Adjudication Wing of the DPA determines upon conducting the balancing test that the interest of the data principal in limiting the disclosure of her personal data does not override the right to freedom of speech and expression as well as the right to information of any other citizen."

2.89 GDPR under Article 17 deals with Right to erasure ('right to be forgotten') which states as under:

"1.The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) for the establishment, exercise or defence of legal claims."

2.90 **The Committee note that Clause 20(1) and Clause 20(2) give the right to the data principal to prevent or restrict the continuing disclosure of his or her personal data. In Committee's view the expression "disclosure" alone can't serve the purpose for which the right to be forgotten is conferred to the data principal. The Committee observe that if right to be forgotten as envisaged under this sub-clause means restriction or prevention of disclosure of personal data, then even after exercising this right, his or her personal data can be processed in varied forms without disclosing the data with anybody. The Committee, therefore, recommend that the along with the word "disclosure", the word "processing" should also be added to make this clause more comprehensive and meaningful. The Committee also recommend that the provision under sub-clause (2) may be further clarified by denoting that the right of the data fiduciary to retain, use and process data are in accordance with the provisions of this Act and the rules and regulations made thereunder. Accordingly, the modifications may be carried out in the sub-clauses (1), (2), (3) and (4) of Clause (20) and the amended Clause 20 may be read as under:**

"20.(1) The data principal shall have the right to restrict or prevent the continuing disclosure **or processing** of his personal data by a data fiduciary where such disclosure **or processing**—

(a) has served the purpose for which it was collected or is no longer necessary for the purpose;

(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or

(c) was made contrary to the provisions of this Act or any other law for the time being in force.

(2) The rights under sub-section (1) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (a), (b) or **(***)**(c) of that sub-section:

Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure **or processing** of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen**or the right of the data fiduciary to retain, use and process such data in accordance with the provisions of this Act and the rules and regulations made thereunder.**

(3) The Adjudicating Officer shall, while making an order under sub-section (2), have regard to—

(a) the sensitivity of the personal data;

(b) the scale of disclosure **or processing** 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 disclosure **or processing** and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures **or processing** of the relevant nature were to be restricted or prevented.

(4) Where any person finds that personal data, the disclosure **or processing** of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2), does not satisfy the conditions referred to in that sub-section **any longer**, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order.

(5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal **under section 73.**

(Recommendation No. 41)

CLAUSE 21 – GENERAL CONDITIONS FOR THE EXERCISE OF RIGHTS OF DATA PRINCIPAL

2.91 Clause 21 dealing with the general conditions for the exercise of the rights in Clauses 17 to 20 and reads as follows:

"21. (1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a consent manager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.

(2) For complying with the request made under sub-section (1), the data fiduciary may charge such fee as may be specified by regulations:

Provided that no fee shall be required for any request in respect of rights referred to in Clause (a) or (b) of sub-section (1) of section 17 or section 18.

(3) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations.

(4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal 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 by regulations.

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

2.92 A gist of the Memoranda received on Clause 21 is as under:

i Clarity and regulatory oversight needed for role and need for consent managers.

ii There should be no or nominal fee.

iii Appointment of authorized representative to exercise these rights.

2.93 **The Committee feel that sub-clause (5) of Clause 21 gives arbitrary powers to data fiduciary to reject the request made by the data principal. In order to prevent any unnecessary refusal of such request, the Committee recommend to insert a proviso for Clause 21(5) empowering the Authority to make the regulations to determine the rationale behind any denial of the request made by the data principal. Accordingly, a new proviso to Clause 21(5) may be added and the sub-clause may be read as under:**

"(5) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act: **Provided that the data fiduciary shall, subject to such conditions as may be specified by regulations, be obliged to comply with such request made by the data principal."**

(Recommendation No. 42)

CLAUSE 22 – PRIVACY BY DESIGN POLICY

2.94 Clause 22 of the Personal Data Protection Bill, 2019 deals with Privacy by Design policy. Clause 22 (3) of the Personal Data Protection Bill, 2019 reads as under:

"(3) The Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1)."

2.95 In this regard, the following suggestions were received from the stakeholders:

i Privacy by Design certification should not be mandatory.
ii Authority should provide uniform guidelines for Privacy by Design policy.
iii The obligation to implement measures and the policy as stipulated in the 2018 Bill should be reinstated.
iv Procedure for certification should be clarified under the Bill. An independent auditor/certifying authority may also be recognized to provide certification under the Bill.

2.96 **The Committee are of the considered view that certification of the privacy by design policy by the Authority or an officer should not be a tedious process and must not hamper the growth of Micro, Small and Medium Enterprises. Sub-clause (3) of Clause 22 in present shape is ambiguous and is not in consonance with sub-clause (2).The Committee, therefore, recommend that sub-clause (3) of Clause 22 be amended to provide for the Authority the avenue to make regulations to grant exceptions to data fiduciaries below a certain threshold. Accordingly, Clause 22 (3) may be amended as under:**

"(3) **Subject to the provisions contained in sub-section (2),** the Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1)."

(Recommendation No. 43)

CLAUSE 23-TRANSPARENCY IN PROCESSING OF PERSONAL DATA

2.97 Clause 23 of the Personal Data Protection Bill, 2019, dealing with transparency in processing of personal data, along with Explanation, reads as under:

"23. (1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations—

(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 the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;

(e) the right of data principal to file complaint against the data fiduciary 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 sub-section (5) of section 29;

(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 regulations.

(2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.

(3) The data principal may give or withdraw his consent to the data fiduciary through a consent manager.

(4) Where the data principal gives or withdraws consent to the data fiduciary through a consent manager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.

(5) The consent manager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.

Explanation.—For the purposes of this section, a "consent manager" is a data fiduciary which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform."

2.98 A gist of the Memoranda received on Clause 23 is as under:

i Clarification may be provided regarding the role and meaning of consent managers within the law, as they technically function like processors, though the law assigns them the role of data fiduciaries.

ii Time period for which the information may be obtained should be specified.

2.99 **The Committee, in order to ensure transparency of algorithms used by various entities for processing of personal data and to prevent its misuse, recommend to add a provision as sub-clause 23(1)(h) and in order to clarify the scope of Clause 23(1), sub-clause (h) may be renumbered as (i) and the same needs to be modified as mentioned below:**

"(h) where applicable, fairness of algorithm or method used for processing of personal data; and

(**i**) any other information as may be specified by regulations**."**

(Recommendation No. 44)

2.100 **Consequently, the original sub-clause (h) shall become sub-clause (i) of Clause (23). Since the explanation regarding "consent manager" provided under Clause 23 has been removed to be placed under Definitions Clause, the Committee recommend to delete the same from Clause 23.**

(Recommendation No. 45)

CLAUSE 25-REPORTING OF PERSONAL DATA BREACH

2.101 Clause 25 of the Personal Data Protection Bill, 2019 which deals with reporting of personal data breach reads as under:

"25. (1) Every data fiduciary shall by notice inform the Authority about the breach of any personal data processed by the data fiduciary where such breach is likely to cause harm to any data principal.

(2) The notice referred to in sub-section (1) shall include the following particulars, namely:—

(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) action being taken by the data fiduciary to remedy the breach.

(3) The notice referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period 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 specified 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 a notice, 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 and to 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 website."

2.102 A gist of the Memoranda received on Clause 25 is as under:

i Default notification of personal data breach to the data principal –a narrow list of exceptions may be created to this rule.

ii Breach notification should not be contingent on likelihood of harm.

iii Onus on unreasonable delay in breach notification should be on the data fiduciary.

iv Personal data breach notification under Clause 25(3) should be without undue delay, and not based on period specified by DPA.

v Proviso should be added to 25(1) to limit the breach reporting mandate to when data was not encrypted according to prevalent standards.

vi All breaches should be logged by the data fiduciary and DPA may take periodic review of the data fiduciary.

vii Reporting requirements should also extend to data processors.

viii All competent authorities should be notified of data breaches.

ix Time restrictions may be imposed for reporting data breaches.

x Data fiduciaries should be indemnified if the DPA decides that data principals need not be notified.

2.103 In this regard, GDPR Recitals (85), (86) and (87) state as under: -

"(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant

economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication."

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation." And Recital 88 reads as "In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach."

2.104 On the issue of breaches of personal data Justice B.N.Srikrishna Committee Report states as follows:

"With large amounts of data being held by fiduciaries, the breach of personal data becomes a real possibility. A breach can have deleterious consequences for individuals whose personal data has been subject of the breach. Therefore, it becomes important to inform data principals about such instances so that they can take suitable measures to shield themselves from their harmful consequences. However, due to considerations of adverse publicity and avoidance of liability, fiduciaries may be dis-incentivised from reporting incidents of breach to individuals. Thus, a notification to the DPA upon the occurrence of a breach has been envisaged, in keeping with trends in other jurisdictions, before a notification to the individual is made. It may be noted that such personal data breaches that are subject to obligations of notification should not be confused with breaches of data protection law generally."

2.105 The Report further states that in order to avoid the notification of relatively benign breaches of personal data, only such breaches will have to be notified that pose a likelihood of harm to the rights of data principals.

2.106 Besides the report also states as under:-

"Upon notification, the DPA shall have the power to decide the severity of the breach and if relevant, the manner in which it needs to be reported to the individuals whose data has been breached. The breach should be notified to the individuals in instances where such a breach not only poses harm to the data principals, but also where some action is required on part of the principals to protect themselves from the consequences of the breach. The DPA has been granted the powers to determine when and how such notification is required to prevent the fiduciary from making a unilateral decision in this regard which may be motivated by factors other than best interests of the data principals. Further, the DPA is expected to better guide the actions of the data fiduciary and suggest or direct remedial measures, and it must be ensured that liability for the breach is suitably accorded in an adjudication action Failure to notify a breach would make the fiduciary liable to penalty under the provisions of the data protection law."

2.107 **Since the current Bill deals with both personal and non-personal data, the Committee recommend that the marginal heading of Clause 25 may be suitably amended as "Reporting of data breach" instead of "Reporting of personal data breach".**

2.108 **The Committee are of the view that the use of word 'likely' under sub-clause (1) of Clause 25 is presumptive. Since the most important obligation of a data fiduciary, under this chapter i.e., Chapter VI is to maintain the security of the data, the Committee feel that the carve outs which lead to ambiguity should be omitted. Hence the Committee recommend to remove the phrase "where such breach is likely to cause harm to any data principal" from sub-clause (1) of Clause 25. Clause 25(1) as amended reads as follows:**

"25.(1) Every data fiduciary shall by notice,**(***) report to** the Authority about the breach of any personal data processed by (***) **such** data fiduciary.**(***)"**

2.109 **Further, the Committee opine that the form of notice mentioned under sub-clause (2) for the use of data fiduciary to report the data breach to Authority may be specified by regulations rather than restricting the scope of the form within this legislation itself. Accordingly, a phrase "be in such form as may be specified by regulations and" may be included before the word "include" in sub-clause (2).**

2.110 **Besides, the Committee feel that text of sub-clause 2(d) needs to be revised to explicitly state that the notice must include particulars of the remedial actions taken by the data fiduciary for the data breach. Therefore, the Committee recommend to amend the framing of sub-clause 2(d) of Clause 25 as follows:**

"(d) **the remedial actions** being taken by the data fiduciary **(***) for such** breach."

2.111 **Sub-clause (3) is too general and does not mention any specific timeline so that the data fiduciary is obliged to report a data breach. The Committee feel that there should be a realistic and finite time frame to follow the same and to report a data breach to the Authority by the data fiduciary. The Committee, therefore, recommend that Clause 25(3) should provide a time period of 72 hours for reporting of data breach under sub-clause (1). Hence, sub-clause (3) is amended to read as below:**

"(3) The notice referred to in sub-section (1) shall be **(***) issued** by the data fiduciary **within seventy-two hours of becoming aware of such breach.(***)"**

2.112 **The Committee also note that sub-clause (5) in the present form doesn't put any obligation on the data fiduciary to report personal data breach to the data principal. Moreover, the Committee observe that it's not**

advisable to report all kinds of data breach to data principal without informing the Authority. The Committee are of the view that some data breach reports may create panic among the citizens and also affect public law and order if reported to every data principal without analyzing the exact harm to a specific data principal. Furthermore, the genuineness of trust between an individual and an entity can be questioned due to the reporting of every kind of personal data breach to data principal. Therefore, the Committee, feel that the Authority must first of all take into account the personal data breach and the severity of harm that may be caused to such data principal and shall direct the data fiduciary to report the data principal about data breach and to take appropriate remedial measures. It is also suggested that a proviso may be added to sub-clause (5) so that the Authority can direct the data fiduciary to adopt urgent measures to mitigate any harm. Accordingly, sub-clause (5) may be amended and the provision under sub-clause (6) with respect to the steps to be taken by the data fiduciary and the provision under sub-clause (7) regarding posting of details of personal data breach on the website of Authority may be incorporated under sub-clause (5) itself. Consequent upon the merger of sub-clause (6) and sub-clause (7) under sub-clause (5), the provisions under sub-clause (6) and sub-clause (7) of Clause 25 may be deleted. After incorporating all these suggestions, the sub-clause (5) of Clause 25 may now read as under:

"(5) The Authority **(***)shall, after taking into account the personal data breach and the severity of harm that may be caused to the data principal,** direct the data fiduciary to **report such breach to the data principal and** take appropriate remedial actions**(***) to mitigate such harm** and to conspicuously post the details of the personal data breach on its website.

Provided that the Authority may direct the data fiduciary to adopt any urgent measures to remedy such breach or mitigate any harm caused to the data principal."

2.113 **Finally, since the Bill deals with both personal and non-personal data, the Committee recommend that suitable provision may be provided in the Bill itself to deal with the reporting of non-personal data breach. Hence a new sub-clause (6) may be inserted as Clause 25(6) with a text as under:**

"(6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed."

2.114 **After incorporating all the above mentioned suggestions, the Committee desire that complete Clause 25 may be amended as under:**

"25.(1) Every data fiduciary shall by notice,**(***) report to** the Authority about the breach of any personal data processed by (***) **such** data fiduciary.**(***)**

(2) The notice referred to in sub-section (1) shall **be in such form as may be specified by regulations and** include the following particulars, namely:—

(a) nature of personal data which is the subject matter of the breach;

(b) number of data principals affected by **(***) such** breach;

(c) possible consequences of **(***) such** breach; and

(d) **the remedial actions** being taken by the data fiduciary **(***) for such** breach.

(3) The notice referred to in sub-section (1) shall be **(***) issued** by the data fiduciary **within seventy-two hours of becoming aware of such breach.(***)**

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

(5) (***)

(5) The Authority **(***)shall, after taking into account the personal data breach and the severity of harm that may be caused to the data principal,** direct the data fiduciary to **report such breach to the data principal and** take appropriate remedial actions**(***) to mitigate such harm** and to conspicuously post the details of the personal data breach on its website.

Provided that the Authority may direct the data fiduciary to adopt any urgent measures to remedy such breach or mitigate any harm caused to the data principal.

(7) (***)

(6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed."

(Recommendation No. 46)

CLAUSE 26 – CLASSIFICATION OF DATA FIDUCIARIES AS SIGNIFICANT DATA FIDUCIARIES

2.115 Clause 26 of the Personal Data Protection Bill, 2019 dealing with classification of data fiduciaries as significant data fiduciaries reads as follows:

"26. (1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—

(a) volume of personal data processed;

(b) sensitivity of personal data processed;

(c) turnover of the data fiduciary;

(d) risk of harm by processing by the data fiduciary;

(e) use of new technologies for processing; and

(f) any other factor causing harm from such processing.

(2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations.

(3) Notwithstanding anything in this Act, if the Authority is of the opinion that any processing by any data fiduciary or class of data fiduciary carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations specified in sections 27 to 30 to such data fiduciary or class of data fiduciary as if it is a significant data fiduciary.

(4) Notwithstanding anything contained in this section, any social media intermediary,—

(i) with users above such threshold as may be notified by the Central Government, in consultation with the Authority; and

(ii) whose actions have, or are likely to have a significant impact on electoral democracy, security of the State, public order or the sovereignty and integrity of India, shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary:

Provided that different thresholds may be notified for different classes of social media intermediaries.

Explanation.—For the purposes of this sub-section, a "social media intermediary" is an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services, but shall not include intermediaries which primarily,—

(a) enable commercial or business oriented transactions;

(b) provide access to the Internet;

(c) in the nature of search-engines, on-line encyclopedias, e-mail services or online storage services."

2.116 A summary of the suggestions received from stakeholders on Clause 26 is as under:

i Notification of social media intermediaries should be as per a procedure and thresholds should be clarified.

ii Social media intermediaries may not be notified by the central government, but by the DPA and further the power to do so already exists with the DPA under 26(1).

iii S.26(4) w.r.t. social media intermediaries may be removed from the Bill because it is outside the ambit of the Bill.

iv State agencies should be subject to obligations of significant data fiduciaries.

v Significant data fiduciaries application to processors should also be clarified. They may be considered to be covered under significant data fiduciaries as well.

2.117 During in depth examination of Clause 26, the Committee noted that today social media intermediaries are above the sovereign and they lay down boundaries which circumscribe the operation of the sovereign. Moreover, the social mediaintermediaries are not actually intermediaries but they are platforms that do the dual functions of an intermediary and a platform.

2.118 **The Clause 26(4) describes "social media intermediary" as an intermediary that facilitates online interaction between two or more users and allows users to disseminate media, while e-commerce internet service providers, search engines and email services are excluded from the definition. In Committee's view presently most of the social media intermediaries are actually working as internet based intermediaries as well as platforms where people communicate through various socializing applications and websites. The Committee therefore, would first of all recommend to replace the expression 'social media intermediary' by 'social media platform' and it may be incorporated as 26(1)(f) as one of the factors for the purpose of classification of data fiduciaries as significant data fiduciaries. After the incorporation of all these changes the amended Clause 26(1)(f) may be reproduced as under:**

"(f) any social media platform-

(i) with users above such threshold as may be prescribed, in consultation with the Authority; and

(ii) whose actions have or are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order:

Provided that different thresholds may be prescribed for different classes of social media platforms;"

2.119 **Moreover, the Committee feel that there is an urgent need to curb the misuse of children's data which compromises the data of parents as well. The Committee, therefore, desire that in order to discourage such mishandling of data, those data fiduciaries which use data to process or to provide services to children should be brought under the ambit of Clause 26 as significant data fiduciaries by inserting Clause 26(1)(g) as one of the factors having text as under:**

"(g) the processing of data relating to children or provision of services to them; or"

2.120 **In Clause 26(1)(f) the Committee have replaced the word "social media intermediary" as "social media platform". Also, the term social media platform has been defined in Clause 3 (44) using the terms given in the explanation excluding various categories. The Committee, therefore, recommend that Clause 26(4) along with the Explanation may be deleted.**

2.121 **Further, the Committee also understand that the significant data fiduciaries have to be regulated under the sectoral regulations also and they need to be very transparent and accountable. Therefore, the Committee recommend that a new provision may be inserted as Clause 26(4) to explicitly deal with sectoral regulation of significant data fiduciaries.**

2.122 **Consequent to above modifications, Clause 26(1)(f) of the original Bill should be changed as Clause 26(1)(h).**

2.123 **After the incorporation of all the changes, Clause 26, as amended may be read as under:**

"**26.**(1) The Authority shall, having regard to the **any of the** following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—

(a) volume of personal data processed;

(b) sensitivity of personal data processed;

(c) turnover of the data fiduciary;

(d) risk of harm by processing by the data fiduciary;

(e) use of new technologies for processing; **(***)**

(f) any social media platform-

(i) with users above such threshold as may be prescribed, in consultation with the Authority; and

(ii) whose actions have or are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order:

Provided that different thresholds may be prescribed for different classes of social media platforms;

(g) the processing of data relating to children or provision of services to them; or

(h)any other factor causing harm from such processing.

(2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations.

(3) Notwithstanding anything **contained** in this Act, if the Authority is **(***) satisfied** that any processing by any data fiduciary or class of data fiduciar**ies** carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations **(***)provided** in sections 27 to 30 to such data fiduciary or class of data fiduciar**ies,** as if it is a significant data fiduciary.

(4) (***)

(4) Subject to the provisions contained in section 56, the significant data fiduciary shall be regulated by such regulations as may be made by the respective sectoral regulators.

(Recommendation No. 47)

CLAUSE 28 – MAINTENANCE OF RECORDS

2.124 Clause 28 of the Personal Data Protection Bill, 2019 seeks to require significant data fiduciaries to maintain accurate and up-to-date records, including requiring significant social media intermediaries to provide for voluntary verification mechanism. The Clause reads as under:

"28. (1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:—

(a) important operations in the data life-cycle including collection, transfers,and erasure of personal data to demonstrate compliance as required under section 10;

(b) periodic review of security safeguards under section 24;

(c) data protection impact assessments under section 27; and

(d) any other aspect of processing as may be specified by regulations.

(2) Notwithstanding anything contained in this Act, this section shall also apply to the State.

(3) Every social media intermediary which is notified as a significant data fiduciary under sub-section (4) of section 26 shall enable the users who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.

(4) Any user who voluntarily verifies his account shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed."

2.125 A gist of the Memoranda received on Clause 28 is as under:

i Clause 28(4) regarding social media intermediaries may be deleted.

ii Documentation on automated decision-making processes may be included within the ambit of record keeping requirements.

iii 'important operations' may be explained for greater clarity under Clause 28(1).

iv Record keeping may be extended to all data fiduciaries.

2.126 The committee observed that social media platforms have to be brought within the ambit of the law of the land wherein the State has an exclusive right over them. During the sitting held on 10 December, 2020, the Committee observed that there should be some sectoral regulation on social media intermediaries in the same lines as defined under IT Act. The Committee noted that the notice and takedown procedures in India (for defamatory and obscene content, for instance) has been seentobe problematic as it now appears that intermediaries have become private censors determining right to freedom of speech. Moreover, in Shreya Singhal v. Union of India judgment, the Supreme Court of India in 2015 held that under the IT Act, intermediaries are required to take down content where they have been notified of objectionable content by the government or through a court order. Considering the role played by social media intermediaries as publishers, the Committee feel that verification of social media accounts by users should be facilitated by the intermediaries and in case of any unverified accounts, social media intermediaries should be held liable. At the same time, the Committee feel that the present Bill is about protection of personal data and social media regulation is altogether a different aspect which needs a detailed deliberation.

2.127 **In view of the replacement of "social media intermediaries" with "social media platform" in Clause 26, the consequential changes may be made in sub-clause 28 (3) replacing the word "intermediary" with "platform". Also, since clause 26(4) has been deleted, the words sub-section (4) of section 26 may be replaced by the words"sub-section(1) of section 26" as section 26(1)(f) classifies the term social media platforms.**

2.128 **Accordingly, Clause 28 (3) & (4) as amended may be read as follows:**

(3) Every social media **(***)** **platform** which is notified as a significant data fiduciary under sub-section (***) (**1**) of section 26 shall enable the **(***)** **persons** who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.

(4) Any **(***)** **person** who voluntarily verifies his account **on a social media platform referred to in sub-section (3)** shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.

(Recommendation No. 48)

CLAUSE 29- AUDIT OF POLICIES AND CONDUCT OF PROCESSING ETC.

2.129 Clause 29 (3) and (4) of the Bill relating to Audit of policies and conduct of processing, etc., reads as under:

"(1) The significant 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 shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—

(a) clarity and effectiveness of notices under section 7;

(b) effectiveness of measures adopted under section 22;

(c) transparency in relation to processing activities under section 23;

(d) security safeguards adopted pursuant to section 24; (e) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25;

(f) timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and

(g) any other matter as may be specified by regulations.

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

(4) The Authority shall register in such manner, the persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may be specified by regulations, 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, by regulations, 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 anything contained in sub-section (1), where the Authority is of the view that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose."

2.130 The following suggestions were received on Clause 29:

i The obligation should extend to all data fiduciaries.

ii Civil penalties for negligence by data auditors should be provided for

under the Bill.

iii "Human rights/ digital rights" should be added as a qualifying criteria for data auditors.

iv Power to direct data fiduciaries to conduct an audit should be circumscribed by directions on when to make such directions as well as procedural safeguards.

v Automated decision-making processes should be added as part of the requirements under Clause 29(2).

vi Data trust score should not be mandatory and criteria for data trust score assignments should be provided.

2.131 **The Committee observe that Clause 29(3) empowers the authority to specify the form and procedure for conducting audits. However, it doesn't mentionanything about the concurrent audits. The Committee, therefore, desire that a phrase relating to encouragement of concurrent audit should be added to thissub-clause. Accordingly, the Clause 29(3) may be read as under:**

"(3) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section **and shall encourage the practice of appropriate concurrent audits."**

(Recommendation No. 49)

CLAUSE 30- DATA PROTECTION OFFICER

2.132 Clause 30 of the Personal Data Protection Bill, 2019 deals with Data Protection Officer. The Clause which seeks to require significant data fiduciaries to appoint a Data Protection Officer reads as follows:

"30. (1) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations 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 on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;

(d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;

(e) providing assistance to and co-operating with the Authority on matters of

compliance of the data fiduciary with the provisions under this Act;

(f) act as the point of contact for the data principal for the purpose of grievances redressal under section 32; and

(g) maintaining an inventory of records to be maintained by the data fiduciaryunder section 28.

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

(3) The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act."

2.133 Suggestions were received from the stakeholders on Clause 30, a gist of which is as under:

i There should be no conflict of interest between the DPO when they perform as per Clause 30 and their interest in the data fiduciary and should be independent.

ii No specific location of the DPO should be specified. At most, a legal representative of the entity should be mandatorily appointed within India.

2.134 A similar provision as Article 37 of GDPR states as under: -

"1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of

controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority."

2.135 About the Data Protection Officer, the Justice B.N.Srikrishna Committee Report also states as follows:

"Given that significant data fiduciaries may process considerably sensitive and large amounts of personal data, it is essential that they appoint a person who facilitates compliance with data protection laws by monitoring and advising these fiduciaries as well as acts as a point of contact with the DPA. The eligibility and qualification requirements of the DPO will be specified by way of delegated legislation. The functions allocated to such DPO could include compliance monitoring, developing and ensuring robust compliance and accountability procedures, cooperating with the DPA, training staff, conducting DPIAs, grievance redressal, monitoring security safeguards, and maintaining records, etc."

2.136 **The Committee find Clause 30 provides for conditions for appointment of Data Protection Officer. The Committee observe that the clause simply mentions that every significant data fiduciary should appoint a Data Protection Officer who should be based in India and represent the data fiduciary in the country. The Committee find that there is no mention of any specific qualification or position of the officer in the company. The Committee therefore, desire that since a Data Protection Officer plays a vital role under the provisions of this Bill, he or she should be holding a key position in the management of the Company or other entities and must have adequate technical knowledge in the field. Accordingly, the Committee recommend that Clause 30 (1) may be modified to read as under:**

"30.(1) Every significant data fiduciary shall appoint a data protection officer **who shall be a senior level officer in the State or a key managerial personnel in relation to a company or such other employee of equivalent capacity in case of other**

entities, as the case may be, possessing such qualification**s** and experience as may be (***) **prescribed** (***) for carrying out the following functions, **namely**:—"

2.137 **The Committee also feel that for further clarification of the expression 'key managerial personnel' an explanation may be incorporated at the end of Clause 30(1) which shall also include the scope of inclusion of other persons in future if the Central Government so desires. Accordingly, Explanation to Clause 30 (1) may be read as under:**

***Explanation*.- For the purposes of this sub-section, the expression "key managerial personnel" means—**

(i) the Chief Executive Officer or the managing director or the manager;

(ii) the company secretary;

(iii) the whole-time director;

(iv) the Chief Financial Officer; or

(v) such other personnel as may be prescribed.

2.138 **The Committee further observe that the sub-clauses under Clause 30 (1) need to be placed chronologically as regards of referencing of the Clauses therein. Accordingly, the Committee desire that the sub-clauses in this Clause may be placed as per the reference of specific sections in each Clause in chronological order. The amended Clause 30(1) may read as under:**

30.(1) Every significant data fiduciary shall appoint a data protection officer **who shall be a senior level officer in the State or a key managerial personnel in relation to a company or such other employee of equivalent capacity in case of other entities, as the case may be,** possessing such qualification**s** and experience as may be (***) **prescribed** (***) for carrying out the following functions, **namely**:—

(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 assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;**

(d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;

(e) (***)**providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;**

(f) (***) **maintaining an inventory of records to be maintained by the data fiduciary under section 28;**and

(g)(***) **act as the point of contact for the data principal for the purpose of grievance (***) redressal under section 32.**

***Explanation*.- For the purposes of this sub-section, the expression "key managerial personnel" means—**

(i)the Chief Executive Officer or the managing director or the manager;

(ii)the company secretary;

(iii)the whole-time director;

(iv)the Chief Financial Officer; or

(v)such other personnel as may be prescribed.

(Recommendation No. 50)

CLAUSE 32-GRIEVANCE REDRESSAL BY DATA FIDUCIARY

2.139 Clause 32 of the Bill which seeks to require every data fiduciary to have a grievance redressal mechanism reads as under:

"(1) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner.

(2) A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made 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 complaint made under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary.

(4) Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority in such manner as may be prescribed."

2.140 A gist of the suggestions received in the Memoranda on Clause 32 is as under:

i. Occurrence of harm or likelihood thereof should not be the condition on which reporting of grievances should be allowed under Clause 32.

ii. Procedure for disposal of the application raised to the Authority under Clause 32(4) should be provided.

iii. Specifying DPOs only in case of significant data fiduciary may be unnecessary under section 32(2) (a) and (b).

2.141 Sub-clause (4) of Clause 32 provides the data principal the opportunity to file a complaint to the Data Protection Authority if his or her complaint is not resolved within the specified period, i.e., not later than 30 days from the date of receipt of the complaint by the data fiduciary or if the data principal is not satisfied with the manner in which the complaint is resolved, or in case the data fiduciary has rejected the complaint. However, in the current Bill the manner in which such a complaint has to be filed to the Authority is not prescribed.

2.142 **Keeping in view of the need to devise a single window system to deal with complaints, penalties and compensation, the Committee recommend for the insertion of a new Clause under 'Chapter X-Penalties and Compensation' to be numbered as 62. Clause 62 confers the right to the data principal to file a complaint to the Authority within such period and in such manner to be specified by regulations. It also says that the Authority shall forward the complaint or application filed by the data principal to the Adjudicating Officer for adjudging such complaint or application. Consequent upon the insertion of a new Clause 62, the Committee feel that it has to be stated under Clause 32(4) itself that the data principal, whose complaint is not resolved within the stipulated time or who is not satisfied with the manner in which the complaint is resolved or whose complaint is rejected by the data fiduciary, may file a complaint to the Authority under Clause 62. The amended Clause 32(4) may read as under:**

"(4)Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority **(***) under section 62."**

(Recommendation No. 51)

CLAUSE 34 – CONDITIONS FOR TRANSFER OF SENSITIVE PERSONAL DATA AND CRITICAL PERSONAL DATA

2.143 Clause 34 of the Personal Data Protection Bill, 2019 seeks to list out conditions under which sensitive personal data and critical personal data could be transferred outside India. Clause 34 of the Bill reads as under:-

"(1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—

(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority:

Provided that such contract or intra-group scheme shall not be approved, unless it makes the provisions for—

(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and

(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; or

(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of entity in a country or, an international organisation on the basis of its finding that—

(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; and

(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction: Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed;

c) the Authority has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.

(2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is—

(a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or

(b) to a country or, any entity or class of entity in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest of the State.

(3) Any transfer under clause (a) of sub-section (2) shall be notified to the Authority within such period as may be specified by regulations."

2.144 A gist of the suggestions received in the Memoranda on Clause 34 is as under:

i Adequacy assessment should be undertaken by the DPA and not the Central Government.

ii Necessity for legal claims, contractual obligations and prompt action should be included as narrow exceptions where explicit consent may not be needed, subject to later approval by the DPA.

iii The Section should be extended to personal data as well.

iv Emergency services for transfer of critical personal data may be defined/clarified.

v Explicit consent should a standalone ground for cross border transfers.

vi Codes of conduct or certifications should be permitted as additional bases for transfer.

vii Model contracts or intra group schemes may be provided by the Authority.

viii Each contract or intra group scheme should not need approval, it should be done on a model basis.

2.145 In this regard, Justice B.N.Srikrishna Committee Report states, "Cross border datatransfers of personal data, other than critical personal data, will be through model contract Clauses containing key obligations with the transferor being liable for harms caused to the principal due to any violations committed by the transferee. Intra-group schemes will be applicable for cross-border transfers within group entities. The Central Government may have the option to green-light transfers to certain jurisdictions in consultation with the DPA."

2.146 The Supreme Court in M.G. Brothers Lorry Service Vs. M/s. Prasad Textiles: 1983 (3) SCC 6 was dealing with a contractual provision which sought to set at naught Section 10 of the Carriers Act 1865. The Court held that a contractual clause which is in the teeth of a provision which furthers the intendment of a statute, has to give way and such a clause becomes void and inoperative by virtue of Section 23 of the Contract Act. In Simplex Concrete Piles (India) Ltd. vs. Union of India (2010) ILR 2 Delhi 699**,** the Hon'ble Delhi High Court noted that provisions of the contractwhich will set at naught the legislative intendment of the Contract Act, I would hold the same to be void being against public interest and public policy. Such clauses are also void because it would defeat the provisions of law which is

surely not in public interest to ensure smooth operation of commercial relations."

2.147 The Committee felt that the 2019 Bill seeks to bring in significant changes in the way data is handled by private entities. It provides for several obligations on a data fiduciary (one who determines the purpose and manner of data processing) including explicit consent requirements and confers a number of different rights to a data principal (to whom the data relates). As a result, the contracts entered into between private parties must comply with the new regime of data protection – as and when it is brought into force.

2.148 Moreover, the nature of intervention in contractual relations between parties is not alien to the Indian legal regime and the way contracts over specific subjects is governed. Parallels may be drawn with the way the Copyright Act, 1957 ("Copyright Act") has been used as a legislative interference in the mode and manner in which parties enter into contracts relating to assignment of copyrighted works. The Copyright Act was amended in 2012 by inserting an additional proviso to Section 18 of the Copyright Act. This newly inserted proviso provided that no assignment can be applied to any medium or mode of exploitation of a work which did not exist, or was not in commercial use, at the time when the assignment was made, unless specifically referred to such medium or mode of exploitation.

2.149 **The Committee note that as per Clause 34(1)(b), the Central Government, in consultation with the Authority, has been empowered to allow transfer of sensitive personal data, for the purpose of processing and with explicit consent of the data principal, to any country with certain safeguards such that transfer is only made to a country having adequate level of protection for the data principal. Similarly, the Authority while approving a contract or intra group scheme under Clause 34(1)(a) which allows the cross-border transfer of data, should invariably consult the Central Government. The Committee,therefore, recommend that the word 'in consultation with the Central Government' be added at the end of Clause 34(1)(a).**

2.150 **The Committee are also concerned about the potential misuse of the provision of the Clause 34(1)(a) by individuals/organizations with *mala-fide* intentions or by foreign entities whose actions might be inimical to the interests of the State. In order to ensure a balance between the legitimate needs of businesses and the protection of the fundamental**

right of privacy of individuals and to protect the larger interests of the data principal *vis-à-vis* public policy, the Committee suggested to insert a provision in the Clause 34(1)(a)whereby any contract or intra-group scheme allowing cross-border transfer of data, evenafter the consent of the data principal, may not be approved if such contract or intra-group scheme is against public policy. The Committee therefore, recommend that the words 'if the object of such transfer is against public policy or State policy and' be inserted after the word 'approved' (line 32, at page 18) in Clause 34(1)(a).

2.151 **Further, to define as to when an act is said to be against public policy, the Committee also desire to insert an explanation at the end of sub-clause 34(1).After the incorporation of amendments as suggested by the Committee, Clause 34(1)(a) in its entirety may be read as under:-**

"(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority **in consultation with the Central Government**:

Provided that such contract or intra-group scheme shall not be approved, **if the object of such transfer is against public policy or State policy and** unless it makes the provisions for—

(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and

(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; **(***)"**

(Recommendation No. 52)

2.152 The Explanation providing the definition of 'act against public or state policy'to be added at the end of Clause 34(1) will read as under:-

"***Explanation.*- For the purposes of this sub-section, an act is said to be against "public policy" or "State policy", if the said act promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizens."**

(Recommendation No. 53)

2.153 The Committee also noted the implications of the adequacy provisions of the Bill under Clause 34 (1) (b) and pointed out that the Bill does not make any provision for restriction of further transfer of data by the country, to which the Government of India has allowed the transfer, to a third country.

2.154 **The Committee are of the opinion that in order to safeguard the data of Indians and keeping in view the shifting nature of international relations, it is necessary to have a directive in the Bill to restrict any country, to which sensitive personal data of Indians would be transferred, from sharing it with a third country or agency, unless such sharing is approved by the Central Government. The Committee therefore, recommend to insert a new sub-clause under Clause 34(1)(b). Accordingly, after the insertionof the new sub-clause Clause 34(1)(b)(iii), Clause 34(1)(b) in its entirety may be read as under:-**

"(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of (***) **entities** in a country or, an international organisation on the basis of its finding that–

(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; **(***)**

(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction**; and**

(iii) such sensitive personal data shall not be shared with any foreign government or agency unless such sharing is approved by the Central Government:

Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed; **or"**

(Recommendation No. 54)

2.155 **Accordingly, to bring all the clauses in sync with each other so that the transfer of any information outside the country is always in consultation with the Central Government, the Committee recommend that sub-clause (c) to Clause 34(1) may now be read as under:**

"(c) the Authority**, in consultation with the Central Government,** has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose."

(Recommendation No. 55)

CLAUSE 35 – POWER OF CENTRAL GOVERNMENT TO EXEMPT ANY AGENCY OF GOVERNMENT FROM APPLICATION OF ACT

2.156 Clause 35 of the Personal Data Protection Bill, 2019 reads as under:

"Where the Central Government is satisfied that it is necessary or expedient,—

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order; or

(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order,

it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

Explanation.—For the purposes of this section,—

(i) the term "cognizable offence" means the offence as defined in Clause (c) of section 2 of the Code of Criminal Procedure, 1973;

(ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal."

2.157 The Committee had received several suggestions on the Clause. A gist of the suggestions received in the form of Memoranda on Clause 35 is as under:

i Public order should be removed as a ground for exemption.

ii Judicial oversight and/ or parliamentary oversight is required for granting these exemptions.

iii There should be an order in writing with reasons for exempting a certain agency from the ambit of the Bill.

iv State /state agencies should not be exempted from all provisions of the Bill – security safeguards, personal data breach notification, confirmation and access rights, notification rights should continue to be applicable for state agencies. Clauses 4, 5, 6, 9, 24, 35 and Chapters I, IX-XIV, protection of children and safeguards provided in Juvenile Justice (Care and Protection of Children) Act, 2015 should not be overruled.

v Safeguards in the PDP Bill 2018 should be inserted to reflect that exemptions are by law/ statute, necessary and proportionate.

vi Appoint DPO for state agencies.

vii Regular public audits and mandatory submission of annual reports to parliament need to be provided.

2.158 During the discussions, the Committee debated about balancing the provisions under this Bill along with the concerns regarding national security, liberty and

privacy of an individual. It was observed that in most of the autocratic countries which usurps global data these conversations with regard to national security and individual freedom are not possible. The Committee felt that a few difficult questions have to be asked about India's threat perception and the choices India makes about its open society and individual freedom, which greatly depends on India's existence as a Nation. The challenge of balancing between the provisions of the Bill and the aforementioned three concerns is not an easy one. There can be no choice between these concerns. A secure nation alone provides the atmosphere which ensures personal liberty and privacy of an individual whereas the multiple number of examples exist where without individual liberty and privacy, national security itself gives rise to autocratic regimes. This Committee had the onerous task of devising an appropriate legal measure to address national security concerns so that we have an atmosphere which protects our liberty and privacy and does not endanger it at the hands of inimical forces to the interest of India.

2.159 With respect to Clause 35, the relevant portion from Puttaswamy judgment is reproduced below:

"The concerns expressed on behalf of the petitioners arising from the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State:

(i) The action must be sanctioned by law;

(ii) The proposed action must be necessary in a democratic society for a legitimate aim;

(iii) The extent of such interference must be proportionate to the need for such interference;

(iv) There must be procedural guarantees against abuse of such interference.

2.160 Further the judgment continues to say as under:

"while it intervenes to protect legitimate state interests, the state must nevertheless put into place a robust regime that ensures the fulfillment of a three-fold requirement. These three requirements apply to all restraints on privacy (not just informational privacy). They emanate from the procedural and content-based mandate of Article 21. The first requirement that there must be a law in existence to justify an encroachment on privacy is an express requirement of Article 21. For, no person can be deprived of his life or personal liberty except in accordance with the procedure established by law. The existence of law is an essential requirement. Second, the requirement of aneed, in terms of a legitimate state aim, ensures that the nature and content of the law which imposes the restriction falls within the zone of reasonableness mandated by Article 14, which is a guarantee against

arbitrary state action. The pursuit of a legitimate state aim ensures that the law does not suffer from manifest arbitrariness. Legitimacy, as a postulate, involves a value judgment. Judicial review does not re-appreciate or second guess the value judgment of the legislature but is for deciding whether the aim which is sought to be pursued suffers from palpable or manifest arbitrariness. The third requirement ensures that the means which are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. Proportionality is an essential facet of the guarantee against arbitrary state action because it ensures that the nature and quality of the encroachment on the right is not disproportionate to the purpose of the law. Hence, the three-fold requirement for a valid law arises out of the mutual inter-dependence between the fundamental guarantees against arbitrariness on the one hand and the protection of life and personal liberty, on the other. The right to privacy, which is an intrinsic part of the right to life and liberty, and the freedoms embodied in Part III, is subject to the same restraints which apply to those freedoms."

2.161 The recent decision in Jeeja Ghosh vs Union of India and Ors construed the constitutional protection afforded to human dignity. The Court observed:

"...human dignity is a constitutional value and a constitutional goal. What are the dimensions of constitutional value of human dignity? It is beautifully illustrated by Aharon Barak (former Chief Justice of the Supreme Court of Israel) in the following manner:

> "The constitutional value of human dignity has a central normative role. Human dignity as a constitutional value is the factor that unites the human rights into one whole. It ensures the normative unity of human rights. This normative unity is expressed in the three ways: first, the value of human dignity serves as a normative basis for constitutional rights set out in the constitution; second, it serves as an interpretative principle for determining the scope of constitutional rights, including the right to human dignity; third, the value of human dignity has an important role in determining the proportionality of a statute limiting a constitutional right;

2.162 In Singapore, the Personal Data Protection Act doesn't apply to Government organizations and is applicable only on the private organizations. The major concerns of the State as mentioned above are addressed by the Government using the Acts (like Official Secrets Act) and not the Personal Data Protection Act. The purpose of the said act is to govern collection, use and disclosure of the personal data by organizations.

2.163 While the Clarifying Lawful Overseas Use of Data Act or CLOUD Act is a United States federal law enacted in 2018 allowing federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or not. It has enabled the US agencies to have an alternate and expedited route to theMLAT (mutual legal assistance treaties) through executive agreements for theprocessing of the data stored outside the US for legitimate purposes. Only federal agencies can enforce CLOUD Act. And in China, government has total control over platforms. All data critical to national security is stored within the country.

2.164 Similarly, under Article 23 of General Data Protection Regulation restricts the obligations and rights of data controller or processor inter-alia for the purpose of national security, defence, public security, the prevention, investigation,detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, economic or financial interest, public health and social security etc.

2.165 Article 9 of GDPR states as under:

"1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

…

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;"

2.166 Justice B.N. Srikrishna Committee, while drafting the Personal Data Protection Bill, had gone into the above concerns of the State as well as delved into the Puttaswamy Judgement of the Hon'ble Supreme Court, wherein these exceptionshave been envisaged as legitimate interests of the state and satisfy the proportionality test, and created several exceptions and exemptions for

processing of data by the State, highlighting the fact that these are situations where rights and obligations of data principals and data fiduciaries may not apply in totality.

2.167 Further, Justice B.N. Srikrishna Committee recommend, "Welfare functions of the state will be recognised as a separate ground for processing. Processing activities carried out by the State under law will be covered under this ground, ensuring that it is in furtherance of public interest and governance. However, only bodies covered under Article 12 of the Constitution may rely on this ground. Processing towards activities that may not be considered part of a welfare functions would, however, not to be permitted. Thus, the availability of this ground is restricted to certain entities and certain functions to avoid vagueness in the law."

2.168 Further the Committee recommend, "The data protection law will enable an exemption to the processing of personal or sensitive personal data if it is necessary in the interest of the security of the state. Any restriction must be proportionate and narrowly tailored to the stated purpose. The Central Government should expeditiously bring in a law for the oversight of intelligence gathering activities."

2.169 The Committee observed that the mandatory concern of a State in the modern political world and with current geo-political situations are the national sovereignty and integrity of country, security of State, friendly relation with foreign countries, prevention of crime and maintenance of public order. In addition to these political mandates, the economic and social well-being of its citizens is another goal of every State.

2.170 In the sitting of the Committee held on 16 December, 2020, the Ministry of Electronics and IT submitted as under:

"while drafting this provision, we have taken the precedents of the Information Technology Act and the Indian Telegraph Act, the provisions mentioned there. …….. What the restrictions mentioned here are on lines of Clause 2 of Article 19 of the Constitution which specifies the reasonable restrictions, that is, sovereignty and integrity of India and other factors mentioned therein."

2.171 **The Committee note that Clause 35 empowers the Central Government to exempt any agency of the Government from the application of this Act for certain legitimate purposes such as security of State, public order etc. While examining Clause 35 in the larger context of constitutional provisions, related court judgments and similar**

provisions in legislations of other countries, the Committee find that the provision of Clause 35 have precedent in the form of the reasonable restrictions imposed upon the liberty of an individual, as guaranteed under Article 19 of the Constitution and the Puttaswamy Judgment. However, the Committee are concerned about the possible misuse of the provisions when a situation arises whereby the privacy rights of the individual, as provided under this Act, have to be subsumed for the protection of the larger interests of the State. The Committee, therefore, feel that though the State has rightly been empowered to exempt itself from the application of this Act, this power may, however, be used only under exceptional circumstances and subject to conditions as laid out in the Act. The Committee note that the GDPR, Cloud Act and the Puttaswamy judgment also recognize the need to provide such powers to the State, albeit with reasonable restrictions, to safeguard national interests. Further, the Committee find that the Puttaswamy Judgment has laid down three tests before the State may infringe upon the privacy of an individual, namely, the tests of necessity, proportionality and legitimate state action. In order to strike a balance between Article 19 of the Constitution, Puttaswamy judgment and individual rights with respect to privacy, as provided in this Act and elsewhere, the Committee recommend that 'such procedure' as stated in Clause 35 (line 28) needs to be defined in the explanation paragraph of Clause 35. The Committee therefore, desire that a new sub-clause (iii) may be added in the explanation to Clause 35 which may read as under:-

"(iii) the expression "such procedure" refers to just, fair, reasonable and proportionate procedure."

2.172 **Clause 35, as amended by the Committee as a whole may be read as under:**

"35. Notwithstanding anything contained in any law for the time being in force, where the Central Government is satisfied that it is necessary or expedient,—

(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States **or** public order; or

(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States **or** public order,

it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such

procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.

Explanation. —For the purposes of this section, —

(i)the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;

(ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal; **and**

(iii) the expression "such procedure" refers to just, fair, reasonable and proportionate procedure."

(Recommendation No. 56)

CLAUSE 36 – EXEMPTION OF CERTAIN PROVISIONS FOR CERTAIN PROCESSING OF PERSONAL DATA

2.173 Clause 36 of the Personal Data Protection Bill, 2019 which seeks to exempt certain provisions for certain processing of personal data reads as under:

"The provisions of Chapter II except section 4, Chapters III to V, Chapter VI except section 24, and Chapter VII shall not apply where-

(a) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law for the time being in force;

(b) 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;

(c) processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;

(d) personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or

(e) processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with any code of ethics issued by the Press Council of India, or by any media self-regulatory organisation."

2.174 A gist of the suggestions received in the form of Memoranda on Clause 36 is as under:

i Exemption should not apply to Clause 4, 5, 6, 9, Chapters III to V, chapter VI except Clause 17, 18, 24, and chapter VII.

ii Clauses 5,6,8,9 and 25 should continue to be applicable.

2.175 With regard to the exemption to be provided for journalistic purpose, Justice B.N. Srikrishna Committee Report says, "Finally, to be accorded an exemption from the data protection law, journalists should be bound by ethics standards like honesty and fairness in collecting and disseminating personal data for the purpose of news reporting. The purpose of having ethics standards in place for the application of the journalistic exemption is to be able to separate credible contributors from less credible ones by establishing benchmarks of professional practice and measuring people against them. Ethics standards have become especially important in the age of the internet which has made publishing infinitely easier, with the result that persons without the skills or training in becoming a journalist are becoming the source for news. The lack of any professional qualification examination further intensifies this problem."

2.176 **The Committee are of the view that there is a requirement of simplification of the language of Clause 36 and thus suggest that the lines 36 and 37 of Clause 36 of the Personal Data Protection Bill, 2019 should be amended as: "36.**The provisions of Chapter II **(***) <u>to VII, except section 24</u>**, shall not apply where—"

(Recommendation No. 57)

2.177 **Clause 36(e) relates to the processing of personal data for journalistic purpose and seeks to regulate it with the code of ethics issued by the Press Council of India or by any statutory media self-regulatory organization. In this regard the Committee are of the view that freedom of expression is necessary for the functioning of the media and should not be curtailed with the coming into effect of this Bill. At the same time the privacy rights of the individual, that the Bill seeks to protect, must also be safeguarded against misuse in the name of journalism. The Committee also feel that self-regulation by the media is insufficient and there is a need of a comprehensive code and a unified entity for the regulation of media, in all its forms and iterations in the country. The Committee note that at present there is no single unified agency that regulates the various forms of media, specifically news media, in the country. In the Committee's view, the existing media regulators such as the Press Council of India are not appropriately equipped to regulate journalism sector that seeks to use modern methods of communication such as social media**

platforms or the internet at large. In this regard, the Committee feel that there is need for the establishment statutory body for media regulation in order to fulfill the above mentioned objectives. The Committee desire that Clause 36(e) may be amended to empower any statutory media regulator that the Government may create in the future and until such time the Government may also issue rules in this regard. The Committee, therefore, recommend that in Clause 36(e) after the words 'compliance with' the words 'the rules and regulations made under this Act," be added and in the same Clause the words 'media self-regulatory organisation' be substituted by the words 'statutory media regulatory organisation'. Clause 36(e) as amended by the Committee may be thus read as under:-

"(e) **the** processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with**the rules and regulations made under this Act**, **(***)** code of ethics issued by the Press Council of India, or by any **statutory** media **(***)** regulatory organisation."

(Recommendation No. 58)

CLAUSE 39 – EXEMPTION FOR MANUAL PROCESSING BY SMALL ENTITIES

2.178 Clause 39 of the Personal Data Protection Bill, 2019 deals with Exemptions for manual processing by small entities. The Clause reads as under:

" (1) The provisions of sections 7, 8, 9, Clause (c) of sub-section (1) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated.

(2) For the purposes of sub-section (1), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to—

(a) the turnover of data fiduciary in the preceding financial year;

(b) the purpose of collection of personal data for disclosure to any other individuals or entities; and

(c) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months."

2.179 A gist of the suggestions received in the form of Memoranda on the Clause is as under:

i Due process safeguards may be included.

ii The scope of exemptions should not cover Clause s 20, and 23-25.

iii "manual processing" may be defined.

iv The exemption should be extended to both manual and automated

processing by small entities.

2.180 In this regard, Justice B.N.Srikrishna Committee Report says, "Since the risk of privacy harms being caused are higher when personal data is processed through automated means, an exemption will be made in the data protection law for manual processing by data fiduciaries that are unlikely to cause significant harm and would suffer the heaviest relative burdens from certain obligations under this law."

2.181 **The Committee observe that the word "manual" used in the marginal note to the Clause is not used anywhere else in the Clause and hence to remove the ambiguity the Committee decided to make the following correction to the marginal note of the Clause :-**

"Exemption for (***) non automated **processing by small entities."**

(Recommendation No. 59)

CLAUSE 40 – SANDBOX FOR ENCOURAGING INNOVATION, ETC.

2.182 Clause 40 of the Personal Data Protection Bill, 2019 deals with Sandbox for encouraging innovation, etc. Sub-sections (1)and (2) of Clause 40 of the Bill read as under:-

"(1) The Authority shall, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox.

(2) Any data fiduciary whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1).

(3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:—

(a) the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months;

(b) the innovative use of technology and its beneficial uses;

(c) the data principals or categories of data principals participating under the proposed processing; and

(d) any other information as may be specified by regulations.

(4) The Authority shall, while including any data fiduciary in the Sandbox, specify—

(a) the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months;

(b) the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of consent of

data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and

(c) that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:—

(i) the obligation to specify clear and specific purposes under sections 4 and 5;

(ii) limitation on collection of personal data under section 6; and

(iii) any other obligation to the extent, it is directly depending on the obligations under sections 5 and 6; and

(iv) the restriction on retention of personal data under section 9.

2.183 The following suggestions were received from the stakeholders in the form of Memoranda:

i "Sandbox" may be defined.

ii Safeguards may be provided for data fiduciaries after the expiration of the sandbox relaxation.

iii Mandate the DPA to conduct review of regulations/ standards etc. based on sandbox findings.

iv Means for coordination may be included with sectoral regulators on sandbox guidelines (for e.g. RBI Fintech Sandbox).

2.184 **The Committee observe that in Clause 40(1) the use of the word "shall" imposes a mandatory obligation upon the Government to create a Sandbox. In the Committee's view, the Clause should be an enabling provision rather than a restrictive one. Moreover, the Committee feel that at present the Government may not have the necessary infrastructure, resources or expertise to implement/create a Sandbox. This in turn might prove detrimental for innovation by the private sector that rely on data. Therefore, the committee suggest that the word "shall" in Clause 40(1) may be replaced with the word "may".**

2.185 **Further, the Committee suggest to insert the words "as well as startups" after the words "any data fiduciary", in sub-clause (2) of the Clause to allow startups, which are crucial in India's bid to emerge as a 5 trillion $ economy, to participate in the Sandbox regime.**

2.186 **Accordingly, Clause 40(1) and (2) may be amended as under:-**

"40.(1) The Authority **(***) <u>may</u>**, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox.

(2) Any data fiduciary **as well as start-ups** whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1)."

(Recommendation No. 60)

2.187 **The Committee also note that the expression 'Sandbox' has not been explained in Clause 40. Since, the expression 'Sandbox' is a technical term, the Committee find it necessary to include an explanation for 'Sandbox' in order to avoid any ambiguity or misinterpretation of the term. The Committee, therefore, desire that the explanation for the term 'Sandbox' may be inserted at the end of Clause 40 to be read as under:-**

"*Explanation*.- For the purposes of this Act, the expression "Sandbox" means such live testing of new products or services in a controlled or test regulatory environment for which the Authority may or may not permit certain regulatory relaxations for a specified period of time for the limited purpose of the testing."

(Recommendation No. 61)

CLAUSE 42 – COMPOSITION AND QUALIFICATIONS FOR APPOINTMENT OF CHAIRPERSON AND MEMBERS

2.188 Clause 42 provides for the provisions for composition and qualifications for Chairperson and Members of the Data Protection Authority which reads as below:

42. (1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law.

(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 Cabinet Secretary, who shall be Chairperson of the selection committee;

(b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and

(c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

(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 shall have qualification and specialised

knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects.

(5) A vacancy caused to the office of the Chairperson or any other member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.

2.189 **The Committee desire that provision for Chairperson and Members in Clause 42(1) should be modified to make it specific and thus it may be modified stating that at least the Member shall be an expert in the area of law having such qualifications and experience as may be prescribed. The modified Clause 42(1) may be read as under:**

"42.(1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) **an expert in the area of law**having**such**qualification**s** and experience (***) **as may be prescribed**."

(Recommendation No. 62)

2.190 **Clause 42 (2) states that 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 Cabinet Secretary, who shall be Chairperson of the selection committee; (b) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and (c) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.**

2.191 **The Committee find that the proposed composition of Selection Committee in the Bill has only three Members and all are Secretary level bureaucrats. The Committee desire that inclusion of technical, legal and academic experts in the Selection Committee should also be made to make it more inclusive, robust and independent. Accordingly, Clause 42 (2) may be amended as under:**

"42.(1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) **an expert in the area of law**having**such**qualification**s** and experience (***) **as may be prescribed.**.

(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a **S**election **C**ommittee consisting of—

(i) the Cabinet Secretary, who shall be Chairperson of the **S**election **C**ommittee;

(ii) the Attorney General of India - Member;

(**iii**) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs - **Member**; **(***)**

(iv) the Secretary to the Government of India in the Ministry or Department dealing with (***) Electronics and Information Technology - **Member;**

(v) an independent expert to be nominated by the Central Government from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related subjects - Member;

(vi)a Director of any of the Indian Institutes of Technology to be nominated by the Central Government – Member; and

(vii)a Director of any of the Indian Institutes of Management to be nominated by the Central Government – Member.

(Recommendation No. 63)

CLAUSE 45- POWERS OF CHAIRPERSON.

2.192 " Clause 45 of the Bill reads as under:

"45. The Chairperson of the Authority 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 this Act."

2.193 During the deliberations, the Committee observed that Clause 45 doesn't specifically mention about the basic power of Chairperson to preside the meetings of Data Protection Authority. Hence the Committee recommend that Clause 45 shall also mention the basic power of the Chairperson of presiding over the meetings of DPA. The committee also recommend that the words 'in the conduct' may be added before 'of the affairs' to qualify the powers of the Chairperson. Accordingly Clause 45 as amended may be read as below:

"45. The Chairperson of the Authority shall (***) have powers of general superintendence and direction **in the conduct** of the affairs of the Authority and **he** shall, (***) **in addition to presiding over the meetings of the Authority,** exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act."

(Recommendation No. 64)

CLAUSE 49– POWERS AND FUNCTIONS OF DATA PROTECTION AUTHORITY

2.194 Clause 49 which enumerates the powers and functions of the Data Protection Authority reads as under:

"(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 about data protection.

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

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

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

(c) 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;

(d) examination of any data audit reports and taking any action pursuant thereto;

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

(f) classification of data fiduciaries;

(g) monitoring cross-border transfer of personal data;

(h) specifying codes of practice;

(i) promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals;

(j) monitoring technological developments and commercial practices that may affect protection of personal data;

(k) promoting measures and undertaking research for innovation in the field of protection of personal data;

(l) advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;

(m) specifying fees and other charges for carrying out the purposes of this Act;

(n) receiving and inquiring complaints under this Act; and

(o) performing such other functions as may be prescribed.

(3) Where, pursuant to the provisions of this Act, the Authority processes any 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 under any law to do so, or where it is required to carry out its function under this section."

2.195 A gist of the suggestions received in the form of Memoranda on Clause is as under:

i Procedures, including a pre consultation mandate for the DPA to make regulations etc may be provided.

ii An obligation may be provided to conduct affairs transparently.

iii DPA should publish reports in public interest and advise Parliament on measures to promote data protection.

2.196 During the deliberation on Clause 49, the Committee raised the concern about hardware integrity which is essential for privacy. The Committee also took note of the report published in Bloomberg Businessweek, wherein it was reported that in 2015-16, Amazon Inc had designed a hardware to carry out a secret services mission and other online services for the United States of America. The server design was finalized and the bulk hardware manufacturing was outsourced to China. However, the said company was surprised to find a tiny microchip fixed in the server's motherboard, which was not a part of the original design. The sheer investment in manufacturing and transmitting it in all devices can give away the gravity of the data breach. A hardware attack is graver than the software-based incidents that the world is accustomed to witnessing. Hardware attacks are more difficult to pull off and potentially more devastating due to its rarity and the lack of regulation for it.

2.197 Additionally, the Committee were apprised of the similar provisions, in this regard, in GDPR. The GDPR under Recital (30) states as "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

2.198 In view of the apprehensions of the Committee with regard to data leakage through hardware components, the Ministry of Electronics and IT submitted during the sitting held on 28 December, 2020 as under:

"Any product that is being sold in India from anywhere in the world, including the Indian manufacturers as well, has to go through the entire process of evaluation, which is at different levels – EAL1 through EAL7. They have to get their products tested and certified at the product level."

2.199 The Committee took note of the above submission but at the same time were of the view that due to limited awareness by people, the Hardware (part of the digital ecosystem) is usually considered relatively safe and secure — as opposed to software threats about which even the ordinary people are becoming increasingly aware of. The Committee expressed their concern over the hardware being imported into the country without any proper testing and certification with regard to data protection which in turn leads to extraction of data and affirm that this kind of intervention amounts to infringement of citizen's fundamental right to privacy.

2.200 **The Committee note that Clause 49(2) (b) empowers the Authority to take prompt and appropriate action in response to personal data breach in accordance with the provisions of this Act. The Committee feel that since the ambit of the Act has been widened to include regulating of non-personal data also, the powers of the Authority to take action in the event of non personal data breach should also be enlarged. The Committee, accordingly recommend that the word "personal" may be deleted from Clause 49 (2) (b). The amended Clause 49 (2) (b) may read as under:**

"(b) taking prompt and appropriate action in response to (***) data breach in accordance with the provisions of this Act;"

(Recommendation No. 65)

2.201 **The Committee observe that the threat of leakage of sensitive personal data through hardware has now become a serious concern for policy makers and security experts worldwide. The global decentralized nature of manufacturing provides the opportunity for individuals/organizations with *mala-fide* intentions to misuse digital hardware. With the advent of IoT devices and proliferation of digital equipment in the daily life of individuals, this threat has multiplied. The Committee, therefore, feel that in order to protect the data of Indians, the Central Government and the Data Protection Authority must suitably be empowered through this legislation to allow them to create a framework that provides for monitoring, testing and certification to ensure integrity of hardware**

equipment and to prevent any interdiction or seeding that may result in breach of personal data. The Committee therefore, recommend for insertion of a new sub -clause under 49(2) replacing 49(2)(o). The original sub-clause 49(2)(o) shall become 49(2)(p). The new sub-clause 49(2)(o) as inserted by the Committee may be read as under:-

"(o) monitoring, testing and certification by an appropriate agency authorized by the Central Government for this purpose to ensure integrity and trustworthiness of hardware and software on computing devices to prevent any malicious insertion that may cause data breach; and"

(Recommendation No. 66)

CLAUSE 50 – CODES OF PRACTICE

2.202 Clause 50 of the Bill deals with the codes of Practice to be specified by the Data Protection Authority to promote good practices of data protection and facilitate compliance with the obligations under this Act. Clause 50 (2) reads as under:-

"(2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by 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."

2.203 A gist of the suggestions received in the form of Memoranda on Clause 50 is as under:

i Codes of practice should not be binding, and data fiduciaries should have the option of demonstrating compliance if higher standards have been adopted.

ii Consultation mandate should include industry, academia and civil society actors specifically.

iii The consultation process should be prescribed under the Bill itself.

iv Power to issue a code of practice for manner of obtaining consent where the principal is incapable of providing consent should be reinstated.

v Obligation to maintain a register of existing codes of practice should be reinstated.

2.204 The Committee took note of a suggestion received from a stakeholder which suggested as follows:

"The Authority should not, itself, be required to make regulations applicable to a given industry. Instead, it should empower self-regulatory organisations to develop regulations and standards that would govern that industry. Similarly, the Authority should not have to specify the technical standards

which are necessary to ensure coherence of data protection and data empowerment processes across sectors. Instead, it should empower technical services organisations to do so."

2.205 **Clause 50(2) makes a provision under which in addition to its power, to specify codes of practice for data protection and compliance under this Act, the Authority has also been empowered to approve any code of practice submitted various associations related to trade or representing interest of data principal etc. The Committee, however, find that there is no mention of technical services organisations which may prepare standard technical codes of practice necessary for data protection and data empowerment processes.**

2.206 **The Committee, therefore, recommend that Clause 50(2) should also include an association representing technical services organistions, in addition to associations related to industry, trade and those representing interest of data principals. Further, in order to avoid the repetition of the word association and to bring clarity, Clause 50(2) may be reframed as under:-**

"(2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by-

(i) the associations representing-

(a) technical services organizations;

(b) **(***)** industry or trade (***)

(c) (***) the interest of data principals

(ii) any sectoral regulator or statutory Authority; or

(iii) any **D**epartments or **M**inistries of the Central **Government** or State Government."

(Recommendation No. 67)

2.207 **The Committee feel that the Bill has already provisions for protection on non-personal data along with personal data. Therefore, data breach, whether personal or non-personal, should be covered under Clause 50 (6) (o). Accordingly, the word 'personal' may be omitted before 'data breach' and Clause 50(6)(o) may be now read as under:**

"(o) appropriate action to be taken by the data fiduciary or data processor in response to a (***) data breach under section 25;"

(Recommendation No. 68)

CLAUSE 55- SEARCH AND SEIZURE.

2.208 Clause 55 reads as below:

55. (1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records

or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such designated court, as may be notified by the Central Government, for an order for the seizure of such books, registers, documents and records.

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

(3) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer—

(a) to enter, with such assistance, as may be required, the place or places where such books, registers, documents and records are kept;

(b) to search that place or those places in the manner specified in the order; and

(c) to seize books, registers, documents and records it considers necessary for the purposes of the inquiry.

(4)The Inquiry Officer shall keep in its custody the books, registers, documents and records seized under this section for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return.

(5) Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.

2.209 **The Committee observe that in the original form Clause 55(1) enables the Inquiry Officer during the course of inquiry to make an application to such designated court, as may be notified by the Central Government for an order for the seizure of such books, registers, documents and records if there is a reasonable ground to believe that these evidences may be tampered with, altered, mutilated, manufactured, falsified or destroyed. However, the Committee feel that there should be a safeguard mechanism in the form of a prior approval from DPA to strengthen the the Inquiry Officer when he renders his duties in this regard. Hence, the Committee recommend to add the words "shall, with the prior approval of the Authority" before the words "make an application" in Clause 55(1) to read as below:**

"**55.**(1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer **(***)shall, with the prior approval of the Authority,**make an application to such designated court, as may be notified by the Central Government, for an order for the seizure of such books, registers, documents**,**(***) records **or data**."

(Recommendation No. 69)

CLAUSE 56-CO-ORDINATION BETWEEN AUTHORITY AND OTHER REGUALTORS OR AUTHORITIES.

2.210 Clause 56 of the Bill reads as under:-

"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."

2.211 The gist of the Memorandum the Committee have received suggests that the Memorandum of Understandings (MoUs) should be mandatorily executed between authorities in case of Clause 56.

2.212 **Clause 56 of the Bill makes it obligatory upon the Authority to consult any other regulator or authority, established under a law made by Parliament or any state legislature, that might have concurrent jurisdiction with respect to any proposed action of the Authority concerning this Act. The Committee note that the proposed action of the Authority under this Clause might also have economic consequences which might require consultation with economic regulators such as RBI. Therefore, in order to increase the scope of the word 'action' and for the sake of clarity, the Committee desire that the words 'including economic activities' might be inserted at the end of the Clause.**

2.213 **Clause 56 as amended by the Committee may be read as under:-**

"56. 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 **including economic activities**."

(Recommendation No. 70)

CLAUSE 57- PENALTIES FOR CONTRAVENING CERTAIN PROVISIONS OF THE ACT.

2.214 Clause 57 of the Bill seeks to list out penalties for contravening certain provisions of the Act. It reads as under:

" 57.(1) Where the data fiduciary contravenes any of the following provisions,—

(a) obligation to take prompt and appropriate action in response to a data security breach under section 25;

(b) failure to register with the Authority under sub-section (2) of section 26,

(c) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;

(d) obligation to conduct a data audit by a significant data fiduciary under section 29;

(e) appointment of a data protection officer by a significant data fiduciary under section 30, it shall be liable to a penalty which may extend to five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher;

(2) Where a data fiduciary contravenes any of the following provisions,—

(a) processing of personal data in violation of the provisions of Chapter II or Chapter III;

(b) processing of personal data of children in violation of the provisions of Chapter IV;

(c) failure to adhere to security safeguards as per section 24; or

(d) transfer of personal data outside India in violation of the provisions of Chapter VII, it shall be liable to a penalty which may extend to fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher.

(3) For the purposes of this section,—

(a) the expression "total worldwide turnover" means the gross amount of revenue recognized 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.

(b) it is hereby clarified that total worldwide turnover in relation to a data fiduciary is 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) the alignment of the overall economic interests of the data fiduciary and the group entity; (ii) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and

(iii) the degree of control exercised by the group entity over the data fiduciary or vice versa, as the case may be.

(c) where of any provisions referred to in this section has been contravened by the State, the maximum penalty shall not exceed five crore rupees under sub-section (1), and fifteen crore rupees under sub-section (2), respectively."

2.215 **The Committee observe that in Clause 57(1), (2) and (3) the quantification of penalty has been quantified in terms of percentage of world-wide turnover or as a specific amount or the world-wide turn over of teh company. In Committee's view such quantification may not be feasible as there are no clear mechanisms to quantify the 'world-wide turnover' of the company and that too along with its group entities. Also keeping in view of the rapidly changing dynamics of the evolving digital technologies, the Committee feel that it would be prudent to enable the Government to quantify the penalties. The Committee, therefore, recommend that the expressions under Clause 57(1) and (2) which specify about the quantum of penalty may be modified. Further, with such modification there is no relevance of Clause 57(3)(a) and (b) and may be omitted and sub-clause (c) under 57(3) may be incorporated under Clause 57(3) in the modified form. The amended Clause 57 may be read as under:**

"57.(1) Where the data fiduciary contravenes any of the following provisions, namely:-

(a) obligation to take prompt and appropriate action in response to a data (***) breach under section 25;

(b) failure to register with the Authority under sub-section (2) of section 26;

(c) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;

(d) obligation to conduct a data audit by a significant data fiduciary under section 29; or

(e) appointment of a data protection officer by a significant data fiduciary under section 30,

it shall be liable to (***) **such** penalty (***) **as may be prescribed** (***).

(2) Where a data fiduciary contravenes any of the following provisions, namely:—

(a) processing of personal data in violation of the provisions of Chapter II or Chapter III;

(b) processing of personal data of children in violation of the provisions of Chapter IV;

(c) failure to adhere to security safeguards as per section 24;or

(d) transfer of personal data outside India in violation of the provisions of Chapter VII,

it shall be liable to (***)**such** penalty (***)**as may be prescribed**(***).

(3) For the purposes of this section, (***) where any of the (***) provisions referred to in this section has been contravened by the State, the maximum penalty shall (***)**be such as may be prescribed.**

(Recommendation No. 71)

CLAUSE 60 – PENALTY FOR FAILURE TO COMPLY WITH DIRECTION OR ORDER ISSUED BYAUTHORITY

2.216 Clause 60 deals with the penalty to be paid by the data fiduciary and data processors for failure to comply with direction or order issued by the Data Protection Authority under section 51 and 54. The Clause, as in the Personal Data Protection Bill, 2019, reads as under:

"If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 51or order issued by the Authority under section 54, such or data processor shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crores in case of a data processor it may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees "

2.217 **The Committee find that Clause 60 provides separate quantum of penalty for data fiduciary and data processor but has been grouped together in**

the text of Clause 60. The Committee desire that the provisions of penalty for data fiduciary and data processor may be segregated in order to bring greater clarity regarding the provisions for data fiduciary and data processors respectively. The Committee therefore, recommend that Clause 60 may be redrafted as under:-

"60. If any data fiduciary or data processor fails to comply with any directions issued by the Authority under section 51 or order issued by the Authority under section 54,-

(i) such data fiduciary **(***)** shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore **rupees(***); or**

(ii) **such** data processor **shall be liable to a penalty which (***)** may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees."

(Recommendation No. 72)

CHAPTER X –PENALTIES AND COMPENSATION

2.218 The Committee are of the view that the provisions of Chapter X dealing with the Penalties and Compensation required reworking to simplify the procedure for the data principal with respect to the Authority that he/she may approach in case of contravention of the concerned provisions of the Act by the Data fiduciary. The Committee observed that a clarity of language would better allow the people to approach the Data Protection Authority and would also lead to expeditious disposal of complaints made under provisions of Clause X.

2.219 **The Committee approve of all the Clauses of Chapter X. However, the Committee find that there is no single window system for deciding the penalties as well as compensation cases to be decided on receipt of complaint/application before the Data Protection Authority. In the view of the Committee, there must be a single methodology to decide the course of action on the filing of complaint/application. There is a provision of filing complaint to the data fiduciary by the data principal under Clause 32 and there is a provision of seeking compensation under Clause 64 by filing a complaint with the Adjudicating Officer. The Committee therefore feel that the Act should clearly lay down the procedure to be followed under both the situations. Accordingly, the Committee desire that the DPA shall forward the complaint or application filed by the Data Principal to the Adjudicating Officer for adjudging such complaint or application. For incorporating all the provisions as suggested, the Committee desire that a separate Clause may be inserted in the Bill with a marginal heading that reads 'Right to file a complaint or application'**

The Committee, therefore, recommend for insertion of a new Clause before Clause 62 of the Bill. The new Clause may then be numbered as 62 and the numbering of the other Clauses may be changed likewise. The new Clause 62, as inserted by the Committee, reads as under:-

"62. (1) The aggrieved data principal referred to in section 32 may file a complaint to the Authority within such period and in such manner as may be specified by regulations.

(2) The data principal may seek compensation under section 65 by filing an application to the Authority in such form, manner and within such period as may be prescribed.

(3) The Authority may forward the complaint or application filed by the data principal to the Adjudicating Officer for adjudging such complaint or application, as the case may be."

(Recommendation No. 73)

2.220 **Consequent upon the insertion of the new Clause 62, the numbering of the subsequent Clauses may also be likewise amended. Accordingly, the required changes, if any, in other part of the Bill may also be carried out.**

CLAUSE 63- PROCEDURE FOR ADJUDICATION BY ADJUDICATING OFFICER.

2.221 Clause 63(4) reads as below:

"4) While deciding whether to impose a penalty under sub-section (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the following factors, namely:—

(a) nature, gravity and duration of violation taking into account the nature, scope and purpose of processing concerned; Penalty for failure to furnish report, returns, information, etc. Penalty for failure to comply with direction or order issued by Authority. Penalty for contravention where no separate penalty has been provided. Appointment of Adjudicating Officer. Procedure for adjudication by Adjudicating Officer.

(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."

2.222 **The Committee observe that Clause 63(4) in the present form confers unrestricted power to the Adjudicating Officer to impose penalty and to determine the quantum of penalty when a data fiduciary violates the provisions under this Act. Hence, the Committee recommend to add a restrictive expression which specifically mention that the Adjudicating officer shall take into account the guidelines specified by the DPA while determining and imposing penalty. Accordingly, the amended Clause 63(4) [renumbered as 64(4)] may read as below:**

"(4) While deciding whether to impose a penalty under sub-section (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the **guidelines as may be specified by the Authority for determination and imposition of penalty taking into account any of the** following factors, namely:—"

(Recommendation No. 74)

CLAUSE 64 - COMPENSATION

2.223 Clause 64 of the Personal Data Protection Bill, 2019 deals with the compensation to be paid to the data principal and the Clause 64(2) reads as under:-

"(2) The data principal may seek compensation under this section by making a complaint to the Adjudicating Officer in such form and manner as may be prescribed."

2.224 A gist of the suggestions received in the form of Memoranda on Clause 64 is as under:

i Complainant should have the right to appeal against order of DPA not to adjudicate.

ii Penalty should not be imposed only upon a finding of harm, but also include reasonable likelihood of harm.

2.225 **Consequent upon the insertion of the new Clause 62 to the Bill dealing with the complaint mechanism for the purpose of Chapter X, the Committee suggest that original Clause 64(2) being superfluous, may accordingly be deleted.**

2.226 **The Committee note that Clause 64(3) refers to the cases where one or more data principals or any identifiable class of data principals, if they suffer a loss then there is a provision for application for compensation on their behalf. Here the word 'one complaint' is not appropriate. In order**

to replace this word from the legalpoint of view 'representative application' may be used. Accordingly, the Clause 64(3) [renumbered as 65(2)] reads as under:

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

(Recommendation No. 75)

2.227 Clause 64(8) to the Bill reads as under:

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

2.228 **The Committee feel that the structure of the Clause may be amended to reflect the procedure of hearing. Accordingly, the original Clause 64 (8)[(renumbered as Clause 65 (7)]may read as under:**

"**(7)**The (***) procedure for hearing of (***) **an application** under this section **shall be such as may be prescribed."**

(Recommendation No. 76)

CLAUSE 67 - ESTABLISHMENT OF APPELLATE TRIBUNAL

2.229 Clause 67 provides for the establishment of an Appellate Tribunal, including but not limited to its composition and jurisdiction. Clause 67 (2) of the Personal Data Protection Bill, 2019 deals with composition of Appellate Tribunal and it reads as under:-

"(2) The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed".

2.230 The following suggestions were received from the stakeholders:

i The word "two" can be added between the words "than" and "Members" so that the amended Clause would read as under; "The Appellate Tribunal shall consist of a Chairperson and not more than two members to be appointed".

ii Appellate Tribunal Benches should be established under the supervision of each High Court, within 1 year of the date of enactment of the bill.

2.231 In this regard, Justice B.N.Srikrishna Committee Report says, "An appellate tribunal shall be set up to hear and dispose of any appeals from the orders of the DPA and the orders of the Adjudicating Officers under the Adjudication Wing of the DPA. Such a tribunal should consist of a chairperson and such

number of members as notified by the Central Government. The Central Government may also confer powers on an existing tribunal for this purpose if it believes that any existing tribunal is competent to discharge the functions of the appellate tribunal envisaged under the data protection law. The orders of the appellate tribunal will be finally appealable to the Supreme Court of India."

2.232 When asked to clarify the issue of the number of members of Tribunal in the Act during the sitting held on 18 December, 2020, the representative of Legislative Department suggested that the number of members to be appointed may be included in the text of the Bill. MEITY in their counter submission contended that since under the provision of 67(3) the Central government was empowered to create multiple benches of the Tribunal at different locations, the number of members to be appointed may not be included in the Bill and should be left to the discretion of the Central Government.

2.233 **Clause 67(2) relates to the establishment of Appellate Tribunals but 67(2) does not specify the number of Members in the Tribunal. The Committee, after due deliberation and taking into account both submissions of the Ministry of Law and Justice and MEITY, desire that the number of Members of the appellate tribunal should be specified in the Bill and the appellate tribunal should comprise of a Chairperson and not more than 6 members. The Committee therefore, recommend that Clause 67(2) (renumbered as 68(2)) as amended may be read as under:-**

"(2) The Appellate Tribunal shall consist of a Chairperson and **(***)** **such number of** members**, not exceeding six,** to be appointed by the Central Government."

(Recommendation No. 77)

CLAUSE 68 – QUALIFICATIONS, APPOINTMENT, TERM, CONDITIONS OF SERVICE OF MEMBERS

2.234 Clause 68 of the Personal Data Protection Bill, 2019 provides for the Qualifications, appointment, term, conditions of service of Members of the Appellate tribunal. The Clause reads as under:-

"68. (1) A person shall not be qualified for appointment as the Chairperson or a member of the Appellate Tribunal unless he—

(a) in the case of Chairperson, is, or has been a Judge of the Supreme Court or Chief Justice of a High Court;

(b) in the case of a member, has held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person who is well versed in the field of data protection, information technology, data management, data science, data security, cyber and internet laws or any related subject.

(*2*) The Central Government may prescribe the manner of 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."

2.235 A gist of the suggestions received in the form of Memoranda on Clause is as under:

i "Data protection laws, human rights/digital rights and data privacy" should be added as additional criteria for the appointment of members.

ii The salary, allowances, the other terms and conditions of service of the chairperson or member of the Appellate Tribunal should not be varied to their disadvantage.

2.236 While examining Clause 68 dealing with the qualifications of the Members of the Tribunal, the Committee was of the firm opinion that on account of the specialized, technical and fast changing nature of the subject that the Bill deals with and keeping in view the qualifications of members of the global regulators, there is a need for the scope of inclusion of people with considerable expertise and experience in the fields related to data and privacy.

2.237 Clause 68(1) of the Bill provides the qualification necessary for appointment as a Chairperson and Member of the Appellate Tribunal. The Committee feel that keeping in view the dynamic and evolving nature of the subject matter in this regard, the young people, technically qualified, should not be obstructed from being a Member of either the Tribunal or the Data Protection Authority. Additionally, the Committee are also of the view that the Government may find it beneficial to include 'Young blood' who might be in better sync with the technological innovations taking place.

2.238 Clause **68(1)(a) of the Bill provides that the Chairperson of the Appellate Tribunal should be or have been a judge of the Supreme Court or the Chief Justice of a High Court. The Committee accept that the Chairperson should be an individual having a trained judicial mind but find it non-plausible to exclude lawyers, who may have experience with cases dealing with data protection and information security, from the scope of Clause 68(1) (a). The Committee, therefore, desire that the scope**

of Clause 68 may be widened. In this regard, the Committee took note of the Article 124(3) of the Constitution of India that provides for the qualification required for appointment as a judge in the Supreme Court. Article 124(3) of the Constitution of India states as under:-

"(3) A person shall not be qualified for appointment as a Judge of the Supreme Court unless he is a citizen of India and—

(a) has been for at least five years a Judge of a High Court or of two or more such Courts in succession; or

(b) has been for at least ten years an advocate of a High Court or of two or more such Courts in succession; or

(c) is, in the opinion of the President, a distinguished jurist."

2.239 **In the view of the Committee, the qualifications laid down in Article 124(3) of the Constitution may be incorporated in the Bill to widen the scope of Clause 68(1)(a) and allow for the appointment of advocates as well as distinguished jurists as Chairperson of the Appellate Tribunal. Accordingly, the Committee recommend to insert the words' or is qualified to be a Judge of the Supreme Court' at the end of Clause 68(1)(a).**

2.240 **Clause 68(1)(b) provides the qualification required for appointment as a Member of the Tribunal. With respect to Clause 68(1)(b) the Committee are of the view that a Secretary to the Government of India, or somebody at an analogous post, may not necessarily have the expertise required to suitably perform the functions as a Member of the Tribunal and the emphasis, for the purpose of appointment, should be on knowledge/experience of the relevant specialized fields of knowledge rather than the post. At the same time, the Committee do not want to restrict the entry of bureaucrats with expertise in the relevant field from becoming Members of the Tribunal. The Committee also desire that there should be no age restriction with regard to the appointment as a Member of the Tribunal and young people with the required expertise may also find place as a Member.**

2.241 **The Committee, accordingly, recommend that after incorporation of the aforementioned changes, the Clause 68(1)(a) and (b) (renumbered as Clause 69(1)(a) and (b) may be as under:**

"69.(1) A person shall not be qualified for appointment as the Chairperson or a Member of the Appellate Tribunal unless he—

(a) in the case of Chairperson, is , or has been a Judge of the Supreme Court or Chief Justice of a High Court **or is qualified to be a Judge of the Supreme Court;**

(b) in the case of a **M**ember, **(***)is** a person who is **(***)an expert and has ability, integrity, standing and specialized knowledge with an experience of not less than twenty years** in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, **public administration** or any related subject."

(Recommendation No. 78)

CLAUSE 72- APPEALS TO APPELLATE TRIBUNAL

2.242 Clause 72 of the Bill reads as under:

"(1) Any person aggrieved by the decision of the Authority, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed:

Provided that the Appellate Tribunal may entertain any appeal 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.

(2) On receipt of an appeal 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 deems fit.

(3) 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.

(4) 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 toin the appeal 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."

2.243 In this regard, one of the suggestion received by the Committee is as under:Replace Section 72(1) with the following:

(1) Any person aggrieved by the decision of the Authority or the Adjudicating Officer, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed.

2.244 **The Committee note that as per the extant provision an appeal to the tribunal lies only against a decision of the Data Protection Authority. In this regard, the Committee are of the view that appeal should lie against a decision as well as against an order of the Authority. Moreover, the right provided under this section should not be confined solely to the**

decision or order of the Data Protection Authority but should also be available against any decision or order of the Adjudicating officer. Accordingly, the Committee desire that in Clause 72(1) the words 'or order' be inserted after the word 'decision' and the words 'or Adjudicating Officer' after the word 'Authority'. Consequently, the words 'or Adjudicating Officer' may also be inserted in Clause 72(3) after the word 'Authority'. After the inclusion of these changes, Clause 72 (renumbered as Clause 73) be may be read as under:-

"73.(1) Any person aggrieved by the decision **or order** of the Authority **or an Adjudicating Officer**, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed:

Provided that the Appellate Tribunal may entertain any appeal 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.

(2) On receipt of an appeal 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 deems fit.

(3) 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 **or the Adjudicating Officer**, as the case may be.

(4) 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 preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal **(***)** and make such orders as it thinks fit."

(Recommendation No. 79)

CLAUSE 74 – ORDERS PASSED BY APPELLATE TRIBUNAL TO BE EXECUTABLE AS A DECREE

2.245 Clause 74 deals with execution of Tribunal orders. The Clause, as in the Personal Data Protection Bill, 2019, reads as under:

"(*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."

2.246 **The Committee observe that while Clause 74(1) already empowers the Appellate Tribunal with the powers of the Civil Court for execution of their orders, sub-clause(2) of Clause 74 dilutes the same by allowing for transmission of any order of the Tribunal to a civil court, having local jurisdiction, for execution. This, in the view of the Committee, may lead to unnecessary protracted litigation. The Committee therefore, recommend that Clause 74(2) may be removed in its entirety from the Bill. The Committee also suggest certain minor modifications in the language of Clause 74(1) by replacing the words 'An order passed' (Page 33, line 29 of the original text) with the words 'Every order made'. Consequently, Clause 74(1) [renumbered as Clause 75] as amended by the Committee may now be read as under:-**

"75.(***)Every order **(***) made** 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) (***)"

(Recommendation No. 80)

CLAUSE 75 – APPEAL TO SUPREME COURT

2.247 Clause 75 of the Bill reads as under:

75. (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law, an appeal shall lie against any order of the Appellate Tribunal, not being an interlocutory order, to the Supreme Court on any substantial question of law.

(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:

Provided that the Supreme Court 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.

2.248 The Committee find that the provision made under Clause 75(2) mentions the decision or order made by the Appellate Tribunal with the consent of parties is redundant in nature. Therefore, sub-clause (2), of Clause (3) may be renumbered as (2).

2.249 **The Committee also feel that the period for making appeal within ninety days is on the higher side and it should be made sixty days being appropriate for appeals. The renumbered Clause 75(2) may be amended and consequential changes may be made in the numbering of Clause for 75 as 76 to read as under:**

"(**2**) Every appeal **made** under this section shall be preferred within a period of (***) **sixty** days from the date of the decision or order appealed against:

Provided that the Supreme Court may entertain the appeal after the expiry of the said period of (***) **sixty** days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time."

(Recommendation No. 81)

CLAUSE 76 – RIGHT TO LEGAL REPRESENTATION

2.250 Clause 76 of the Personal Data Protection Bill, 2019 provides for the right to legal representation and the Clause reads as under:-

"76. The applicant or appellant may either appear in person or 136uthorize one or more legal practitioners or any of its officers to present his 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."

2.251 With respect to Clause 76, the Committee received a suggestion from a stakeholder stating that the term 'advocate' under Clause 76 should be defined as per the Advocate Act.

2.252 The Committee was of the view that, the applicant or the appellant should also have the option to authorise an expert, who in his/her view may be better able to present his or her case before the Tribunal. In this regard, the MEITY submitted that the term "or any of its officer" covers that point and would allow the applicant to call an expert. The Committee agreed to the view of the Ministry, but decided to insert the word "*or experts*" after the words "*or any of its officer*", for the sake of bringing in greater clarity.

2.253 **The Committee note that the Clause makes a provision that an applicant or appellant may present his case before the Tribunal either in person, or through a legal practitioner or through any of its officer. The Committee, however, feel that the matter relating to data needs the feedback or support of domain experts as well. The Committee therefore desire that the applicant/appellant should have the right to represent his case before**

the Tribunal through any domain expert whether employed by him or from outside. Therefore, accordingly, the words 'or experts' should be inserted after the words 'its officers' in the said Clause. Moreover, the Committee feel that words "and includes a pleader" be deleted from the Explanation to Clause 76 since the word 'pleader' is antiquated and the words advocate or attorney convey the desired meaning of the term legal practitioner.

2.254 **The amended Clause 76 (to be renumbered as Clause 77) may be read as under:-**

"77. The applicant or appellant may either appear in person or authorize one or more legal practitioners or any of its officers **or experts** to present his or its case before the Appellate Tribunal.

Explanation.—For the purposes of this section, **the expression** "legal practitioner" **shall** include (***) an advocate or an attorney**(***)**."

(Recommendation No. 82)

CLAUSE 84- OFFENCES BY COMPANIES

2.255 Clause 84 of the Bill reads as under:

"84. (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 he proves that the offence was committed without his knowledge or that he 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 anybody 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 thereof."

2.256 **The Committee understand that any offence may be attributed to specific part of the business and not to the entire business of the company. The Committee, therefore desire that words "that part of" may be added before "the business" to make this Clause clear and comprehensive. The Committee further observe that Clause 84(2) [renumbered as 85(2)] sets the alleged person free if it is proved that the offence was committed without his knowledge or he has exercised due diligence to prevent such offence. But the Committee find that this sub-clause should explicitly mention that the person shall be free from 'proceedings' and 'punishment' once he proves his innocence. Hence the Committee recommend to amend the sub-clauses [renumbered as Clause 85(1) and85(2)] as follows:**

85.(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 **(***) that part of** the business of the company **to which the offence relates**, as well as the company, (***) shall be liable to be proceeded against and punished accordingly.

"(2) Nothing contained in sub-section (1) shall render any such person liable to **(***) be proceeded against and punished accordingly under** this Act, if he proves that the offence was committed without his knowledge or that he had exercised all due diligence to prevent the commission of such offence."

(Recommendation No. 83)

2.257 **The Committee note that Clause 84 relates to offences by the companies. However, sub-clauses (1), (2), and (3) do not include any provision for liability of independent Director or a non-executive Director of a company. Thus, the Committee desire that a proviso to sub-clause (3) may be inserted to cover these two categories of Directors also. The proviso to sub-clause (3) of the renumbered Clause 85 may be framed as under:**

"**Provided that an independent director and a non-executive director of a company shall be held liable only if it is shown that the acts of omission or commission by the company had occurred with his knowledge or with his consent attributable to him or where he had not acted diligently."**

(Recommendation No. 84)

CLAUSE 85 – OFFENCES BY STATE

2.258 Clause 85 seeks to list out the provisions relating to commission of offence, under this Act, by any State Government or Central Government Department or agency. The Clause reads as under:-

"85. (1) Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body 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 he proves that the offence was committed without his knowledge or that he 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.

(4) Notwithstanding anything in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply."

2.259 The following suggestion was received in the form of memorandum:

"The person in charge should be liable, based on the offence being committed. It should not be based on the offence being proved."

2.260 The Ministry submitted before the Committee on 18 December, 2020 that considering that State is a sovereign entity it may not be directly indicated as responsible for any offence. Therefore, the marginal heading to the Clause 85 which reads "Offences by State" may be amended and the same may be read as "Offences by Public Data fiduciaries".

2.261 **Accepting the submission of MEITY, the Committee find that the objective of this Clause is to actually indicate the data fiduciaries of the Government sector. The Committee therefore, desire that the marginal heading to the Clause 85(renumbered Clause 86) may be amended to read "Offences by Government Data fiduciaries".**

2.262 **The Committee express their concern with respect to the capacity of Government departments to protect the large volume of data that they collect. The Committee observe that since the Government will be a significant data fiduciary, as per the provisions of the Bill, it will have to establish Standard Operating Procedures in the Ministries and Departments etc. to protect the huge amount of data that is collected. The Committee note that as per the provision of Clause 85(1) and Clause 85(3) any offence, under the Act, is said to be committed by a department, authority or body of State. In the view of the Committee, actually the offence should be said to be committed by any particular government data fiduciary and not by any department, authority or body of State. Moreover, as per the provision of the Clause the responsibility of any offence under this Act is placed on the Head of the Department concerned. With respect to Clause 85(1) &(3), the Committee feel that if the responsibility for any offence with respect to the provisions of this Act, is placed on the Head of the Department, it may impede decision making process in the department. Further, this will likely create multiple hurdles in the everyday functioning of the government department. In the view of the Committee, in case of any offence under the provisions of this Act, the Head of the Department concerned should first conduct an in-house inquiry to determine the person or officer responsible for the particular offence and subsequently the liability may be decided. In view of the above, Clause 85 (renumbered as Clause 86) may be modified to be read as under:-**

"86.(1) Where (***) an offence under this Act has been committed by any (***)**Government data fiduciary, an in-house enquiry shall be conducted by the Head of Office of the concerned data fiduciary and the person or officer concerned responsible for such offence** shall be liable to be proceeded against and punished accordingly.

(2) Nothing contained in sub-section (1) shall render any such person **or officer** liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he 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 **(***) Government data fiduciary** 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 **(***) person or officer concerned referred to in sub-section (1)**, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(4)Notwithstanding anything **contained** in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply."

(Recommendation No. 85)

CLAUSE 86 – POWER OF CENTRAL GOVERNMENT TO ISSUE DIRECTIONS

2.263 Clause 86 of the Personal Data Protection Bill, 2019 which deals with power of Central Government to issue directions to the Authority reads as under:-

"86. (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:

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

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

2.264 A gist of the suggestions received in the form of Memoranda on Clause is as under:

i This provision undermines the DPA's authority and should be deleted.

ii Power to issue directions to the DPA should be limited to policy issues. Administrative and technical matters and matters that impinge upon the DPA's independence should not be covered under the scope of this power.

2.265 **The Committee find that the Central Government has been empowered to issue directions to the Authority under Clause 86 only on the questions of policy. The Committee also note that under the provision of Clause 86 (2) the Authority is bound by the directions of the Central Government only on questions of policy and side by side a safeguard has been provided where the Authority is given an opportunity to express its views before any direction is given under this sub-section.**

2.266 **The Committee feel that the Authority should be bound by the directions of the Central Government under all cases and not just on questions of policy. The Committee, therefore, recommend that the words 'on questions of policy' be removed from Clause 86(2). Further, after the**

removal of the words 'on question of policy' from Clause 86(2), the directions of Central Government are final in every case. Thus, Clause 86(3) becomes superfluous and may be deleted in its entirety. Clause 86 (renumbered as Clause 87) thus amended by the Committee may be read as under:-

"87.(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 **(***)** as the Central Government may give in writing to it from time to time:

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

(3) **(***)"**

(Recommendation No. 86)

CLAUSE 91 – ACT TO PROMOTE FRAMING OF POLICIES FOR DIGITAL ECONOMY, ETC.

2.267 Clause 91 of the Personal Data Protection Bill, 2019 seeks to empower the Central Government to frame policies for digital economy in respect of non-personal data by giving it the power to collect any non-personal data or anonymised personal data from any data fiduciary. The Clause reads as under:-

"91. (1) Nothing in this Act shall prevent the Central Government from framing of any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policy do not govern personal data.

(2) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data.

(3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed."

2.268 A gist of the suggestions received in the form of Memoranda on Clause is as under:

i The provision should be deleted as it is outside the scope of this Act.

ii The grounds for application of this Clause need to be specified.

iii There are no safeguards for protecting the privacy of data principals in the case of re-identification risks associated with anonymized data, IPR, trade secrets, and applicability of RTI Act.

iv Ethics certification and audits may be made mandatory to such data sharing mandates, and risk of harm may be made a criteria for allowing such data sharing.

2.269 In this regard, MEITY submitted as, "under 91(2), the directions of the Central Government are limited to certain specific purposes. The first one is to enable better targeting of delivery of services and the second for the formulation of evidence based policies. It is only for these two specific purposes, the Central Government, in consultation with the DPA, can issue directions to any data fiduciary to provide any anonymized personal data or other non-personal data."

2.270 While examining the Clause, the Committee in the sitting held on 29 December, 2020 felt that the Central Government should place before the Parliament the directions made by it under sub-section(2). MEITY submitted that Clause 95 and 97 provides for the rules, regulations, orders and notifications made under the Act to be laid before the Parliament and directions made under Clause 91(2) may be exempted from being placed before the Parliament.

2.271 **Clause 91(1) provides the Central Government the freedom to frame policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse such that they do not govern personal data. But in this Clause there is no specific mention of policy regarding non personal data including anonymised personal data and the words 'inso far as such policy do not govern personal data' does not provide clarity with regard to the data that is excluded from the ambit of the power of Central Government under Clause 91.Therefore, the Committee desire that the words 'in so far as such policy do not govern personal data' be removed from 91(1) and be replaced with the words ' handling of non-personal data including anonymised personal data'. Clause 91(1) [renumbered as 92(1)]as amended by the Committee may be read as under:-**

"**92.**(1) Nothing in this Act shall prevent the Central Government from framing (***) any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse,**(***)** **and handling of non personal data including anonymised**personal data."

(Recommendation No. 87)

2.272 **Moreover, the explanation regarding the expression of non-personal data given in 91(2) may be deleted since this explanation has already been incorporated under newly inserted Clause3(28).**

2.273 **The Committee also note that since the Bill already has provisions for the rules, regulations, orders and notifications including the Annual report of the DPA to be laid before the Parliament, the directions issued from time to time under Clause 91(2) may also be put forth before the Parliament in the form of a report to be placed annually before both the Houses. This will ensure greater accountability of the executive towards the legislature with respect to the directions under this Bill. The Committee, accordingly, recommend amendment in Clause 91(3) [renumbered as 92(3)] as under:-**

"(3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed **and such disclosure shall be included in its Annual Report which shall be laid before each House of Parliament**"

(Recommendation No. 88)

CLAUSE 93 - POWER TO MAKE RULES (OF THE CENTRAL GOVERTNMENT)

2.274 With regard to Clause 93, the gist of suggestions received by the Committee in the form of memoranda is as follows:

i. The power to prescribe new categories of sensitive personal data should be provided to the DPA and should be subject to stakeholder consultation.

ii. The power to prescribe methods for voluntary identification by social media intermediaries should be omitted from this Act.

iii. Power to make rules under Clause 93(2)(f) regarding countries or international organisations to which cross border transfers may be permitted require Parliamentary scrutiny.

iv. A mandatory consultation and transparency requirement should be imposed on the Central Government's power to make Rules under the Act.

v. Power to prescribe other factors to be taken into account regarding age verification mechanisms specified by the authority should be provided to the DPA and not the Central Government as the DPA are likely to have the necessary technical expertise in this regard.

2.275 **On account of the changes made in the substantive provisions in the Bill ranging from Clause 1 to Clause 92 of the extant Bill, the Committee also direct that the following consequent changes may also be made in the rule making power of the central government as enshrined in Clause 93 (renumbered Clause 94):-**

i. Addition of the words 'and subject to the condition of previous publication' after the word 'notification' in Clause 94(1) ‘, ‘not inconsistent with the provisions of this Act, after the word ‘rules and replace the word ‘provisions’ with ‘purposes’.

ii. Removal of Clause 94(2) (a)

iii. Insertion of a new Clause 94(2)(a) as under:

"(a) (***) any other harm under sub-clause (xii) of clause (23) of section 2;"

iv. Insertion of new Clause 94(2)(b) as under:
“(b) the manner in which a data fiduciary can share, transfer or transmit the personal data to any person as part of any business transaction under sub-section (4) of section 8;”
The numbering of the Clause may be likewise amended.

v. Insertion of Clause 94(2)(e) as under:-
“(e) the steps to be taken by the Authority in case of breach of non-personal data under sub-section (6) of section 25;”

vi. Insertion of a new Clause 94(2)(f) as under:
“(f) the threshold with respect to users of social media platform under sub-clause (i) of clause (f) of sub-section (1) and different thresholds for different classes of social media platforms under the proviso to clause (f) of sub-section (1) of section 26;”

The numbering of the Clause may be likewise amended.

vii. Removal of Clause 94(2)(e) and changing the numbering of the Clause accordingly.

viii. Insertion of a new Clause 94(2)(h) and Clause 94(2)(i) as under:

"(h) (***) the manner of registration of data auditors under sub-section (4) of section 29;
(i) the qualifications and experience of a data protection officer under sub-section (1) of section 30;"

ix. Insertion of Clause 94(2)(r) as under:-
(r) the penalties for contravening of certain provisions of this Act by data fiduciaries including by State under sub-sections (1), (2) and (3) of section 57;

x. Insertion of Clause 94(2)(s) as under:-
"(s) the form, manner and the period for filing an application for compensation under sub-section (2) of section 62;"

xi. Insertion of new Clause 94(2)(ze) as under:-
"(ze) the details of biometric data not to be processed under section 93;"

(Recommendation No. 89)

CLAUSE 94 - POWER TO MAKE REGULATIONS (OF THE DATA PROTECTION AUTHORITY)

2.276 With respect to the regulation making power of the Authority, gist of suggestions received by the Committee is as under:

i The power to make regulations regarding reasonable purposes for which personal data may be processed under Clause 14(2) should be provided under Clause 94.

ii The meaning and nature of consent managers needs more clarity under the Bill as there is no guidance in the Bill regarding their roles and safeguards and their operations.

iii A mandatory consultation and transparency requirement should be imposed on the DPA's power to make Regulations under the Act.

iv Standards for anonymization should be provided by Regulations.

v Further categories of sensitive personal data should be specified by the DPA in consultation with stakeholders.

2.277 **On account of the changes made in provisions ranging from Clause 1 to Clause 92 of the extant Bill, the Committee also direct that the following consequent changes may also be made in the regulation making power of the Data Protection Authority as enshrined in Clause 94 (renumbered Clause 95):-**

i. **Insertion of the words 'and subject to the condition of previous publication' after the word 'notification', replacing the word "provisions" with "purposes" and replacing the words 'consistent with this Act' with the words 'not inconsistent with the provisions of this Act' in Clause 95(1) {earlier 94(1)}.**

ii. **Insertion of the words 'the reasonable purposes under sub-section (1)' in Clause 95(2)(c)so that the whole Clause 95(2)(c) may now be read as under:-**

"(c) **the reasonable purposes under sub-section (1)** and the safeguards for protecting the rights of data principals under sub-section (3) of section 14;"

iii. **Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(f) to be read as under:-**

"(f) the manner in which the data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them under sub-section (3) of section 17;"

iv. **Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(g) to be read as under:-**

"(g) the conditions and the manner in which the data principal shall have the right to correction and erasure of the personal data under section 18;"

v. **Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(h) to be read as under:-**

"(h) the manner for determining the compliance which would not be technically feasible for non-application of the provisions of sub-section (1) under clause (b) of sub-section (2) of section 19;"

vi. **Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(j) to be read as under:-**

"**(j) the conditions under which the data fiduciary shall oblige to comply with the request made by the data principal under sub-section (5) of section 21;"**

vii. Insertion of the words 'and the period' after the word 'manner' in 94(2)(g).(renumbered as 95(2)(k))

"(i) the manner **and the period** for submission of privacy by design policy under sub-section (2) of section 22;"

viii. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(l) to be read as under:-

"(l) the form and manner for making the information available, any other information to be maintained by the data fiduciary under sub-section (1) and the manner of notifying the important operations in the processing of personal data related to data principal under sub-section (2) of section 23;"

ix. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(n) to be read as under:-

***"*(n) the manner of review of security safeguards periodically by data fiduciary or data processor under sub-section (2) of section 24;"**

x. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(o) to be read as under:-

"**(o) the form of notice under sub-section (2) of section 25;"**

xi. Insertion of words "**and the conditionsfor processing under sub-section (5) of section 27; in Clause 94(2)(j) (renumbered as 94(2)(q)**

xii. Removal of Clause 94 (2) (m) *and* changing the numbering of the sub clauses accordingly

xiii. Insertion of the word '*archiving'* after the word '*research'* in Clause 94(2)(o) (renumbered as 94(2)(u)).

xiv. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(v) to be read as under:-

"(v) the manner of inclusion by the data fiduciary for inclusion in the Sandbox under sub-section (2) and any other information required to be included in the Sandbox by the data fiduciary under clause (d) of sub-section (3) of section 40;"

xv. Rewording of Clause 95(2)(y) (earlier 94(2)(r)), so that now it may be read as under:-

"(**y**) the **manner, period and** form(***) for providing information to the Authority by the data fiduciary **or data processor** under sub-section (3) of section 52;"

xvi. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(z) to be read as under:-

***"*(z) the place and time for discovery and production of books of account, data and other documents to the Authority or Inquiry Officer under clause (a) of sub-section (8) of section 53;"**

xvii. Insertion of a new sub-clause under Clause 95 (earlier Clause 94) namely, 95(2)(za) to be read as under:-

***"*(y) the period and the manner of filing a complaint by the data principal before the Authority under sub-section (1) of section 62;"**

(Recommendation No. 90)

THE SCHEDULE

2.278 The Schedule of the Personal Data Protection Bill, 2019 reads as under:

"AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000

(21 OF 2000)

1. Section 43A of the Information Technology Act, 2000 (hereafter in this Schedule referred to as the principal Act) shall be omitted.

2. In section 87 of the principal Act, in sub-section (2), Clause (ob) shall be omitted."

2.279 **The Committee consider that in view of amendments made in the Personal Data Protection Bill, 2019, the Information Technology Act, 2000 also need to be amended. The schedule of the Bill depicts the amendments to be brought in related Acts. In this case, the original Bill mentions two amendments in the IT ACT, 2000 ie. in section 43 A and section 87. The Committee, however, find that after the commencement of Data Protection Act, 2021 section 81 of the IT Act, 2000 also needs to be amended so that the words and figures "or the Information Technology Act, 2000" are inserted after the words "the Patents Act, 1970". Accordingly, the Committee do amend The Schedule as under:**

"1. Section 43A of the Information Technology Act, 2000 (hereafter in this Schedule referred to as the principal Act) shall be omitted.

2. In section 81 of the principal Act, in the proviso, after the words and figures "the Patents Act, 1970", the words and figures "or the Data Protection Act, 2021" shall be inserted.

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

(Recommendation No. 91)

2.280 **Consequently, the marginal note of para 2 of the schedule, as inserted by the Committee, may read as "Amendment of section 81."**

2.281 **Drafting corrections/improvement**

Sl. No.:	Clause No.:	Drafting corrections/improvement
1.	Long Title	At Page No.:1 Add "to" before the words "specify", "create" and "protect". For "social media intermediary" substitute social media platforms". For "laying" substitute "to lay".
2.	Preamble	At Page No.: 2 For "Seventieth Year" substitute "Seventy-second Year"
3.	2 Marginal Heading	Insert "and non-personal data" after "personal data"
4.	2	At Page No.:2, Line No.:9 Add "shall apply to" after "this Act" At Page No.:2, Line No.:10 Omit "shall apply to-" At Page No.:2, Line No.: 22 After word "India" add ";and".
5.	3(1)	At Page No.:2, Line No.:27 For "section 62' substitute "section 63"
6.	3(4)	At Page No.:2, Line No.:34 For "section 67' substitute "section 68"
7.	3(6)	At Page No.:2, Line No.:38 After "given" add "or otherwise"
8.	3(13)	At Page No.:3, Line No.:11 For "the" substitute "a" before "State" After word "company" add words "a non-government organization" . Omit "any" before "juristic entity".
9.	3(15)	At Page No.:3, Line No.:15

		After word “company” add words “a non-government organization” For “the” substitute “a” before “State” After word “company” add words “a non-government organization” . Omit “any” before “juristic entity”.
10.	3(19)	At Page No.:3, Line No.:29 For “give” substitute “gives”. At Page No.:3, Line No.:31 For “result” substitute “results”.
11.	3(20)	At Page No.:3, Line No.:41 For “good” substitute “goods”. At Page No.:3, Line No.:45 Omit “or”
12.	3(21)	At Page No.:4, Line No.:6 For “associating” substitute “associated with”.
13.	3(25)	At Page No.:4, Line No.:19 For “expression” substitute “expressions”. At Page No.:4, Line No.:19 After “notify”, add “and “notified””
14.	3(29)	At Page No.:4, Line No.:38 For “or” substitute “including” At Page No.:4, Line No.:39 Omit “of” after “destruction”
15.	5	At Page No.:6, Line No.:9 After “incidental” add “thereto”
16.	7	At Page No.:6, Line No.:15 Omit “a notice” after “data principal” At Page No.:6, Line No.:17 Add “is” before “reasonably” At Page No.:6, Line No.:17 Add “a notice” before “containing” At Page No.:6, Line No.:27 For “specified” substitute “provided” At Page No.:6, Line No.: 32 Add “the” before “information” At Page No.:7, Line No.: 2 For “a reasonable person” substitute “an individual” At Page No.:7, Line No.: 2 For “where” substitute “to the extent”

		At Page No.:7, Line No.: 4 Omit “substantially” after “notice”
17.	8(3)	At Page No.:7, Line No.:13 Omit “take reasonable steps to”. At Page No.:7, Line No.:13 For “requirement” substitute “requirements”
18.	10	At Page No.:7, Line No.:27 After “Act” add words “and the rules and regulations made thereunder”
19.	11	At Page No.:8, Line No.:05 Add “to be drawn either” after “inference” At Page No.:8, Line No.:05 For “in” substitute “or” At Page No.:8, Line No.:15 Omit “all legal” before “consequences”, and add “the” At Page No.:8, Line No.:15 For “effects of such withdrawal” substitute “same”.
20.	12	At Page No.:8, Line No.:22 Insert “including” before “for-” At Page No.:8, Line No.:27 Omit “or” after “Legislature;” At Page No.:8, Line No.:28 For "order or judgment" substitute "judgment or order"; Insert ", quasi-judicial authority" after “court”
21.	13	At Page No.:8, Line No.:36 After “subject to” add “the provisions contained in” At Page No.:8, Line No.:38
22.	14	At Page No.:9, Line No.:12 Omit “such” before “reasonable”. At Page No.:9, Line No.:14 Add “legitimate” before “interest” At Page No.:9, Line No.:25 Omit word "and" after "acquisition" At Page No.:9, Line No.:41, Omit “substantial” before “prejudice”
23.	15	At Page No.:9, Line No.:46 Omit “the” after “by”

		At Page No.:10, Line No.:03 Add “the” after “to”
24.	Chapter IV Heading	At Page No.:10, Line No.:09 Omit “and sensitive personal data” after “personal data”
25.	16 Marginal Heading	At Page No.:10 Omit “and sensitive personal data” after “personal data”
26.	16	At Page No.:10, Line No.:09 Omit “and sensitive personal data”. At Page No.:10, Line No.: 11 Omit “and is in the best interests of.” At Page No.:10, Line No.: 15 For words " be specified by regulations, taking" substitute "take” At Page No.:10, Line No.: 19 Add “the” before “possibility” At Page No.:10, Line No.: 25 Omit “guardian” before “data fiduciary”. At Page No.:10, Line No.: 28 For “(5)” substitute “(4)”
27.	17	At Page No.:10, Line No.: 39 Add “the” before “confirmation” At Page No.:11, Line No.: 5 For " person" substitute " individual in a similar context”
28.	18	At Page No.:11, Line No.: 15 For “updating” substitute “updation” At Page No.:11, Line No.: 27 After “accordance with” add “ the provisions contained in" At Page No.:11, Line No.: 27 Add words "and practicable" after "necessary" At Page No.:11, Line No.: 29 For “particularly where” substitute “having regard to the impact” At Page No.:11, Line No.: 30 Omit words "an impact" after "have”
29.	19	At Page No.:11, Line No.: 41 For the word "have" substitute "Transfer" and omit "transferred"

		At Page No.:11, Line No.: 44 For the words "of law" substitute " with any judgement"; At Page No.:11, Line No.: 45 For the words "of court" substitute " any court, quasi-judicial authority or Tribunal"
30.	20	At Page No.:12, Line No.s:02 Add “or processing” before “of his” At Page No.:12, Line No.s:02, 14, 20, 24, 26,28 After “disclosure” add “ or processing”. At Page No.:12, Line No.:12 Omit “clause” before “(c)” At Page No.:12, Line No.:30 Add “any longer” after “sub-section” At Page No.:12, Line No.:34 Add “under section 73” after “Tribunal” Here section 73 refers to the new Clause inserted in the Bill by the Committee.
31.	21	At Page No.:12, Line No.:42 For “referred to in” substitute “under” At Page No.:12, Line No.:37 For “consent manager” substitute “Consent Manager” At Page No.:12, Line No.:42 For “to in” substitute “under” At Page No.:12, Line No.:43 Add “clause” before “(b)”
32.	22	At Page No.:13, Line No.:20 Omit “Subject to the regulations made by the Authority" before "the data fiduciary" At Page No.:13, Line No.:23 Add “Subject to the provisions contained in sub-section (2),” before “The Authority”.
33.	23	At Page No.:13, Line No.:42 Omit “and” after “out;” At Page No.:14, Line No.s:5, 7 &9 For “consent manager” substitute “Consent Manager”
34.	25	Omit “personal” before “data”

	Marginal Heading	
35.	25	At Page No.:14, Line No.:26 For “inform” substitute “report to” At Page No.:14, Line No.:27,32 & 33 For “the” substitute “such”. At Page No.:14, Line No.:39 For “specified” substitute “provided” At Page No.:14, Line No.:41 After “without” insert “any”.
36.	26	At Page No. 15, Line No.: 7 Add words "any of the" before following At Page No. 15, Line No.: 13 Omit “and” after “processing;” At Page No. 15, Line No.: 17 Add word “contained” after “anything” At Page No. 15, Line No.: 17 For "of the opinion" substitute "satisfied" At Page No.:15, Line No.:19 For “specified” substitute “provided” At Page No.:15, Line No.:20 For “data fiduciary” after “class of” substitute “data fiduciaries”
37.	27	At Page No.:15, Line No.: 39 For “the” substitute “a”. At Page No.:16, Line No.:2 For “fiduciary” substitute “fiduciaries” At Page No. 16, Line No.: 15 For "reason to believe" subsitute "satisfied itself" At Page No.:16, Line No.: 16 For “the Authority” substitute “it”. At Page No.:16, Line No.: 18 For “the Authority may deem fit” substitute “may be specified by regulations.”
38.	28	At Page No.:16, Line No.:27 For “intermediary” substitute “platform”. At Page No.:16, Line No.:28 For “4"substitute “1”. At Page No.:16, Line No.:28 For “users” substitute “persons”. At Page No.:16, Line No.:31

		For “user” substitute “person”.
39.	29	At Page No.:19, Line No.:5 Add “and shall encourage the practice of appropriate concurrent audits” after “section” At Page No.:17, Line No.:9 Omit “it” after “ may be specified” At Page No.:17, line No.:10 Omit “under this Act” At Page No.:17, Line No.:15 For “of the view” substitute “satisfied” At Page No.:17, Line No.:17 For “the data” substitute “such data”
40.	30	At Page No. 17, Line No.: 20 For “qualification” substitute “qualifications” For “specified by regulations” substitute “prescribed” At Page No. 17, Line No.: 21 Add “namely” after “functions” At Page No. 17, Line No.: 32 For “grievances” substitute “grievance”
41.	31	At Page No. 18, Line No.: 3 Add "as" before "confidential"
42.	32	At Page No. 18, Line No.: 17 For “in such manner as may be prescribed” substitute “under section 62” Here section 62 refers to the new Clause inserted in the Bill by the Committee.
43.	33	At Page No. 18, Line No.: 20 Add "provided" after "condition"
44.	34	At Page No.: 18, Line No.: 37 Omit “or” appearing at the end. At Page No.: 18, Line No.: 39 For "entity" substitute "entities" before "in a country" At Page No.: 18, Line No.: 43 Omit “and” appearing at the end. At Page No.: 19, Line No.: 2 Add “;and” after the word “jurisdiction”

		At Page No.:19 , Line No.:4 Add 'or' after “prescribed;” appearing at the end. At Page No.:19 , Line No.:5 Add “in consultation with the Central government” after “Authority” At Page No.: 19, Line No.: 11 For "entity" substitute "entities" before “in a country” At Page No.:19 , Line No.:14 For “interest” substitute “interests” At Page No.:19 , Line No.:16 For 'notified' substitute 'informed'
45.	35	At Page No.: 19, Line No.: 20 Add " Notwithstanding anything contained in any law for the time being in force," before "where" At Page No.: 19, Line No.: 22,25 Add "or" after "States" At Page No.:19 , Line No.:35 Add ';and' at the end of the line.
46.	36	At Page No.: 19, Line No.: 38 Add “the” before “personal data” At Page No.: 19, Line No.: 39 Omit "any other" At Page No.: 20, Line No.: 1,4,6 & 9 Add “the” at the beginning At Page No.:20 , Line No.:10 For “any” substitute “rules and regulations made under this Act” At Page No.:20 , Line No.:11 Add ‘statutory” before “media” Omit “self” before “regulatory”
47.	39 Marginal Heading	At Page No.: 20 For “manual” substitute “ nonautomated”
48.	40	At age No.:20, Line No.:42 For "shall" substitute "may" At Page No.: 21, Line No.:22 For "specify clear and specific purposes" substitute "comply with the provisions" At Page No.: 21, Line No.:25 Omit " the " after "on" At Page No.:26, Line No.:26

		Omit "obligations under" before "sections"
49.	42 Marginal Heading	Add "Chairperson and" before "Members"
50.	42	At Page No.: 21, Line No.:42 For "selection committee" substitute "Selection Committee" At Page No.: 21, Line No.:43 For "selection committee" substitute "Selection Committee" At Page No.: 22, Line No.:6 For "qualification" substitute "qualifications" At Page No.: 22, Line No.:7 Omit "and" after "of" At Page No.: 22, Line No.:10 For "member " substitute "Member"
51.	44	At Page No.: 22, Line No.:32 For "member " substitute "Member" At Page No.: 22, Line No.:38 For "their" substitute "his"; For “member” substitute “Member” At Page No.: 22, Line No.:40 For "a " substitute "an" and Omit "reasonable"
52.	45	At Page No.: 22, Line No.:42 Add " in the conduct" after "direction" Add "he" after "and" Omit “also” after “shall” Add "in addition to presiding over the meetings of the Authority " before "exercise"
53.	46	At Page No.: 23, Line No.:5 Add "over" after "preside" At Page No.: 23, Line No.:8 For "member " substitute "Member
54.	48	At Page No.: 23, Line No.:20 Omit "of"
55.	49	At Page No.: 23, Line No.:30 Add " the rules and regulations made thereunder:" after "and" At Page No.: 23, Line No.:31 Omit "personal" before "data" At Page No. 24, Line No.: 12 Omit the word 'and' At Page No.: 24, Line No.:18 For "the" substitute"such" At Page No.: 24, Line No.:18 Add "for the time being in force" after law

56.	50	At Page No.: 25, Line No.:19 Omit "personal" before "data" At Page No.: 25, Line No.:19 Omit "the" before "view" At Page No.:25 Line No.:19 Add "or relevant" after "necessary"
57.	51	At Page No.: 25, Line No.:27 For "a" substitute "an" Omit "reasonable" before "opportunity" For "fiduciaries" subsitute "fiduciary" Add "the" before "data"
58.	53	At Page No.: 25, Line No.:46 For "interest" substitute "interests" At Page No.: 26, Line No.:19 For "Inquiry Officer" substitute "scope of inquiry" At Page No.: 26, Line No.:30 Add “data” after “account” At Page No.: 26, Line No.:31 Add "by regulations" after "specified" At Page No.: 26, Line No.:34 Omit “or” after “register” Add "or data" after "record"
59.	54	At Page No. 26, Line No.s: 44 and 46 For the word 'require' substitute 'direct' At Page No.: 27, Line No.:6 For the word 'require' substitute 'direct' At Page No.: 27, Line No.:5 For “flow” substitute “transfer” At Page No.: 27, Line No.: 7 For “deems” substitute “deem” At Page No.: 27, Line No.:9 Add "under section 73 " after "Tribunal" Here section 73 refers to the new Clause inserted in the Bill by the Committee.
60.	55	At Page No.: 27, Line No.:15,22,24,26 Add "," after "documents"; Omit "and" before "records" Add "or data" after "records" At Page No.: 27, Line No.:17 Add "or State Government" after "Central Government" For "both" substitute "all" For “specified” substitute “provided” At Page No.: 27, Line No.:26 For "its" substitute "his”

		At Page No.: 27, Line No.:28 For "it" substitute "he"
61.	56	At Page No. 27, Line No. 38 Add the words 'including economic activities' after the word 'actions'
62.	57 Marginal Heading	Omit "the" before "Act"
63.	59	At page No. 29, Line No. 3 Add "a" after the word "penalty"
64.	62	At Page No. 29, Line No. 18 For " section 64" substitute "section 65"; For "Officer" substitute "Officers" At Page No. 29, Line No. 19 For "prescribed" substitute "required" At Page No. 29, Line No. 22,23,25 Add "the" at the beginning At Page No. 29, Line No. 25 Add "and" at the end At Page No. 29, Line No. 26 Omit "Central Government" after "as" At Page No. 29, Line No. 26 For "deem fit" substitute "be prescribed" At Page No. 29, Line No. 28 For "must have" Substitute "shall possess such qualifications" For "of and not less than seven years" Substitute "and adequate" At Page No. 29, Line No. 30 Add the words ",as may be prescribed" after" subjects"
65.	63	At Page No.: 29, Line No.:33 For "a" substitute "an"; "Omit "reasonable" before "opportunity" At Page No.: 29, Line No.43 Add "as" after "penalty" At Page No.: 30, Line No.:09 Omit "and" after "data principals;" At Page No.: 30, Line No.:13 Add "made" after "order" At Page No.: 30, Line No.:14 Add the words "under section73" after "Tribunal Here section 73 refers to the new Clause inserted in the Bill by the Committee.
66.	64	At Page No.30, Line No.23

		Omit words "expressly applicable to it" At Page No.30, Line No.34 Omit words "prescribed" and "specified" Add word "made" before there under At Page No.30, Line No.:46 Add "or" after "data fiduciary;" At Page No. 31, Line No. 9 For “sub-section (5)” substitute “sub-section (4)” At Page No. 31, Line No. 15 Add 'under Section 73' after the word 'Tribunal' At Page No. 31, Line No. 16 Omit “The Central Government may prescribe the” For “a complaint” substitute “an application” At Page No. 31, Line No. 17 Add “shall be such as may be prescribed” after “Section” Here section 73 refers to the new Clause inserted in the Bill by the Committee.
67.	67	At Page No. 31, Line No.:34 For “section 63” substitute “section 64” At Page No. 31, Line No.:36 For “(7)" substitute “(6)” At Page No. 31, Line No.:36 For “section 64” substitute “section 65” At Page No. 31, Line No.:43,44 For 'body" substitute "Tribunal"
68.	68 Marginal Heading	Add “Chairperson and” after “service of”
69.	68	At Page No. 32, Line No.:10 Omit words " Central Government may prescribed the"; At Page No. 32, Line No.:12 For "member" substitute "Member" Add words "shall be such as may be prescribed " after "Tribunal,"
70.	69	At Page No. 32, Line No.:15 For the word “prescribed” substitute “made thereunder”
71.	70	At Page No. 32, Line No.:22 Add words "payable to" after "allowances" Add words "terms and" before "conditions"
72.	72	At Page No.: 32, Line No.:34 After the word “decision” add “or order”

		Add “or an Adjudicating Officer” after “Authority” At Page No.: 32, Line No.:45 Add “or the Adjudicating Officer” after “Authority” At Page No.:33, Line No.:04 Omit "or application" after "such appeal"
73.	73	At Page No.: 33, Line No.:12 For “his” substitute “him” At Page No. 33, Line No.:16 For “section” substitute “sections” after “provisions of” At Page No. 33, Line No. 16 Omit the word "section" before “124”. At Page No. 33, Line No.:21 Omit "," after "it" At Page No. 33, Line No.:21 Omit "," after "it"
74.	74	Page No.:33, Line No.:29 Substitute “an” for “every” and “passed” for “made”
75.	75	At Page No. 33, Line No. 35 Omit “in” after “or” At Page No. 33, Line No. 36 Add "for the time being in force" after "other law" At Page No. 33, Line No. 36 Omit words", not being an interlocutory order," At Page No. 33, Line No. 40 Add the word "made" after "appeal" For word "ninety" substitute"sixty" At Page No. 33, Line No. 43 For word "ninety" substitute"sixty"
76.	76	At Page No. :34, Line No.:2 Add words “or experts” after “its officials”. At Page No. :34, Line No.:4 Add words “the expression” before “legal practitioner”; Add word "shall" before include, For word "includes" substitute "include" At Page No. 34, Line No.:5 Omit “and includes a pleader in practice”
77.	79 Marginal heading	Omit words" of India" For "Funds" substitute "Fund"
78.	80	At Page No. 34, Line No. 40 For "Comptroller and Auditor General of India" substitute "him" At Page No. 34, Line No. 42

		Add the words "by the Authority" after "Government";
79.	82	At Page No.; 35, Line No.:11 Add “the” before “personal data” At Page No.:35, line No.:16 Add "with" before "both"
80.	83	At Page No.; 35, Line No.:25 Add the word "punishable" after "offence" Add the words "in writing" after complaint At Page No.; 35, Line No.:26 Add the words "or by any officer duly authorized by it for this purpose" after Authority
81.	84	At Page No. 35, Line No. 30 Omit "shall be deemed to be guilty of the offence and" At Page No. 35, Line No. 3o Omit "deemed to be guilty of the offence and shall" At Page No. 35, Line No. 42 For “purpose” substitute “purposes” After "this section" add "the expressions"
82.	85 Marginal Heading	For "State" substitute "Government data fiduciaries"
83.	85	At Page No.:36, Line No.:11 Add “or officer” after “such person” At Page No.:36, Line No.:21 Add the word 'contained' after 'anything'
84.	86	At Page No.:36, Line No.:30 Omit "on questions of policy"
85.	88	At Page 36, Line No.:41 For “member” substitute “Member” At Page No.:36, Line No.:41 Omit "done" before "in good faith" Add "done" after "good faith" At Page No.: 36, Line No.:42 For the words “ prescribed, or the regulations specified” substitute “or regulations made”
86.	90	At page 37, Line No.:1 For “member” substitute “Member” At Page No. 37, Line No.:3 Add the words "to make regulations" after" powers" For “section 94” substitute “section 95”
87.	91	At Page No.:37, Line No.:05

		Omit "of" after "framing" At Page No.:37, Line No.:07 Omit "insofar" before "as such"
88.	92	At page 37, Line No.:16 For the word "no" substitute "any"; Add 'not' after shall For "notified by the Central Government Substitute "prescribed"
89.	93	At Page No. 37, Line No. 19 For "provisions" Substitute "purposes" At Page No.:37, Line No.:23 Add "the " before "other" At Page No. 37, Line No.:28 For “methods” substitute “manner” At Page No. 37, Line No.:28 For “identification to identify” substitute “verification of the accounts of the” At Page No. 37, Line No.:28 Add “platform” after “media” At Page No. 37, Line No.:33 For "class of entity" substitute "class of entities" At Page No. 37, Line No.:36 Add 'the " before "procedure" At Page No. 37, Line No. 42 Add "(including quorum)" after "meetings" At Page No.: 37, Line No.: 43 For “(o)” substitute “(p)” At Page No. 38, Line No.:7 For “section 62” substitute “section 63” At Page No. 38, Line No.:9 For “section 63” substitute “section 64” At Page No. 38, Line No.:10 For "a complaint" substitute "an application"; Omit " under sub section 2," At Page No. 38, Line No.:11 For "a complaint" substitute "an application"; For “sub-section (8)” substitute “sub-section (7)” At Page No. 38, Line No.:11 For “section 64” substitute “section 65” At Page No. 38, Line No.:14 For “section 68” substitute “section 69” At Page No. 38, Line No.:15 For “section 69” substitute “section 70” At Page No. 38, Line No.:17 For “section 70” substitute “section 71” At Page No. 38, Line No.:18

		Omit 'or applications, as the case may be" At Page No. 38, Line No.:19 For “section 72” substitute “section 73” At Page No. 38, Line No.:20 For “section 73” substitute “section 74” At Page No. 38, Line No.:24 For “section 80” substitute “section 81” At Page No. 38, Line No.:25 Omit words "in which" At Page No. 38, Line No.:27 For “section 81” substitute “section 82” At Page No. 38, Line No.:30 For “section 91” substitute “section 92” At Page No. 38, Line No.:30 Omit “or” after “section 91;”
90.	94	At Page No. 38, Line No. 34 For "provisions" Substitute "purposes" At Page No. 38, Line No. 37 Add the words 'any other' before the word 'information'. At Page No. 38, Line No. 39 Add “the” at the beginning At Page No. 38, Line No. 41 Add “the reasonable purpose under sub-section (1)” at the beginning At Page No. 38, Line No. 44 For “under sub-section (2)” substitute “and” At Page No. 38, Line No. 45 For “sub section 3”substitute “section 2” At Page No.: 39, Line No. :2 For “ (6)” substitute "(5)” At Page No. 39, Line No.10 For 'operation' substitute "operational" At Page No. 39, Line No. 11 For "consent manager" Substitute "Consent Manager" At Page No. 39, Line No. 11 Omit 'and its compliance” At Page No. 39, Line No. 15 Substitute 'class' for 'classes' At Page No. 39, Line No. 17 Substitute 'appointed' for 'engaged'. At Page No. 39, Line No. 17 Omit "and" before "the manner" At Page No. 39, Line No. 24 Omit "the manner of registration of auditors under sub-section(4);" At Page No. 39, Line No. 31

		For “archival” substitute “archiving” At Page No.:39, , Line No. 38 Add 'or data processor' after 'fiduciary'.
91.	95 Marginal Heading	Omit “and” after “rules” Add 'and notification' after 'regulations'
92.	95	At Page No. 39, Line No.:42 For “section 67” substitute “section 68”
93.	96	At Page No. 40, Line No. 2 Add "contained in" after "therewith" At Page No.:40, Line No.:3 For “law other than this Act” substitute “such law”
94.	97	At Page No.40, Line No.:6 Add "to it" before "to be" At Page No.40, Line No.:9 Add words "date of" before "commencement"

(Recommendation No. 92)

2.282 The Joint Committee, therefore, recommend that the Bill as amended after inclusion of suggestions/recommendations made by the Committee be passed and the General Recommendations made in the Part-I may be implemented in due course.

(Recommendation No. 93)

THE PERSONAL DATA PROTECTION BILL, 2019

AS REPORTED BY THE JOINT COMMITTEE

[WORDS AND FIGURES IN BOLD AND UNDERLINED INDICATE THE AMENDMENTS AND (***) MARK INDICATES THE OMISSION SUGGESTED BY THE JOINT COMMITTEE]

	THE **(***)** DATA PROTECTION BILL, 20**21**	
	A **BILL**	
	to provide for protection of the ***digital****privacy of individuals relating to their personal data,* ***to****specify the flow and usage of* ***(***)*** *data,* ***to*** *create a relationship of trust between persons and entities processing the* ***(***)*** *data,* ***to****protect the rights of individuals whose* ***(***)*** *data are processed,* to *create a framework for organisational and technical measures in processing of data,* ***to****lay****(***)*** *down norms for social media* ***(***)platforms****, cross-border transfer, accountability of entities processing* ***(***)*** *data, remedies for unauthorised and harmful processing,* ***to ensure the interest and security of the State*** *and to establish a Data Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto.*	
	WHEREAS the right to privacy is a fundamental right and it is necessary to protect personal data **of an individual**as an essential facet of informational privacy;	
	AND WHEREAS the growth of the digital economy has expanded the use of data as a critical means of communication between persons;	
	AND WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals **that fosters sustainable growth of digital products and services** and ensuring empowerment, progress and innovation through digital governance and inclusion and for matters connected therewith or incidental thereto.	

	BE it enacted by Parliament in the **Seventy-second** Year of the Republic of India as follows:—	
	CHAPTER I **PRELIMINARY**	
	1. (*1*) This Act may be called the **(***)** Data Protection Act, 20**21**.	Short title and commence ment.
	(*2*) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.	
	2. The provisions of this Act **shall apply to**,– **(A) (***)**	Application of Act to processing of personal data**and non-personal data**
	(*a*) the processing of personal data where such data has been collected, **stored,** disclosed, shared or otherwise processed within the territory of India;	
	(*b*) the processing of personal data by **(***)** any person **(***)** under Indian law;	
	(*c*) the processing of personal data by data fiduciaries or data processors not present within the territory of India, if such processing is—	
	(*i*) 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	
	(*ii*) in connection with any activity which involves profiling of data principals within the territory of India**; and**	
	(d) the processing of non-personal data including anonymised personal data.	
	(B) (***)	

	3. In this Act, unless the context otherwise requires,—	Definitions.
	(*1*) "Adjudicating Officer" means the Adjudicating Officer appointed as such under sub-section (*1*) of section 6**3**;	
	(*2*) "anonymisation" in relation to personal data, means such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority;	
	(*3*) "anonymised data" means data which has undergone the process of anonymisation;	
	(*4*) "Appellate Tribunal" means the Tribunal established under sub-section (*1*) or notified under sub-section (*4*) of section 6**8**;	
	(*5*) "Authority" means the Data Protection Authority of India established under sub-section (*1*) of section 41;	
	(*6*) "automated means" means any equipment capable of operating automatically in response to instructions given **or otherwise** for the purpose of processing data;	
	(*7*) "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 behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person;	
	(*8*) "child" means a person who has not completed eighteen years of age;	
	(*9*) "code of practice" means a code of practice issued by the Authority under section 50;	
	(*10*) "consent" means the consent referred to in section 11;	
	(11) "Consent Manager" means a data fiduciary which enables a data principal to give, withdraw, review and manage his consent through an accessible, transparent and interoperable platform;	

	(***12***) "data" 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 auditor" means a **(***)** data auditor referred to in section 29;	
	(14)**"data breach" includes personal data breach and non-personal data breach;**	
	(***15***) "data fiduciary" means any person, including **a** State, a company, **a non-government organisation**, **(***)** juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data;	
	(***16***) "data principal" means the natural person to whom the personal data relates;	
	(***17***) "data processor" means any person, including **a** State, a company, **a non-government organisation,(***)** juristic entity or any individual, who processes personal data on behalf of a data fiduciary;	
	(18) "data protection officer" means an officer who shall be appointed by the significant data fiduciary under section 30;	
	(19) "de-identification" means the 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;	
53 of 2005.	***(20)*** "disaster" shall have the same meaning as assigned to it in clause (*d*) of section 2 of the Disaster Management Act, 2005;	
	(21)"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;	
	(22) "genetic data" means personal data relating to the inherited or acquired genetic characteristics of a natural person which give**s** unique information about the behavioral characteristics, physiology or the health of that natural	

	person and which result**s**, in particular, from an analysis of a biological sample from the natural person in question;	
	(*23*) "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**s** 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; **(***)**	
	(*x*) any observation or surveillance that is not reasonably expected by the data principal;	
	(xi) psychological manipulation which impairs the autonomy of the individual; or	
	(xii) such other harm as may be prescribed;	
	(*24*) "health data" means the 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 **associated with** the data principal to the provision of specific health services;	
	(*25*) "intra-group schemes" means the schemes approved by the Authority under clause (*a*) of sub-section (*1*) of section 34;	
	(*26*) "in writing" includes any communication **or information** in electronic form **(***) generated, sent, received or stored in media, magnetic, optical,**	(***)

	computer memory, micro film, computer generated micro fiche or similar device (***);	
	(27) "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;	
	(28) "non-personal data" means the data other than personal data;	
	(29) "non-personal data breach" means any unauthorized including accidental disclosure, acquisition, sharing, use, alteration, destruction or loss of access to non-personal data that compromises the confidentiality, integrity or availability of such data;	
	(30)"notification" means a notification published in the Official Gazette and the expression**s** "notify" **and "notified"** shall be construed accordingly;	
	(31) "official identifier" means any number, code, or other identifier, 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;	
	(32)"person" includes—	
	(*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;	
	(*33*) "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, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;	
	(*34*) "personal data breach" means any unauthorised **(***) including** accidental disclosure, acquisition, sharing, use, alteration, destruction (***) or loss of access to personal data that compromises the confidentiality, integrity or availability of personal data to a data principal;	
	(*35*) "prescribed" means prescribed by rules made under this Act;	
	(*36*) "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;	
	(*37*) "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behavio**u**r, attributes or interests of a data principal;	
	(*38*) "regulations" means the regulations made by the Authority under this Act;	
	(*39*) "re-identification" means the process by which a data fiduciary or data processor may reverse a process of de-identification;	
	(40) "Schedule" means the Schedule appended to this Act;	
	(*41*) "sensitive personal data" means such personal data, which may reveal, be related to, or constitute—	
	(*i*) financial data;	
	(*ii*) health data;	

	(*iii*) official identifier;	
	(*iv*) sex life;	
	(*v*) sexual orientation;	
	(*vi*) biometric data;	
	(*vii*) genetic data;	
	(*viii*) transgender status;	
	(*ix*) intersex status;	
	(*x*) caste or tribe;	
	(*xi*) religious or political belief or affiliation; or	
	(*xii*) any other data categorised as sensitive personal data under section 15;	
	Explanation.— For the purposes of this clause, the expressions,—	
	(*a*) "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;	
	(*b*) "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;	
	(*42*) "significant data fiduciary" means a data fiduciary classified as such under sub-section (*1*) of section 26;	
	(*43*) "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;	

	(44)**"social media platform" means a platform which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services;**	
	(45) "State" means the State as defined under article 12 of the Constitution;	
	(46) "systematic activity" means any structured or organised activity that involves an element of planning, method, continuity or persistence.	
	CHAPTER II **OBLIGATIONS OF DATA FIDUCIARY**	
	4. (***) The processing of personal data (***) by any person **(***) shall be subject to the provisions of this Act and the rules and regulations made thereunder.**	**(***)** Processing of personal data.
	5. Every person processing personal data of a data principal shall process such personal data—	Limitation on purpose of processing of personal data.
	(a) in a fair and reasonable manner and ensure the privacy of the data principal; and	
	(b) for the purpose consented to by the data principal or which is incidental **there**to or connected with such purpose **or which is for the purpose of processing of personal data under section 12**, and which the data principal would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected.	
	6. The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.	Limitation on collection of personal data.

	7.(1) Every data fiduciary shall give to the data principal **(***)**, 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 notice** containing the following information, namely:—	Requirement of notice for collection or processing of personal data.
	(a) the purposes for which the personal data is to be processed;	
	(b) the nature and 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 his 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 **(***)provided** in sections 12 to 14;	
	(f) the source of such collection, if the personal data is not collected from the data principal;	
	(g) the individuals or entities including other data fiduciaries or data processors, with whom such personal data may be shared, if applicable;	
	(h) **the**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 shall be retained in terms of section 9 or where such period is not known, the criteria for determining such period;	

	(j) the existence of and procedure for the exercise of rights mentioned in Chapter V and any related contact details for the same;	
	(k) the procedure for grievance redressal under section 32;	
	(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 assigned to the data fiduciary under sub-section (5) of section 29; and	
	(n) any other information as may be specified by regulations.	
	(2) The notice referred to in sub-section (1) shall be clear, concise and easily comprehensible to a**n(***)individual** and in multiple languages **(***) to the extent** necessary and practicable.	
	(3) The provisions of sub-section (1) shall not apply where such notice **(***)** prejudices the purpose of processing of personal data under section12.	
	8.(1) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.	Quality of personal data processed.
	(2) While taking any steps under 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 any other individual or entity, including other data fiduciary or processor, and the data fiduciary finds that such data does not comply with the	

	requirement**s** of sub-section (1), the data fiduciary shall **(***)** notify such individual or entity of this fact: **Provided that the provisions of this sub-section shall not apply where such notice prejudices the purpose of processing of personal data under section 12.**	
	(4) A data fiduciary may share, transfer or transmit the personal data to any person as part of any business transaction in such manner as may be prescribed: **Provided that the provisions of this sub-section shall not apply where such sharing, transfer or transmission of personal data prejudices the purpose of processing of personal data under Section 12.**	
	9.(1) The data fiduciary shall not retain any personal data beyond the period necessary to satisfy the purpose for which it is processed and shall delete the personal data at the end of (***)**such period.**	Restriction on retention of personal data.
	(2) Notwithstanding anything contained in sub-section (1), the personal data may be retained for a longer period if explicitly consented to by the data principal, or necessary to comply with any obligation under any law for the time being in force.	
	(3) The data fiduciary shall undertake periodic review 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-section (1) or sub-section (2), then, such personal data shall be deleted in such manner as may be specified by regulations.	
	10. The data fiduciary shall be responsible for complying with the provisions of this Act **and the rules and regulations made thereunder** in respect of any processing undertaken by it or on its behalf.	Accountability of data fiduciary.
	11.(1) The personal data shall not be processed, except on the consent given by the data principal at the commencement of its processing.	Consent necessary for processing of personal data.

	(2) The consent of the data principal shall not be valid, unless such consent is—	
9 of 1872.	(a) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872;	
	(b) informed, having regard to whether the data principal has been provided with the information required under section 7;	
	(c)specific, having regard to whether the data principal can determine the scope of consent in respect of the purpose 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) In addition to the provisions contained in sub-section (2), the consent of the data principal in respect of processing of any sensitive personal data shall be explicitly obtained—	
	(a) after informing him the purpose of, or operation in, processing which is likely to cause significant harm to the data principal;	
	(b) in clear terms without recourse to inference **to be drawn either** from conduct (***) **or** context; and	
	(c) after giving him the choice of separately consenting to the purposes of operations in the use of different categories of sensitive personal data relevant to processing.	
	(4) The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be,-	
	(i) made conditional on the consent to the processing of any personal data not necessary for that purpose; **and**	

	(ii) <u>denied based on exercise of choice.</u>	
	(5) The burden of proof that the consent has been given by the data principal for processing of the personal data under this section shall be on the data fiduciary.	
	(6) Where the data principal withdraws his consent from the processing of any personal data without any valid reason, **(***) <u>the</u>** consequences for the **(***) <u>same</u>** shall be borne by such data principal.	
	CHAPTER III **GROUNDS FOR PROCESSING OF PERSONAL DATA** **WITHOUT CONSENT**	
	12. Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,—	Grounds for processing of personal data without consent in certain cases.
	(a) for the performance of any function of the State authorised by law, **<u>including</u>** for—	
	(*i*) the provision of any service or benefit to the data principal from the State; or	
	(*ii*) the issuance of any certification, licence or permit for any action or activity of the data principal by the State;	
	(b) under any law for the time being in force made by Parliament or any State Legislature; **(***)**	
	(c) for compliance with any (***) judg**<u>e</u>**ment **<u>or order</u>** of any court**<u>, quasi-judicial authority</u>** or Tribunal in India;	
	(d) 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;	
	(e) 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	
	(f) 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.	
	13.(1)Notwithstanding anything contained in section 11 and subject to **the provisions contained in** sub-section (2), any personal data, not being any sensitive personal data, may be processed, if such processing is necessary **or can reasonably be expected by the data principal** for—	Processing of personal data necessary for purposes related to employment, etc.
	(a) recruitment or 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) Any personal data, not being sensitive personal data, may be processed under sub-section (1), where the 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 under the said sub-section.	
	14.(1) (***) **Notwithstanding anything contained in section 11,** the personal data may be processed (***), if such processing is necessary for **(***)** reasonable purposes as may be specified by regulations, after taking into consideration—	Processing of personal data for other reasonable purposes.
	(a) the **legitimate** interest of the data fiduciary in processing for that purpose;	

	(b)whether the data fiduciary can reasonably be expected, **and it is practicable** to obtain the consent of the data principal;	
	(c) any public interest in processing for that purpose;	
	(d) the **degree of any adverse** 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 expression "reasonable purposes" may include—	
	(a) prevention and detection of any unlawful activity including fraud;	
	(b) whistle blowing;	
	(c) mergers **(***),** acquisitions, **any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws**;	
	(d) network and information security;	
	(e) credit scoring;	
	(f) recovery of debt;	
	(g) processing of publicly available personal data; and	
	(h) the operation of search engines.	
	(3) Where the Authority specifies a reasonable purpose under sub-section (1), it shall—	
	(a) lay down, by regulations, 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 7shallapply or not apply having regard to the fact whether such provision shall **(***)** prejudice the relevant reasonable purpose.	
Categorisation of personal	**15.**(1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such	

data as sensitive personal data.	categories of personal data as "sensitive personal data", having regard to—	
	(a) the risk of significant harm that may be caused to the data principal by **(***)** 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 **the** personal data.	
	(2) The Authority may specify, by regulations, the additional safeguards or restrictions for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.	
	CHAPTER IV **PERSONAL DATA (***) OF CHILDREN**	
	16.(1)Every data fiduciary shall process **the** personal data of a child in such manner that protects the rights of **(***)** the child.	Processing of personal data **(***)** of children.
	(2)The data fiduciary shall, before processing of any personal data of a child, verify his age and obtain the consent of his parent or guardian, in such manner as may be specified by regulations;	
	(3) The manner for verification of the age of child under sub-section (2) shall (***) **take** into consideration—	
	(a) the volume of personal data processed;	
	(b) the proportion of such personal data likely to be that of child;	
	(c) **the** possibility of harm to child arising out of processing of personal data; and	

	(d) such other factors as may be prescribed.	
	(4) (***)	
	(4) The **(***)** data fiduciary shall be barred from profiling, tracking, or behavio**u**ral monitoring of, or targeted advertising directed at children and undertaking any other processing of personal data that can cause significant harm to the child.	
	(5) The provisions of sub-section (4) shall apply in such modified form to the data fiduciary offering counselling or child protection services to a child, as the Authority may by regulations specify.	
	(7) (***)	
	***Explanation.*-(***)**	
	CHAPTER V **RIGHTS OF DATA PRINCIPAL**	
	17.(1) The data principal shall have the right to obtain from the data fiduciary—	Right to confirmation and access.
	(a) **the** confirmation whether the data fiduciary is processing or has processed personal data of the data principal;	
	(b) the personal data of the data principal being processed or that has been processed by the data fiduciary, or any summary thereof; **and**	
	(c) a brief 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 7 in relation to such processing.	
	(2) The data fiduciary shall provide the information under sub-section (1) to the data principal in a clear and concise manner that is easily comprehensible to (***) **a reasonable individual in a similar context**.	

	(3) The data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of personal data shared with them, in such manner as may be specified by regulations.	
	(4) The data principal shall have the following options, namely:-	
	(a) to nominate a legal heir or a legal representative as his nominee;	
	(b) to exercise the right to be forgotten; and	
	(c) to append the terms of agreement,	
	with regard to processing of personal data in the event of the death of such data principal.	
Right to correction and erasure.	**18.**(1) The data principal shall, where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to—	
	(a) the correction of inaccurate or misleading personal data;	
	(b) the completion of incomplete personal data;	
	(c) the**(***)updation**of personal data that is out-of-date; and	
	(d) the erasure of personal data which is no longer necessary for the purpose for which it was processed.	
	(2) Where the data fiduciary receives a request under sub-section (1), and the data fiduciary does not agree with such correction, completion, updation or erasure having regard to the purposes of processing, such data fiduciary shall provide the data principal with adequate justification in writing for rejecting the application.	
	(3) Where the data principal is not satisfied with the justification provided by the data fiduciary under sub-section (2), the data principal may 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, updates or erases any personal data in accordance with **the provisions contained in** sub-section (1), such data fiduciary shall also take, necessary **and practicable,** steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updation or erasure, **(***)having regard to the impact(***)**such action may have (***) on the rights and interests of the data principal or on decisions made regarding them.	
	19.(1) Where the processing has been carried out through automated means, the data principal shall have the right to—	Right to data portability.
	(a) receive the following personal data in a structured, commonly used and machine-readable format—	
	(i) the personal data provided to the data fiduciary;	
	(ii) the data which has been generated in the course of provision of services or use of goods by the data fiduciary; or	
	(iii) the data which forms part of any profile on the data principal, or which the data fiduciary has otherwise obtained; and	
	(b) (***) **transfer** the personal data referred to in clause (a) (***) to any other data fiduciary in the format referred to in that clause.	
	(2) The provisions of sub-section (1) shall not apply where—	
	(a) processing is necessary for functions of the State or in compliance of law or **any judgement or** order of a court**, tribunal or quasi-judicial authority** under section 12;	
	(b) compliance with the request in sub-section (1) would **(***)** not be technically feasible**,as determined by the data fiduciary in such manner as may be specified by regulations.**	
	20.(1) The data principal shall have the right to restrict or prevent the continuing disclosure **or processing** of his personal data by a data fiduciary where such disclosure **or processing**—	Right to be forgotten.

	(a) has served the purpose for which it was collected or is no longer necessary for the purpose;	
	(b) was made with the consent of the data principal under section 11 and such consent has since been withdrawn; or	
	(c) was made contrary to the provisions of this Act or any other law for the time being in force.	
	(2) The rights under sub-section (1) may be enforced only on an order of the Adjudicating Officer made on an application filed by the data principal, in such form and manner as may be prescribed, on any of the grounds specified under clauses (a), (b) or **(***)**(c) of that sub-section:	
	Provided that no order shall be made under this sub-section unless it is shown by the data principal that his right or interest in preventing or restricting the continued disclosure **or processing** of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen **or the right of the data fiduciary to retain, use and process such data in accordance with the provisions of this Act and the rules and regulations made thereunder.**	
	(3) The Adjudicating Officer shall, while making an order under sub-section (2), have regard to—	
	(a) the sensitivity of the personal data;	
	(b) the scale of disclosure **or processing** 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 disclosure **or processing** and of the activities of the data fiduciary, particularly whether the data fiduciary systematically facilitates access to personal data and whether the activities shall be significantly impeded if disclosures **or processing** of the relevant nature were to be restricted or prevented.	
	(4) Where any person finds that personal data, the disclosure **or processing** of which has been restricted or prevented by an order of the Adjudicating Officer under sub-section (2), does not	

	satisfy the conditions referred to in that sub-section **any longer**, he may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and the Adjudicating Officer shall review his order.	
	(5) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal **under section 73.**	
General conditions for **(***)** exercise of rights in this Chapter.	**21.**(1) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a **C**onsent **M**anager with the necessary information as regard to his identity, and the data fiduciary shall acknowledge the receipt of such request within such period as may be specified by regulations.	
	(2) For complying with the request made under sub-section (1), the data fiduciary may charge such fee as may be specified by regulations:	
	Provided that no fee shall be required for any request in respect of rights **(***) under** clause (a) or **clause** (b) of sub-section (1) of section 17 or section 18.	
	(3) The data fiduciary shall comply with the request under this Chapter and communicate the same to the data principal, within such period as may be specified by regulations.	
	(4) Where any request made under this Chapter is refused by the data fiduciary, it shall provide the data principal the reasons in writing for such refusal 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 by regulations.	
	(5) The data fiduciary is not obliged to comply with any request under this Chapter where such compliance shall harm the rights of any other data principal under this Act:	
	Provided that the data fiduciary shall, subject to such conditions as may be specified by regulations, be obliged to comply with such request made by the data principal.	
	CHAPTER VI **TRANSPARENCY AND ACCOUNTABILITY MEASURES**	

Privacy by design policy.	**22.**(1)Every data fiduciary shall prepare a privacy by design policy, containing—	
	(a) the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to the data principal;	
	(b) the obligations of data fiduciaries;	
	(c) the technology used in the processing of personal data is in accordance with commercially accepted or certified standards;	
	(d) the legitimate interests of businesses including any innovation is achieved without compromising privacy interests;	
	(e) the protection of privacy throughout processing from the point of collection to deletion of personal data;	
	(f) the processing of personal data in a transparent manner; and	
	(g) the interest of the data principal is accounted for at every stage of processing of personal data.	
	(2) **(***)**<u>**T**</u>he data fiduciary may submit its privacy by design policy prepared under sub-section (1) to the Authority for certification within such period and in such manner as may be specified by regulations.	
	(3) <u>**Subject to the provisions contained in sub-section (2),**</u> the Authority, or an officer authorised by it, shall certify the privacy by design policy on being satisfied that it complies with the requirements of sub-section (1).	
	(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.	
	23.(1) Every data fiduciary shall take necessary steps to maintain transparency in processing personal data and shall make the following information available in such form and manner as may be specified by regulations—	Transparency in processing of personal data.
	(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 the procedure for exercise of rights of data principal under Chapter V and any related contact details for the same;	
	(e)the right of data principal to file complaint against the data fiduciary 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 sub-section (5) of section 29;	
	(g) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; **(***)**	
	(h) where applicable, fairness of algorithm or method used for processing of personal data; and	
	(**i**) any other information as may be specified by regulations**.**	
	(2) The data fiduciary shall notify, from time to time, the important operations in the processing of personal data related to the data principal in such manner as may be specified by regulations.	
	(3) The data principal may give or withdraw his consent to the data fiduciary through a **C**onsent **M**anager.	
	(4) Where the data principal gives or withdraws consent to the data fiduciary through a **C**onsent **M**anager, such consent or its withdrawal shall be deemed to have been communicated directly by the data principal.	
	(5) The **C**onsent **M**anager under sub-section (3), shall be registered with the Authority in such manner and subject to such technical, operational, financial and other conditions as may be specified by regulations.	
	Explanation.-**(***)**	

Security safeguards.	**24.**(1) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary 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 periodically in such manner as may be specified by regulations and take appropriate measures accordingly.	
Reporting of **(***)** data breach.	**25.**(1) Every data fiduciary shall by notice,**(***)** **report to** the Authority about the breach of any personal data processed by (***) **such** data fiduciary.**(***)**	
	(2) The notice referred to in sub-section (1) shall **be in such form as may be specified by regulations and** include the following particulars, namely:—	
	(a) nature of personal data which is the subject matter of the breach;	
	(b) number of data principals affected by **(***)** **such** breach;	
	(c) possible consequences of **(***)** **such** breach; and	
	(d) **the remedial actions** being taken by the data fiduciary **(***)** **for such** breach.	
	(3) The notice referred to in sub-section (1) shall be **(***)** **issued** by the data fiduciary **within seventy-two hours of becoming aware of such breach.(***)**	
	(4) Where it is not possible to provide all the information **(***)** **provided** in sub-section (2) at the same time, the data	

	fiduciary shall provide such information to the Authority in phases without **any** undue delay.	
	(5) (***)	
	(5) The Authority **(***)shall, after taking into account the personal data breach and the severity of harm that may be caused to the data principal,** direct the data fiduciary to **report such breach to the data principal and** take appropriate remedial actions**(***) to mitigate such harm** and to conspicuously post the details of the personal data breach on its website.	
	Provided that the Authority may direct the data fiduciary to adopt any urgent measures to remedy such breach or mitigate any harm caused to the data principal.	
	(7) (***)	
	(6) The Authority shall, in case of breach of non-personal data, take such necessary steps as may be prescribed.	
	26.(1) The Authority shall, having regard to the **any of the** following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—	Classification 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 by processing by the data fiduciary;	
	(e) use of new technologies for processing; **(***)**	
	(f) any social media platform-	
	(i) with users above such threshold as may be prescribed, in consultation with the Authority; and	
	(ii) whose actions have or are likely to have a significant impact on the sovereignty and integrity of India, electoral democracy, security of the State or public order:	

	Provided that different thresholds may be prescribed for different classes of social media platforms;	
	(g) the processing of data relating to children or provision of services to them; or	
	(h)any other factor causing harm from such processing.	
	(2) The data fiduciary or class of data fiduciary referred to in sub-section (1) shall register itself with the Authority in such manner as may be specified by regulations.	
	(3) Notwithstanding anything **contained** in this Act, if the Authority is **(***) satisfied** that any processing by any data fiduciary or class of data fiduciar**ies** carries a risk of significant harm to any data principal, it may, by notification, apply all or any of the obligations **(***)provided** in sections 27 to 30 to such data fiduciary or class of data fiduciar**ies,** as if it is a significant data fiduciary.	
	(4) (***)	
	(4) Subject to the provisions contained in section 56, the significant data fiduciary shall be regulated by such regulations as may be made by the respective sectoral regulators.	
Data protection impact assessment.	**27.**(1) Where **(***) a** significant 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 by regulations specify, such circumstances or class of data fiduciar**ies** or processing operation where such data protection impact assessment shall be mandatory, and also specify the 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, *inter alia*, contain—	
	(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 appointed under sub-section (1) of section 30, shall review the assessment and submit the assessment with his finding to the Authority in such manner as may be specified by regulations.	
	(5) On receipt of the assessment and its review, if the Authority has (***) **satisfied itself** that the processing is likely to cause harm to the data principals, (***) **it** may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as (***) **may be specified by regulations**.	
	28.(1) The significant data fiduciary shall maintain accurate and up-to-date records of the following, in such form and manner as may be specified by regulations, namely:—	Maintenance of records.
	(a) important operations in the data life-cycle including collection, transfers, and erasure of personal data to demonstrate compliance as required under section 10;	
	(b) periodic review of security safeguards under section 24;	
	(c) data protection impact assessments under section 27; and	
	(d) any other aspect of processing as may be specified by regulations.	

	(2) Notwithstanding anything contained in this Act, this section shall also apply to the State.	
	(3) Every social media **(***) platform** which is notified as a significant data fiduciary under sub-section (***) (**1**) of section 26 shall enable the **(***) persons** who register their service from India, or use their services in India, to voluntarily verify their accounts in such manner as may be prescribed.	
	(4) Any **(***) person** who voluntarily verifies his account**on a social media platform referred to in sub-section (3)** shall be provided with such demonstrable and visible mark of verification, which shall be visible to all users of the service, in such manner as may be prescribed.	
	29.(1) The significant 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.	Audit of policies and conduct of processing, etc.
	(2) The data auditor shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—	
	(a) clarity and effectiveness of notices under section 7;	
	(b) effectiveness of measures adopted under section 22;	
	(c) transparency in relation to processing activities under section 23;	
	(d) security safeguards adopted pursuant to section 24;	
	(e) instances of personal data breach and response of the data fiduciary, including the promptness of notice to the Authority under section 25;	
	(f) timely implementation of processes and effective adherence to obligations under sub-section (3) of section 28; and	
	(g) any other matter as may be specified by regulations.	
	(3) The Authority shall specify, by regulations, the form and procedure for conducting audits under this section **and shall encourage the practice of appropriate concurrent audits.**	

	(4) The Authority shall register in such manner the persons, with expertise in the area of information technology, computer systems, data science, data protection or privacy, possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as (***) may be (***) **prescribed**, as data auditors (***).	
	(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, by regulations, 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 anything contained in sub-section (1), where the Authority is (***) **satisfied** that the data fiduciary is processing personal data in such manner that is likely to cause harm to a data principal, the Authority may direct (***) **such** data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.	
Data protection officer.	**30.**(1) Every significant data fiduciary shall appoint a data protection officer **who shall be a senior level officer in the State or a key managerial personnel in relation to a company or such other employee of equivalent capacity in case of other entities, as the case may be,**possessing such qualification**s** and experience as may be (***) **prescribed** (***) for carrying out the following functions, **namely**:—	
	(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 assistance to and co-operating with the Authority on matters of compliance of the data fiduciary with the provisions under this Act;**	
	(d) providing advice to the data fiduciary on the development of internal mechanisms to satisfy the principles specified under section 22;	

	(e) (***)**providing advice to the data fiduciary on carrying out the data protection impact assessments, and carry out its review under sub-section (4) of section 27;**	
	(f) (***) **maintaining an inventory of records to be maintained by the data fiduciary under section 28;**and	
	(g) (***) **act as the point of contact for the data principal for the purpose of grievance (***) redressal under section 32.**	
	***Explanation*.- For the purposes of this sub-section, the expression "key managerial personnel" means—** **(i) the Chief Executive Officer or the managing director or the manager;** **(ii) the company secretary;** **(iii) the whole-time director;** **(iv) the Chief Financial Officer; or** **(v) such other personnel as may be prescribed.**	
	(2) Nothing contained in sub-section (1) shall prevent the data fiduciary from assigning any other function to the data protection officer, which it may consider necessary.	
	(3) The data protection officer appointed under sub-section (1) shall be based in India and shall represent the data fiduciary under this Act.	
	31.(1) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.	Processing by entities other than data fiduciaries.
	(2) The data processor referred to in sub-section (1) shall not engage, appoint, use, or involve another data processor in the processing on its behalf, except with the authorisation of the data fiduciary and unless permitted in 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 and treat it **as** confidential.	

	32.(1) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner.	Grievance redressal by data fiduciary.
	(2) A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made 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 complaint made under sub-section (2) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary.	
	(4)Where a complaint is not resolved within the period specified under sub-section (3), or where the data principal is not satisfied with the manner in which the complaint is resolved, or the data fiduciary has rejected the complaint, the data principal may file a complaint to the Authority **(***) <u>under section 62</u>.**	
	CHAPTER VII **RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA**	
Prohibition on processing of sensitive personal data and critical personal data outside India.	**33.**(1) Subject to the conditions **<u>provided</u>**in sub-section (1) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.	
	(2) The critical personal data shall only be processed in India.	
	Explanation.—For the purposes of sub-section (2), the expression "critical personal data" means such personal data as	

	may be notified by the Central Government to be the critical personal data.	
Conditions for transfer of sensitive personal data and critical personal data.	**34.**(1) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—	
	(a) the transfer is made pursuant to a contract or intra-group scheme approved by the Authority **in consultation with the Central Government**:	
	Provided that such contract or intra-group scheme shall not be approved, **if the object of such transfer is against public policy or State policy and** unless it makes the provisions for—	
	(i) effective protection of the rights of the data principal under this Act, including in relation to further transfer to any other person; and	
	(ii) liability of the data fiduciary for harm caused due to non-compliance of the provisions of such contract or intra-group scheme by such transfer; **(***)**	
	(b) the Central Government, after consultation with the Authority, has allowed the transfer to a country or, such entity or class of (***) **entities** in a country or, an international organisation on the basis of its finding that–	
	(i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements; **(***)**	
	(ii) such transfer shall not prejudicially affect the enforcement of relevant laws by authorities with appropriate jurisdiction**; and**	
	(iii) such sensitive personal data shall not be shared with any foreign government or agency	

	unless such sharing is approved by the Central Government:	
	Provided that any finding under this clause shall be reviewed periodically in such manner as may be prescribed; **or**	
	(c) the Authority**, in consultation with the Central Government,** has allowed transfer of any sensitive personal data or class of sensitive personal data necessary for any specific purpose.	
	***Explanation.*- For the purposes of this sub-section, an act is said to be against "public policy" or "State policy", if the said act promotes the breach of any law or is not in consonance with any public policy or State policy in this regard or has a tendency to harm the interest of the State or its citizens.**	
	(2) Notwithstanding anything contained in sub-section (2) of section 33, any critical personal data may be transferred outside India, only where such transfer is—	
	(a) to a person or entity engaged in the provision of health services or emergency services where such transfer is necessary for prompt action under section 12; or	
	(b) to a country or, any entity or class of (***) **entities** in a country or, to an international organisation, where the Central Government has deemed such transfer to be permissible under clause (b) of sub-section (1) and where such transfer in the opinion of the Central Government does not prejudicially affect the security and strategic interest**s** of the State.	
	(3) Any transfer under clause (a) of sub-section (2) shall be **(***) informed** to the Authority within such period as may be specified by regulations.	

	CHAPTER VIII **EXEMPTIONS**	
	35. <u>Notwithstanding anything contained in any law for the time being in force,</u> where the Central Government is satisfied that it is necessary or expedient,—	Power of Central Governmen t to exempt any agency of Governmen t from application of **(***)** Act.
	(i) in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States **<u>or</u>** public order; or	
	(ii) for preventing incitement to the commission of any cognizable offence relating to sovereignty and integrity of India, the security of the State, friendly relations with foreign States **<u>or</u>** public order,	
	it may, by order, for reasons to be recorded in writing, direct that all or any of the provisions of this Act shall not apply to any agency of the Government in respect of processing of such personal data, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, as may be prescribed.	
	Explanation. —For the purposes of this section, —	
2 of 1974.	(i)the term "cognizable offence" means the offence as defined in clause (c) of section 2 of the Code of Criminal Procedure, 1973;	
	(ii) the expression "processing of such personal data" includes sharing by or sharing with such agency of the Government by any data fiduciary, data processor or data principal; **<u>and</u>**	
	<u>(iii) the expression "such procedure" refers to just, fair, reasonable and proportionate procedure.</u>	
Exemption of certain	**36.**The provisions of Chapter II **(***) <u>to VII, except section 24</u>**, shall not apply where—	

provisions for certain processing of personal data.		
	(a) **the**personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or (***) contravention of any law for the time being in force;	
	(b) **the** 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;	
	(c) **the**processing of personal data by any court or tribunal in India is necessary for the exercise of any judicial function;	
	(d) **the** personal data is processed by a natural person for any personal or domestic purpose, except where such processing involves disclosure to the public, or is undertaken in connection with any professional or commercial activity; or	
	(e) **the** processing of personal data is necessary for or relevant to a journalistic purpose, by any person and is in compliance with**the rules and regulations made under this Act**, **(***)** code of ethics issued by the Press Council of India, or by any **statutory** media **(***)** regulatory organisation.	
Power of Central Governme nt to exempt certain data processors.	**37.** The Central Government may, by notification, exempt from the application of this Act, the 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.	
Exemption for research,	**38.**Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that—	

archiving or statistical purposes.		
	(a) the compliance with the provisions of this Act shall disproportionately divert resources from such purpose;	
	(b) the purposes of processing cannot be achieved if the personal data is anonymised;	
	(c) the data fiduciary has carried out de-identification in accordance with the code of practice specified under section 50 and the purpose of processing can be achieved if the personal data is in de-identified form;	
	(d) the personal data shall not be used to take any decision specific to or action directed to the data principal; and	
	(e) the personal data shall not be processed in the manner that gives rise to a risk of significant harm to the data principal,	
	it may, by notification, exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations.	
	39.(1) The provisions of sections 7, 8, 9, clause (c) of sub-section (1) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated.	Exemption for **(***) <u>non automated</u>** processing by small entities.
	(2) For the purposes of sub-section (1), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to—	
	(a) the turnover of data fiduciary in the preceding financial year;	
	(b) the purpose of collection of personal data for disclosure to any other individuals or entities; and	

	(c) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.	
	40.(1) The Authority **(***)** **<u>may</u>**, for the purposes of encouraging innovation in artificial intelligence, machine-learning or any other emerging technology in public interest, create a Sandbox.	Sandbox for encouraging innovation, etc.
	(2) Any data fiduciary **<u>as well as start-ups</u>** whose privacy by design policy is certified by the Authority under sub-section (3) of section 22 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1).	
	(3) Any data fiduciary applying for inclusion in the Sandbox under sub-section (2) shall furnish the following information, namely:—	
	(a) the term for which it seeks to utilise the benefits of Sandbox, provided that such term shall not exceed twelve months;	
	(b) the innovative use of technology and its beneficial uses;	
	(c) the data principals or categories of data principals participating under the proposed processing; and	
	(d) any other information as may be specified by regulations.	
	(4) The Authority shall, while including any data fiduciary in the Sandbox, specify—	
	(a) the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months;	
	(b)the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and	
	(c) that the following obligations shall not apply or apply with modified form to such data fiduciary, namely:—	

	(*i*) the obligation to (***) **comply with the provisions** under sections 4 and 5;	
	(*ii*) limitation on collection of personal data under section 6; and	
	(*iii*) any other obligation to the extent, it is directly depending on (***) sections 5 and 6; and	
	(iv) the restriction on retention of personal data under section 9.	
	***Explanation*.- For the purposes of this Act, the expression "Sandbox" means such live testing of new products or services in a controlled or test regulatory environment for which the Authority may or may not permit certain regulatory relaxations for a specified period of time for the limited purpose of the testing.**	
	CHAPTER IX **DATA PROTECTION AUTHORITY OF INDIA**	
Establishment of Authority.	**41.**(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 referred to in sub-section (1) 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.	
Composition and qualifications for appointment of **Chairpers**	**42.**(1) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be (***) **an expert in the area of law** having **such** qualification**s** and experience (***) **as may be prescribed**.	

on and Members.		
	(2) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a **S**election **C**ommittee consisting of—	
	(i) the Cabinet Secretary, who shall be Chairperson of the **S**election **C**ommittee;	
	(ii) the Attorney General of India - Member;	
	(**iii**) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs **- Member**; **(***)**	
	(iv) the Secretary to the Government of India in the Ministry or Department dealing with (***) Electronics and Information Technology **- Member;**	
	(v) an independent expert to be nominated by the Central Government from the fields of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration or related subjects - Member;	
	(vi) a Director of any of the Indian Institutes of Technology to be nominated by the Central Government – Member; and	
	(vii) a Director of any of the Indian Institutes of Management to be nominated by the Central Government – Member.	
	(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 shall have qualification**s** and specialised knowledge and experience of (***) not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects.	

	(5) A vacancy caused to the office of the Chairperson or any other **M**ember of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.	
	43.(1) The Chairperson and the Members of the Authority 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.	Terms and conditions of appointment.
	(2) The salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority shall be such as may be prescribed.	
	(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 of the Authority 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.	
	44.(1) The Central Government may remove from office, the Chairperson or any Member of the Authority who—	Removal of Chairperson or other Members.
	(a) has been adjudged as an insolvent;	
	(b) has become physically or mentally incapable of acting as a Chairperson or **M**ember;	
	(c) has been convicted of an offence, which in the opinion of the Central Government, involves moral turpitude;	

	(d) has so abused their position as to render their continuation in office detrimental to the public interest; or	
	(e) has acquired such financial or other interest as is likely to affect prejudicially(***) **his** functions as a Chairperson or a Member.	
	(2) No Chairperson or any Member of the Authority shall be removed under clause (d) or (e) of sub-section (1) unless he has been given a**n**(***) opportunity of being heard.	
Powers of Chairperson.	**45.**The Chairperson of the Authority shall (***) have powers of general superintendence and direction **in the conduct** of the affairs of the Authority and **he** shall, (***) **in addition to presiding over the meetings of the Authority,** exercise all powers and do all such acts and things which may be exercised or done by the Authority under this Act.	
Meetings of Authority.	**46.**(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 **over** 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 his absence, the **M**ember presiding, shall have the right to exercise a second or casting 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 his 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.	
Vacancies, etc., not to invalidate proceedings of Authority.	**47.**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.	
Officers and other employees of Authority.	**48.**(1) The Authority may appoint such officers, other 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 by regulations.	
Powers and functions of Authority.	**49.**(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 about data protection.	
	(2) Without prejudice to the generality of the foregoing and other functions under this Act, the functions of the Authority shall include—	
	(a) monitoring and enforcing application of the provisions of this Act and **the rules and regulations made thereunder**;	
	(b) taking prompt and appropriate action in response to (***) data breach in accordance with the provisions of this Act;	
	(c) 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;	
	(d) examination of any data audit reports and taking any action pursuant thereto;	
	(e) issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data auditors and specifying the qualifications, code of	

	conduct, practical training and functions to be performed by such data auditors;	
	(f) classification of data fiduciaries;	
	(g) monitoring cross-border transfer of personal data;	
	(h) specifying codes of practice;	
	(i) promoting awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data amongst data fiduciaries and data principals;	
	(j) monitoring technological developments and commercial practices that may affect protection of personal data;	
	(k) promoting measures and undertaking research for innovation in the field of protection of personal data;	
	(l) advising Central Government, State Government and any other authority on measures required to be taken to promote protection of personal data and ensuring consistency of application and enforcement of this Act;	
	(m) specifying fees and other charges for carrying out the purposes of this Act;	
	(n) receiving and inquiring complaints under this Act; **(***)**	
	(o) monitoring, testing and certification by an appropriate agency authorized by the Central Government for this purpose to ensure integrity and trustworthiness of hardware and software on computing devices to prevent any malicious insertion that may cause data breach; and	
	(p) performing such other functions as may be prescribed.	
	(3) Where, pursuant to the provisions of this Act, the Authority processes any 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 (***) **such** data fiduciary or data processor, it shall not disclose such information unless required under any law **for the time being in**	

	force to do so, or where it is required to carry out its function**s** under this section.	
Codes of practice.	**50.**(1) The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act.	
	(2) Notwithstanding anything contained in sub-section (1), the Authority may approve any code of practice submitted by-	
	(i) **the associations representing-**	
	(a) technical services organizations;	
	(b) (***) industry or trade (***)	
	(c) (***) the interest of data principals	
	(ii) any sectoral regulator or statutory Authority; or	
	(iii) any **D**epartments or **M**inistries of the Central **Government** or State Government.	
	(3) The Authority shall ensure transparency and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving any code of practice under this section.	
	(4) A code of practice under sub-section (1) or sub-section (2), shall not be issued unless the Authority has made consultation with the sectoral regulators and other stakeholders including the public and has followed such procedure as may be prescribed.	
	(5) A code of practice issued under this section shall not derogate from the provisions of this Actor any other law for the time being in force.	
	(6) The code of practice under this Act may include the following matters, namely:—	
	(a) requirements for notice under section 7 including any model forms or guidance relating to notice;	
	(b) measures for ensuring quality of personal data processed under section 8;	
	(c) measures pertaining to the retention of personal data under section 9;	

	(d) manner for obtaining valid consent under section 11;	
	(e) processing of personal data under section 12;	
	(f) activities where processing of personal data may be undertaken under section 14;	
	(g) processing of sensitive personal data under Chapter III;	
	(h) processing of personal data under any other ground for processing, including processing of personal data of children and age-verification under this Act;	
	(i) exercise of any right by data principals under Chapter V;	
	(j) the standards and means by which a data principal may avail the right to data portability under section 19;	
	(k) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter VI;	
	(l) standards for security safeguards to be maintained by data fiduciaries and data processors under section 24;	
	(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 (***) data breach under section 25;	
	(p) manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section 27;	
	(q) transfer of personal data outside India pursuant to section 34;	
	(r) processing of any personal data or sensitive personal data to carry out any activity necessary for research, archiving or statistical purposes under section 38; and	

	(s) any other matter which, in (***) view of the Authority, may be necessary **or relevant** to be provided in the code of practice.	
	(7) The Authority may review, modify or revoke a code of practice issued under this section in such manner as may be prescribed.	
	51.(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 any data fiduciary or data processor who shall be bound to comply with such directions.	Power of Authority to issue directions.
	(2) No direction shall be issued under sub-section (1) unless the Authority has given a**n** (***) opportunity of being heard to the data fiduciar**y** (***) or **the** data processor 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 deems fit, subject to which the modification, suspension, withdrawal or cancellation shall have effect.	
	52.(1) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.	Power of Authority to call for information .
	(2) If the Authority requires a data fiduciary or a data processor to provide any information under sub-section (1), it shall provide a notice in writing to the data fiduciary or the data processor stating the reasons for such requisition.	
	(3) The Authority shall, by regulations, specify the manner in which the data fiduciary or 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, the period within which such information is to be furnished and the form in which such information may be provided.	
Power of Authority to conduct inquiry.	**53.**(1) The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that—	

	(a) the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interest**s** of data principals; or	
	(b) any data fiduciary or data processor has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority.	
	(2) For the purposes 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 fiduciary or data processor and to report to the Authority on any inquiry made.	
	(3) For the purpose of any inquiry under this section, the Inquiry Officer may, wherever necessary, seek the assistance of any other person.	
	(4) The order referred to in sub-section (2) shall specify the reasons for 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, 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 provide a notice in writing to the persons referred to in sub-section (5) stating the reasons thereof and the relationship between the data fiduciary and the **scope of 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**s** 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.	

5 of 1908.	(8) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under this section, the Authority or the Inquiry Officer, as the case may be, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely—	
	(a) the discovery and production of books of account, **data** and other documents, at such place and at such time as may be specified **by regulations**;	
	(b) summoning and enforcing the attendance of persons and examining them on oath;	
	(c) inspection of any book, document, register, record or**data** of any data fiduciary;	
	(d) issuing commissions for the examination of witnesses or documents; and	
	(e) any other matter which may be prescribed.	
	54.(1) On receipt of a report under sub-section (2) of section 53, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—	Action to be taken by Authority pursuant to **(***)** inquiry.
	(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) **(***)** **direct** the data fiduciary or data processor to cease and desist from committing or causing any violation of the provisions of this Act;	
	(d) **(***)** **direct** the data fiduciary or 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 significant data fiduciary;	
	(g) suspend or discontinue any cross-border (***) **transfer** of personal data; or	
	(h) **(***) direct** 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 deem**(***)** fit.	
	(2) A data fiduciary or data processor aggrieved by an order made under this section may prefer an appeal to the Appellate Tribunal **under section 73**.	
Search and seizure.	**55.**(1) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer **(***)shall, with the prior approval of the Authority,**make an application to such designated court, as may be notified by the Central Government, for an order for the seizure of such books, registers, documents**,**(***) records **or data**.	
	(2) The Inquiry Officer may require the services of any police officer or any officer of the Central Government **or State Government**, or of (***) **all**, to assist him for the purposes **(***) provided** in sub-section (1) and it shall be the duty of every such officer to comply with such requisition.	
	(3) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer—	
	(a) to enter, with such assistance, as may be required, the place or places where such books, registers, documents, (***) records **or data** are kept;	
	(b) to search that place or those places in the manner specified in the order; and	

	(c) to seize books, registers, documents, (***) records **or data** it considers necessary for the purposes of the inquiry.	
	(4) The Inquiry Officer shall keep in (***) **his** custody the books, registers, documents, **(***)** records **or data** seized under this section for such period not later than the conclusion of the inquiry as (***) **he** considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return.	
2 of 1974.	(5) Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.	
Co-ordination between Authority and other regulators or authorities.	**56.**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 **including economic activities**.	
	CHAPTER X **PENALTIES AND COMPENSATION**	
Penalties for contravening certain provisions of **(***)** Act.	**57.**(1)Where the data fiduciary contravenes any of the following provisions, **namely:-**	
	(a) obligation to take prompt and appropriate action in response to a data **(***)** breach under section 25;	
	(b) failure to register with the Authority under sub-section (2) of section 26;	
	(c)obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;	
	(d)obligation to conduct a data audit by a significant data fiduciary under section 29;**or**	

	(e)appointment of a data protection officer by a significant data fiduciary under section 30,	
	it shall be liable to **(***)<u>such</u>**penalty**(***) <u>as may be prescribed</u> (***)**.	
	(2)Where a data fiduciary contravenes any of the following provisions, **<u>namely:</u>**—	
	(a) processing of personal data in violation of the provisions of Chapter II or Chapter III;	
	(b) processing of personal data of children in violation of the provisions of Chapter IV;	
	(c) failure to adhere to security safeguards as per section 24;or	
	(d) transfer of personal data outside India in violation of the provisions of Chapter VII,	
	it shall be liable to **(***) <u>such</u>**penalty**(***) <u>as may be prescribed</u> (***)**.	
	(3) For the purposes of this section, **(***)** where **<u>any</u>** of **<u>the</u>** (***) provisions referred to in this section has been contravened by the State, the maximum penalty shall **(***) <u>be such as may be prescribed</u>**.	
Penalty for failure to comply with data principal requests under Chapter V.	**58.**Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V, 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.	
Penalty for failure to furnish report, returns, informatio n, etc.	**59.** If any data fiduciary, who is required under this Act or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such data fiduciary shall be liable to **<u>a</u>** 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.	

Penalty for failure to comply with direction or order issued by Authority.	**60.**If any data fiduciary or data processor fails to comply with any directions issued by the Authority under section 51 or order issued by the Authority under section 54,-	
	(i) such data fiduciary **(***)** shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crore **rupees(***); or**	
	(ii) **such** data processor **shall be liable to a penalty which (***)** may extend to five thousand rupees for each day during which such default continues, subject to a maximum of fifty lakh rupees.	
Penalty for contravention where no separate penalty has been provided.	**61.**Where any person fails to comply with any provision of this Act or the rules or regulations made thereunder applicable to such person, for which no separate penalty has been provided, then, such person shall be liable to a penalty which may extend to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty-five lakh rupees in other cases.	
Right to file complaint or application.	**62. (1) The aggrieved data principal referred to in section 32 may file a complaint to the Authority within such period and in such manner as may be specified by regulations.**	
	(2) The data principal may seek compensation under section 65 by filing an application to the Authority in such form, manner and within such period as may be prescribed.	
	(3) The Authority may forward the complaint or application filed by the data principal to the Adjudicating Officer for adjudging such complaint or application, as the case may be.	
Appointment of	**63.**(1)For the purpose of adjudging the penalties under sections 57 to 61or awarding compensation under section 6**5**, the	

Adjudicating Officer.	Authority shall appoint such Adjudicating Officer**s** as may be(***) **required**.	
	(2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication under this Act, prescribe—	
	(a) **the**number of Adjudicating Officers to be appointed under sub-section (1);	
	(b) **the**manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;	
	(c) **the**jurisdiction of Adjudicating Officers; **and**	
	(d) such other requirements as (***) may (***) **be prescribed**.	
	(3)The Adjudicating Officers shall be persons of ability, integrity and standing, and (***) **shall possess such qualifications,** specialized knowledge, (***) **and (***) adequate** (***) professional experience**,** in the fields of law, cyber and internet laws, information technology law and policy, data protection and related subjects**,as may be prescribed**.	
	64.(1) No penalty shall be imposed under this Chapter, except after an inquiry made in such manner as may be prescribed, and the data fiduciary or data processor or any person, as the case may be, has been given a**n** (***)opportunity of being heard:	Procedure for adjudication by Adjudicating Officer.
	Provided that no inquiry under this section shall be initiated except by a complaint made by the Authority.	
	(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 contravention of the provisions of this Act, the	

	Adjudicating Officer may impose such penalty **as** specified under relevant section.	
	(4) While deciding whether to impose a penalty under sub-section (3) and in determining the quantum of penalty under sections 57 to 61, the Adjudicating Officer shall have due regard to the **guidelines as may be specified by the Authority for determination and imposition of penalty taking into account any of the**following factors, namely:—	
	(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; (***) **or**	
	(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 **made** under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal **under section 73**.	
Compensation.	**65.**(1) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, 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 section 31, 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 24, or where it has violated any provisions of this Act. (***)	
	(2) **(***)**	
	(2) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any contravention by the same data fiduciary or data processor, (***) **a representative application**may be instituted on behalf of all such data principals seeking compensation for the harm suffered.	
	(3) While deciding to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have regard to**any of** the following factors, namely:—	
	(a) nature, duration and extent of violation of the provisions of the Act, rules (***) or regulations (***) **made** 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;**or**	
	(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.	
	(4) 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, then, each data fiduciary or data processor may be ordered to pay the entire compensation for the harm to ensure effective and speedy compensation to the data principal.	
	(5) Where a data fiduciary or a data processor has, in accordance with sub-section **(4)**, 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.	
	(6) Any person aggrieved by an order made under this section by the Adjudicating Officer may prefer an appeal to the Appellate Tribunal **under section 73**.	
	(7) The (***) procedure for hearing of (***) **an application** under this section **shall be such as may be prescribed.**	
	66. No compensation awarded, or penalty imposed, under this Act shall prevent the award of compensation or imposition of any other penalty or punishment under this Act or any other law for the time being in force.	Compensation or penalties not to interfere with other punishment.
	67.(1) The amount of any penalty imposed or compensation awarded under this Act, if not paid, may be recovered as if it were an arrear of land revenue.	Recovery of amounts.
	(2) All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.	
	CHAPTER XI **APPELLATE TRIBUNAL**	
Establishment of	**68.**(1) The Central Government shall, by notification, establish an Appellate Tribunal to—	

Appellate Tribunal.		
	(a) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 20;	
	(b) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 54;	
	(c) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section **64**; and	
	(d)hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (***) **(6)**of section **65**.	
	(2) The Appellate Tribunal shall consist of a Chairperson and **(***) such number of** members**, not exceeding six,** to be appointed by the Central Government.	
	(3) The Appellate Tribunal shall be established at such place or places, as the Central Government may, in consultation with the Chairperson of the Appellate Tribunal, notify.	
	(4) Notwithstanding anything contained in sub-sections (1) to (3), where, in the opinion of the Central Government, any existing (***) **Tribunal** is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such (***) **Tribunal** to act as the Appellate Tribunal under this Act.	
Qualifications, appointment, term, conditions of service of **Chairperson and** Members.	**69.**(1) A person shall not be qualified for appointment as the Chairperson or a Member of the Appellate Tribunal unless he—	
	(a) in the case of Chairperson, is , or has been a Judge of the Supreme Court or Chief Justice of a High Court **or is qualified to be a Judge of the Supreme Court;**	

	(b) in the case of a **M**ember, **(***)is** a person who is **(***)an expert and has ability, integrity, standing and specialized knowledge with an experience of not less than twenty years** in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, **public administration** or any related subject.	
	(2) (***) The manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any **M**ember of the Appellate Tribunal, **shall be such as may be prescribed.**	
	70. 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 **(***)made thereunder** to fill the vacancy and the proceedings may be continued before the Appellate Tribunal from the stage at which the vacancy is filled.	Vacancies.
	71.(1) The Central Government shall provide the Appellate Tribunal with such officers and employees as it may deem fit.	Staff of Appellate Tribunal.
	(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 **payable to** and other **terms and** conditions of service of such officers and employees of the Appellate Tribunal shall be such as may be prescribed.	
	72.(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.	Distributio n of business amongst Benches.
	(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.	
	73.(1) Any person aggrieved by the decision **or order** of the Authority **or an Adjudicating Officer**, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed:	Appeals to Appellate Tribunal.
	Provided that the Appellate Tribunal may entertain any appeal 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.	
	(2) On receipt of an appeal 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 deems fit.	
	(3) 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 **or the Adjudicating Officer**, as the case may be.	
	(4) 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 preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal **(***)** and make such orders as it thinks fit.	
Procedure and powers of Appellate Tribunal.	**74.**(1) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 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.	5 of 1908.
	(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, while trying a suit, in respect of the following matters, namely—	5 of 1908.
	(a) summoning and enforcing the attendance of any person and examining **him** on oath;	

	(b) requiring the discovery and production of documents;	
	(c) receiving evidence on affidavits;	
	(d) subject to the provisions of section**s** 123 and **(***)** 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office;	1 of 1872.
	(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 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.	45 of 1860. 2 of 1974.
Orders passed by Appellate Tribunal to be executable as (***) decree.	**75.(***)Every** order **(***) made** 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) (***)	
Appeal to Supreme Court.	**76.**(1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or **(***)** any other law **for the time being in force**, an appeal shall lie against any order of the Appellate Tribunal (***) to the Supreme Court on any substantial question of law.	5 of 1908.

	(2) (***)	
	(**2**) Every appeal **made** under this section shall be preferred within a period of (***) **sixty** days from the date of the decision or order appealed against:	
	Provided that the Supreme Court may entertain the appeal after the expiry of the said period of (***) **sixty** days, if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time.	
	77. The applicant or appellant may either appear in person or authorize one or more legal practitioners or any of its officers **or experts** to present his or its case before the Appellate Tribunal.	Right to legal representation.
	Explanation.—For the purposes of this section, **the expression** "legal practitioner" **shall** include (***) an advocate or an attorney**(***)**.	
	78. 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.	Civil court not to have jurisdiction.
	CHAPTER XII **FINANCE, ACCOUNTS AND AUDIT**	
	79. 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.	Grants by Central Government.
	80.(1) There shall be constituted a Fund to be called the Data Protection Authority Fund to which the following shall be credited—	Data Protection Authority (***) Fund (***).
	(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.	
	(2) 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.	
	81.(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 in consultation with the Comptroller and Auditor-General of India.	Accounts and Audit.
	(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 him in connection with such audit shall be reimbursed to him by the Authority.	
	(3) The Comptroller and Auditor-General of India and any other person appointed by him 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 (***) **him** in this behalf together with the audit report thereon shall be forwarded annually to the Central Government **by the Authority** and the Central Government shall cause the same to be laid, as soon as may be after it is made, before each House of the Parliament.	
Furnishing of returns, etc., to Central Governme nt.	**82.**(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 (including statement on enforcement action taken) 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 prepared under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament.	
	(4) A copy of the report prepared under sub-section (2) shall also be made publicly available by the Authority.	
	CHAPTER XIII **OFFENCES**	
Re-identification and processing of de-identified personal data.	**83.**(1) Any person who, knowingly or intentionally—	
	(a) re-identifies **the** 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 with a fine which may extend to two lakh rupees or **with**both.	
	(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment under this section, if he 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.	

2 of 1974.	**84.**(1)Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable.	Offences to be cognizable and non-bailable.
	(2) No court shall take cognizance of any offence **punishable** under this Act, save on a complaint **in writing** made by the Authority **or by any officer duly authorized by it for this purpose**.	
	85.(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 **(***) that part of** the business of the company **to which the offence relates**, as well as the company, (***)shall be liable to be proceeded against and punished accordingly.	Offences by companies.
	(2) Nothing contained in sub-section (1) shall render any such person liable to **(***) be proceeded against and punished accordingly under** this Act, if he proves that the offence was committed without his knowledge or that he 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 **(***)**liable to be proceeded against and punished accordingly**:**	
	Provided that an independent director and a non-executive director of a company shall be held liable only if it is shown that the acts of omission or commission by the company had occurred with his knowledge or with his consent attributable to him or where he had not acted diligently.	
	Explanation.— For the purpose**s** of this section, **the expressions**—	
	(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 thereof.	
Offences by **(***)** **Government data fiduciaries** .	**86.**(1) Where **(***)** an offence under this Act has been committed by any **(***) Government data fiduciary, an in-house enquiry shall be conducted by the Head of Office of the concerned data fiduciary and the person or officer concerned responsible for such offence** shall be liable to be proceeded against and punished accordingly.	
	(2) Nothing contained in sub-section (1) shall render any such person **or officer** liable to any punishment provided in this Act, if he proves that the offence was committed without his knowledge or that he 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 **(***) Government data fiduciary** 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 **(***) person or officer concerned referred to in sub-section (1)**, such officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.	
	(4)Notwithstanding anything **contained** in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply.	2 of 1974.
	CHAPTER XIV **MISCELLANEOUS**	
Power of Central Government to issue directions.	**87.**(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 **(***)** as the Central Government may give in writing to it from time to time:	
	Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.	
	(3) **(***)**	
Members, etc., to be public servants.	**88**. 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.	45 of 1860.
Protection of action taken in good faith.	**89.**No suit, prosecution or other legal proceedings shall lie against the Authority or its Chairperson, **M**ember, employee or officer for anything which is (***) in good faith **done**or intended to be done under this Act, or the rules **(***)** or **(***)** regulations **(***) made** thereunder.	
43 of 1961.	**90.**Notwithstanding anything contained in the Income Tax Act, 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.	Exemption from tax on income.
	91. The Authority may, by general or special order in writing delegate to any **M**ember 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 **to make regulations** under section 9**5**, as it may deem necessary.	Delegation.
	92.(1) Nothing in this Act shall prevent the Central Government from framing (***) any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse,**(***) and handling of non personal data including anonymised**personal data.	Act to promote framing of policies for digital economy, etc..
	(2) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-	

	based policies by the Central Government, in such manner as may be prescribed.	
	Explanation.-**(***)**	
	(3) The Central Government shall disclose annually the directions, made by it under sub-section (2), in such form as may be prescribed **and such disclosure shall be included in its Annual Report which shall be laid before each House of Parliament**.	
	93. (***) **Any** data fiduciary shall **not** process such biometric data as may be **(***) prescribed**, unless such processing is permitted by law.	Bar on processing certain forms of biometric data.
	94.(1)The Central Government may, by notification **and subject to the condition of previous publication,** make rules, **not inconsistent with the provisions of this Act,** to carry out the **(***) purposes** of this Act.	Power to make rules.
	(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) (***) any other harm under sub-clause (xii) of clause (23) of section 2;	
	(b) the manner in which a data fiduciary can share, transfer or transmit the personal data to any person as part of any business transaction under sub-section (4) of section 8;	
	(**c**) **the** other factors to be taken into consideration under clause (d) of sub-section (3) of section 16;	
	(**d**) the form and manner in which an application may be made to exercise the right under sub-section (2), and the manner of review of the order passed by the Adjudicating Officer under sub-section (4) of section 20;	
	(e) the steps to be taken by the Authority in case of breach of non-personal data under sub-section (6) of section 25;	

	(f) the threshold with respect to users of social media platform under sub-clause (i) of clause (f) of sub-section (1) and different thresholds for different classes of social media platforms under the proviso to clause (f) of sub-section (1) of section 26;	
	(**g**) the **(***) manner** of voluntary **(***) verification of the accounts of the** users of social media **platform** under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28;	
	(**h**) **(***) the manner of registration of data auditors under sub-section (4) of section 29;**	
	(i) the qualifications and experience of data protection officer and other personnel to be included under the expression "key managerial personnel" under sub-section (1) of section 30;	
	(**j**) the entity or class of (***) **entities** in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34;	
	(**k**) the place of head office of the Authority under sub-section (3) of section 41;	
	(**l**) **the** procedure to be followed by the selection committee under sub-section (3) of section 42;	
	(**m**) 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 43;	
	(**n**) the time and place for, and the rules and procedures in regard to transaction of business at the meetings **(including quorum)** of the Authority under sub-section (1) of section 46;	
	(**o**) other functions of the Authority under clause (**p**) of sub-section (2) of section 49;	
	(**p**) the procedure of issuance of a code of practice under sub-section (4), the manner in which the Authority may review, modify or revoke a code of practice under sub-section (7), of section 50;	
	(**q**) other matters under clause (e) of sub-section (8) of section 53 in respect of which the Authority shall have powers;	

	(r) the penalties for contravening of certain provisions of this Act by data fiduciaries including by State under sub-sections (1), (2) and (3) of section 57;	
	(s) the form, manner and the period for filing an application for compensation under sub-section (2) of section 62;	
	(**t**) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) **and the qualifications and the experience of such Adjudicating Officers under sub-section (3)**of section 6**3**;	
	(**u**) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 6**4**;	
	(**v**) the form and manner of making **an application**(***) and the procedure for hearing of (***) **an application** under sub-section (**7**) of section 6**5**;	
	(**w**) the manner of 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 (2) of section 6**9**;	
	(**x**)the procedure of fil**l**ing of vacancies in the Appellate Tribunal under section **70**;	
	(**y**) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 7**1**;	
	(**z**) the form, manner and fee for filing an appeal (***) with the Appellate Tribunal under sub-section (1) of section 7**3**;	
	(**za**) other matters under clause (i) of sub-section (2) of section 7**4** in respect of powers of the Appellate Tribunal;	
	(**zb**) the form of accounts, other relevant records and annual statement of accounts under sub-section (1), the intervals at which the accounts of the Authority shall be audited under sub-section (2) of section 8**1**;	
	(**zc**) the time, (***) the form and manner in which the returns, statements, and particulars are to be furnished to the	

	Central Government under sub-section (1), and annual report under sub-section (2) of section 8**2**;	
	(**zd**) the manner in which the Central Government may issue a direction, including the specific purposes for which data is sought under sub-section (2) and the form of disclosure of such directions under sub-section (3) of section 9**2**;	
	(ze) the details of biometric data not to be processed under section 93;	
	(**zf**) any other matter which is required to be, or may be prescribed, or in respect of which provision is to be made, by rules.	
	95.(1) The Authority may, by notification **and subject to the condition of previous publication**, make regulations, **not inconsistent with the provisions of this Act** and the rules made thereunder, to carry out the **(***) purposes** of this Act.	Power to make regulations.
	(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) **any other** 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 7;	
	(b) **the** manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9;	
	(c) **the reasonable purposes under sub-section (1)** and the safeguards for protecting the rights of data principals under sub-section (3) of section 14;	
	(d) the additional safeguards or restrictions under sub-section (2) of section 15;	
	(e) the manner of obtaining consent of the parent or guardian of a child (***) **and** the manner of verification of age of a child under sub-section **(2),** application of provision in modified form to data fiduciaries offering counsel**l**ing or child protection services under sub-section **(5)** of section 16;	
	(f) the manner in which the data principal shall have the right to access in one place the identities of the data fiduciaries with whom his personal data has been shared by any data fiduciary together with the categories of	

	personal data shared with them under sub-section (3) of section 17;	
	(g) the conditions and the manner in which the data principal shall have the right to correction and erasure of the personal data under section 18;	
	(h) the manner for determining the compliance which would not be technically feasible for non-application of the provisions of sub-section (1) under clause (b) of sub-section (2) of section 19;	
	(**i**) the period within which a data fiduciary must acknowledge the receipt of request under sub-section (1), the fee to be charged under sub-section (2),the period within which request is to be complied with under sub-section (3), and the manner and the period within which a data principal may file a complaint under sub-section (4) of section 21;	
	(j) the conditions under which the data fiduciary shall oblige to comply with the request made by the data principal under sub-section (5) of section 21;	
	(**k**) the manner **and the period** for submission of privacy by design policy under sub-section (2) of section 22;	
	(l) the form and manner for making the information available, any other information to be maintained by the data fiduciary under sub-section (1) and the manner of notifying the important operations in the processing of personal data related to data principal under sub-section (2) of section 23;	
	(**m**) the manner and the technical, operation**al**, financial and other conditions for registration of the **C**onsent **M**anager **(***)** under sub-section (5) of section 23;	
	(n) the manner of review of security safeguards periodically by data fiduciary or data processor under sub-section (2) of section 24;	
	(o) the form of notice under sub-section (2) of section 25;	
	(**p**) the manner of registration of significant data fiduciaries under sub-section (2) of section 26;	
	(**q**) the circumstances or class**(***)** of data fiduciaries or processing operations where data protection impact	

	assessments shall be mandatory and instances where data auditor shall be **(***) engaged** under sub-section (2), (***) the manner in which data protection officer shall review the data protection impact assessment and submit to the Authority under sub-section (4) of section 27(***)**and the conditions for processing under sub-section (5) of section 27;**	
	(**r**) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under sub-section (1) of section 28;	
	(**s**) the other factors to be taken into consideration under clause (g) of sub-section (2); the form and procedure for conducting audits under sub-section (3); (***) 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 29;	
	(**t**) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34;	
	(**u**) the provisions of the Act and the class of research, **archiving** or statistical purposes which may be exempted under section 38;	
	(v) the manner of inclusion by the data fiduciary for inclusion in the Sandbox under sub-section (2) and any other information required to be included in the Sandbox by the data fiduciary under clause (d) of sub-section (3) of section 40;	
	(**w**) 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 48;	
	(**x**) the code of practice under sub-section (1) of section 50;	
	(**y**) the **manner, period and** form(***) for providing information to the Authority by the data fiduciary **or data processor** under sub-section (3) of section 52;	
	(z) the place and time for discovery and production of books of account, data and other documents to the Authority or Inquiry Officer under clause (a) of sub-section (8) of section 53;	

	(za) the period and the manner of filing a complaint by the data principal before the Authority under sub-section (1) of section 62;	
	(**zb**) 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.	
	96. Every rule and regulation made under this Act and notification issued under sub-section (4) of section 6**8** 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 notification or both Houses agree that the rule or regulation or notification should not be made, the rule or regulation or notification 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 or notification.	Rules **(***),** regulations **and notification** to be laid before Parliament.
	97. Save as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained **in** any other law for the time being in force or any instrument having effect by virtue of any **such** law **(***)**.	Overriding effect of this Act.
	98.(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 it** to be necessary or expedient for removing the difficulty:	Power to remove difficulties.
	Provided that no such order shall be made under this section after the expiry of five years from the **date of** commencement of this Act.	
	(2)Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.	
(***)	**99.** The Information Technology Act, 2000 shall be amended in the manner specified in the Schedule to this Act.	Amendment of Act 21 of 2000.

	SCHEDULE **(*see* section 99)**	
	AMENDMENT TO THE INFORMATION TECHNOLOGY ACT, 2000 **(21 of 2000)**	
	1. Section 43A of the Information Technology Act, 2000 (hereafter in this Schedule referred to as the principal Act) shall be omitted.	Omission of section 43A.
39 of 1970	**2. In section 81 of the principal Act, in the proviso, after the words and figures "the Patents Act, 1970", the words and figures "or the Data Protection Act, 2021" shall be inserted.**	**Amendment of section 81.**
	3.In section 87 of the principal Act, in sub-section (2), clause (ob) shall be omitted.	Amendment of section 87.
