An Annotated Version of the Personal Data Protection Bill 2019

Comments and Recommendations

20 February, 2020

By **Amber Sinha**, **Elonnai Hickok**, **Pallavi Bedi**, **Shweta Mohandas** and **Tanaya Rajwade**

The Centre for Internet and Society, India

General Comments

1. *Executive notification cannot abrogate fundamental rights*

In 2017, the Supreme Court in *K.S. Puttaswamy v Union of India*[1] held the right to privacy to be a fundamental right. While this right is subject to reasonable restrictions, the restrictions have to meet a three fold requirement, namely (i) existence of a law; (ii) legitimate state aim; (iii) proportionality.

Under the 2018 Bill, the exemption to government agencies for processing of personal data from the provisions of the Bill in the '*interest of the security of the State*'[2] was subject to a law being passed by Parliament. However, under Clause 35 of the present Bill, the Central Government is merely required to pass a written order exempting the government agency from the provisions of the Bill.

Any restriction on the right to privacy will have to comply with the conditions prescribed in Puttaswamy I. An executive order issued by the central government authorising any agency of the government to process personal data does not satisfy the first requirement laid down by the Supreme Court in *Puttaswamy I* — as it is not a law passed by Parliament. The Supreme Court while deciding upon the validity of Aadhar in *K.S. Puttaswamy v Union of India*[3] noted that *"an executive notification does not satisfy the requirement of a valid law contemplated under Puttaswamy. A valid law in this case would mean a law passed by Parliament, which is just, fair and reasonable. Any encroachment upon the fundamental right cannot be sustained by an executive notification."*

2. *Exemptions under Clause 35 do not comply with the legitimacy and proportionality test*

The lead judgement in Puttaswamy I while formulating the three fold test held that the restraint on privacy emanate from the procedural and content based mandate of Article 21.[4] The Supreme Court in *Maneka Gandhi v Union India*[5] had clearly established that *"mere prescription of some kind of procedure cannot ever meet the mandate of Article 21. The procedure prescribed by law has to be fair, just and reasonable, not fanciful, oppressive and arbitrary."*[6]

The existence of a law is the first requirement; the second requirement is that of 'legitimate state aim'. As per the lead judgement this requirement 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."*[7] It is established that for a provision which confers upon the executive or administrative authority discretionary powers to be regarded as non-arbitrary, the provision should lay down clear and specific guidelines for the executive to exercise the power.[8]

The third test to be complied with is that the restriction should be 'proportionate,' i.e. the means that are adopted by the legislature are proportional to the object and needs sought to be fulfilled by the law. The Supreme Court in *Modern Dental College & Research Centre v State of Madhya Pradesh*[9] specified the components of proportionality standards —

i. A measure restricting a right must have a legitimate goal;
ii. It must be a suitable means of furthering this goal;
iii. There must not be any less restrictive, but equally effective alternative; and
iv. The measure must not have any disproportionate impact on the right holder

Clause 35 provides extensive grounds for the Central Government to exempt any agency from the requirements of the bill but does not specify the procedure to be followed by the agency while processing personal data under this provision. It merely states that the 'procedure, safeguards and oversight mechanism to be followed' will be prescribed in the rules.

The wide powers conferred on the central government without clearly specifying the procedure may be contrary to the three fold test laid down in Puttaswamy I, as it is difficult to ascertain whether a legitimate or proportionate objective is being fulfilled.[10]

3. *Limited powers of Data Protection Authority in comparison with the Central Government*

In comparison with the last version of the Personal Data Protection Bill, 2018 prepared by the Committee of Experts led by Justice Srikrishna, we witness an abrogation of powers of the Data Protection Authority (Authority), to be created, in this Bill. The powers and functions that were originally intended to be performed by the Authority have now been allocated to the Central Government. For example:

i. In the 2018 Bill, the Authority had the power to notify further categories of sensitive personal data. Under the present Bill, the Central Government in consultation with the sectoral regulators has been conferred the power to do so.
ii. Under the 2018 Bill, the Authority had the sole power to determine and notify significant data fiduciaries, however, under the present Bill, the Central Government has in consultation with the Authority been given the power to notify social media intermediaries as significant data fiduciaries.

In order to govern data protection effectively, there is a need for a responsive market regulator with a strong mandate, ability to act swiftly, and resources. The political nature of the personal data also requires that the governance of data, particularly the rule-making and adjudicatory functions performed by the Authority are independent of the Executive.

4. *No clarity on data sandbox*

The Bill contemplates a sandbox for "innovation in artificial intelligence, machine-learning or any other emerging technology in public interest." A Data Sandbox is a non-operational environment where the analyst can model and manipulate data inside the data management system. Data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[11] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions. This purportedly encourages innovation through the lowering of entry barriers by protecting newer entrants from unnecessary and burdensome regulation. Regulatory sandboxes can be interpreted as a form of responsive regulation by governments that seek to encourage innovation – they allow selected companies to experiment with solutions within an environment that is relatively free of most of the cumbersome regulations that they would ordinarily be subject to, while still subject to some appropriate safeguards and regulatory requirements. Sandboxes are regulatory tools which may be used to permit companies to innovate in the absence of heavy regulatory burdens. However, these ordinarily refer to burdens related to high barriers to entry (such as capital requirements for financial and banking companies), or regulatory costs. In this Bill, however, the relaxing of data protection provisions for data fiduciaries could lead to restrictions of the privacy of individuals. Limitations to fundamental rights on grounds of 'fostering innovation' is not a constitutional tenable position, and contradict the primary objectives of a data protection law. As the government continues to explore frameworks for innovation, it will be important that it coordinates with sectoral regulators to ensure harmonization. For example, The RBI has established a sandbox for banking sector[12] and TRAI has explored setting up a sandbox for the Telecom sector.[13]

5. *The primacy of 'harm' in the Bill ought to be reconsidered*

While a harms based approach is necessary for data protection frameworks, such approaches should be restricted to the positive obligations, penal provisions and responsive regulation of the Authority. The Bill does not provide any guidance on either the interpretation of the term 'harm,'[14] or "significant harm"[15] or on the various activities covered within the definition of the term. Terms such as 'loss of reputation or humiliation' 'any discriminatory treatment' are a subjective standard and are open to varied interpretations. This ambiguity in the definition will make it difficult for the data principal to demonstrate harm and for the DPA to take necessary action as several provisions are based upon harm being caused or likely to be caused. This is particularly concerning as the Bill envisions a tiered approach to harms - "harm" and "significant harm".Some of the significant provisions where 'harm' is a precondition for the provision to come into effect are —

i. **Clause 25:** Data Fiduciary is required to notify the Authority about the breach of personal data processed by the data fiduciary, if such breach **is likely to cause harm** to any data principal. The Authority after taking into account the severity of the harm that may be caused to the data principal will determine whether the data principal should be notified about the breach.

ii. **Clause 32 (2):** A data principal can file a complaint with the data fiduciary for a contravention of any of the provisions of the Act, **which has caused or is likely to cause 'harm'** to the data principal.

iii. **Clause 64 (1):** A data principal who **has suffered harm** as a result of any violation of the provision of the Act by a data fiduciary, has the right to seek compensation from the data fiduciary.

Clause 16(5): The guardian data fiduciary is barred from profiling, tracking or undertaking targeted advertising directed at children and undertaking any other processing of personal data that can cause **significant harm** to the child.

6. *Non personal data should be outside the scope of this Bill*

Clause 91(1) states that the Act does not prevent the Central Government from framing a policy for the digital economy, in so far as such policy does not govern personal data. The Central Government can, in consultation with the Authority, direct any data fiduciary to provide any anonymised personal data or other non-personal data to enable better targeting of delivery of services or formulation of evidence based policies in any manner as may be prescribed.

It is concerning that the data protection bill has specifically carved out an exception for the Central Government to frame policies for the digital economy and seems to indicate that the government plans to freely use any and all anonymized and/or non-personal data that rests with any data fiduciary that falls under the ambit of the bill to support the digital economy including for its growth, security, integrity, and prevention of misuse. It is unclear how the government, in practice, will be able to compel organizations to share this data. Further, there is a lack of clarity on the contours of the definition of non-personal data and the Bill does not define the term. It is also unclear whether the Central Government can compel the data fiduciary to transfer/share all forms of non-personal data and the rights and obligations of the data fiduciaries and data principals over such forms of data. Anonymised data refers to data which has 'irreversibly' been converted into a form in which the data principal cannot be identified. However, as several instances have shown 'irreversible' anonymisation is not possible. In the United States, the home addresses of taxi drivers were uncovered and in Australia individual health records were mined from anonymised medical bills.[16]

In September 2019, the Ministry of Electronics and Information Technology, constituted an expert committee under the chairmanship of Kris Gopalkrishnan to study various issues relating to non-personal data and to deliberate over a data governance framework for the regulation of such data.

The provision should be deleted and the scope of the bill should be limited to protection of personal data and to provide a framework for the protection of individual privacy. Until the report of the expert committee is published, the Central Government should not frame any law/regulation on the access and monetisation of non-personal/anonymised data nor can they create a blanket provision allowing them to request such data from any data fiduciary that falls within the ambit of the bill. If the government wishes to use data resting with a data fiduciary; it must do so on a case to case basis and under formal and legal agreements with each data fiduciary.

7. *Steps towards greater decentralisation of power*

We propose the following steps towards greater decentralisation of powers and devolved jurisdiction —

i. **Creation of State Data Protection Authorities:** A single centralised body may not be the appropriate form of such a regulator. We propose that on the lines of central and state commissions under the Right to Information Act, 2005, state data protection authorities are set up which are in a position to respond to local complaints and exercise jurisdiction over entities within their territorial jurisdictions.

ii. **More involvement of industry bodies and civil society actors:** In order to lessen the burden on the data protection authorities it is necessary that there is active engagement with industry bodies, sectoral regulators and civil society bodies engaged in privacy research. Currently, the Bill provides for involvement of industry or trade association, association representing the interests of data principals, sectoral regulator or statutory Authority, or an departments or ministries of the Central or State Government in the formulation of codes of practice. However, it would be useful to also have a more active participation of industry associations and civil society bodies in activities such as promoting awareness among data fiduciaries of their obligations under this Act, promoting measures and undertaking research for innovation in the field of protection of personal data.

8. *The Authority must be empowered to exercise responsive regulation*

In a country like India, the challenge is to move rapidly from a state of little or no data protection law, and consequently an abysmal state of data privacy practices to a strong data protection regulation and a powerful regulator capable of enabling a state of robust data privacy practices. This requires a system of supportive mechanisms to the stakeholders in the data ecosystem, as well as systemic measures which enable the proactive detection of breaches. Further, keeping in mind the limited regulatory capacity in India, there is a need for the Authority to make use of different kinds of inexpensive and innovative strategies.

We recommend the following additional powers for the Authority to be clearly spelt out in the Bill —

i. **Informal Guidance:** It would be useful for the Authority to set up a mechanism on the lines of the Security and Exchange Board of India (SEBI)'s Informal Guidance Scheme, which enables regulated entities to approach the Authority for non-binding advice on the position of law. Given that this is the first omnibus data protection law in India, and there is very little jurisprudence on the subject from India, it would be extremely useful for regulated entities to get guidance from the regulator.

ii. **Power to name and shame:** When a DPA makes public the names of organisations that have seriously contravened data protection legislation, this is a practice known as "naming and shaming." The UK ICO and other DPAs recognise the power of publicity, as evidenced by their willingness to co-operate with the media. The ICO does not simply post monetary penalty notices (MPNs or fines) on its websites for journalists to find, but frequently issues press releases, briefs journalists and uses social media. The ICO's publicity statement on communicating enforcement activities states that the "ICO aims to get media coverage for enforcement activities."

iii. **Undertakings:** The UK ICO has also leveraged the threats of fines into an alternative enforcement mechanism seeking contractual undertakings from data controllers to take certain remedial steps. Undertakings have significant advantages for the regulator. Since an undertaking is a more "co-operative"solution, it is less likely that a data controller will change it. An undertaking is simpler and easier to put in place. Furthermore, the Authority can put an undertaking in place quickly as opposed to legal proceedings which are longer.

9. *No clear roadmap for the implementation of the Bill*

The 2018 Bill had specified a roadmap for the different provisions of the Bill to come into effect from the date of the Act being notified.[17] It specifically stated the time period within which the Authority had to be established and the subsequent rules and regulations notified.

The present Bill does not specify any such blueprint; it does not provide any details on either when the Bill will be notified or the time period within within which the Authority shall be established and specific rules and regulations notified. Considering that 25 provisions have been deferred to rules that have to be framed by the Central Government and a further 19 provisions have been deferred to the regulations to be notified by the Authority the absence and/or delayed notification of such rules and regulations will impact the effective functioning of the Bill.

The absence of any sunrise or sunset provision may disincentivise political or industrial will to support or enforce the provisions of the Bill. An example of such a lack of political will was the establishment of the Cyber Appellate Tribunal. The tribunal was established in 2006 to redress cyber fraud. However, it was virtually a defunct body from 2011 onwards when the last chairperson retired. It was eventually merged with the Telecom Dispute Settlement and Appellate Tribunal in 2017.

We recommend that Bill clearly lays out a time period for the implementation of the different provisions of the Bill, especially a time frame for the establishment of the Authority. This is important to give full and effective effect to the right of privacy of the individual. It is also important to ensure that individuals have an effective mechanism to enforce the right and seek recourse in case of any breach of obligations by the data fiduciaries.

For offences, we suggest a system of mail boxing where provisions and punishments are enforced in a staggered manner, for a period till the fiduciaries are aligned with the provisions of the Act. The Authority must ensure that data principals and fiduciaries have sufficient awareness of the provisions of this Bill before bringing the provisions for punishment are brought into force. This will allow the data fiduciaries to align their practices with the provisions of this new legislation and the Authority will also have time to define and determine certain provisions that the Bill has left the Authority to define. Additionally enforcing penalties for offences initially must be in a staggered process, combined with provisions such as warnings, in order to allow first time and mistaken offenders from paying a high price. This will relieve the fear of smaller companies and startups who might fear processing data for the fear of paying penalties for offences.

10. *Lack of interoperability*

In its current form, a number of the provisions in the Bill will make it difficult for India's framework to be interoperable with other frameworks globally and in the region. For example, differences between the draft Bill and the GDPR can be found in the grounds for processing, data localization frameworks, the framework for cross border transfers, definitions of sensitive personal data, inclusion of the undefined category of 'critical data', and the roles of the authority and the central government.

11. *Legal Uncertainty*

In its current structure, there are a number of provisions in the Bill that, when implemented, run the risk of creating an environment of legal uncertainty. These include: lack of definition of critical data, lack of clarity in the interpretation of the terms 'harm' and 'significant harm', ability of the government to define further categories of sensitive personal data, inclusion of requirements for 'social media intermediaries', inclusion of 'non-personal data', framing of the requirements for data transfers, bar on processing of certain forms of biometric data as defined by the Central Government, the functioning between a consent manager and another data fiduciary, the inclusion of an AI sandbox and the definition of state. To ensure the greatest amount of protection of individual privacy rights and the protection of personal data while also enabling innovation, it is important that any data protection framework is structured and drafted in a way to provide as much legal certainty as possible.

Section Wise Comments and Recommendations

COMMENTS

The inclusion of 'norms for social media intermediary' in the introduction and subsequent provisions (Clause 26 which creates the category of social media intermediary and Clause 28 which allows for users of the services of a social media intermediary to voluntarily verify their accounts) of the Bill is out of scope of a data protection legislation and risks conflicting with provisions provided for intermediaries under Section 79[18] of the Information Technology Act, 2000.

RECOMMENDATIONS

We recommend that this category and relevant provisions be removed from the Bill.

THE PERSONAL DATA PROTECTION BILL, 2019

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:—

3(2)

COMMENTS

The Bill defines anonymisation as “Anonymisation” in relation to personal data, means the irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Authority.

RECOMMENDATIONS

Despite making the standards more specific by adding ‘standards of irreversibility’ **we reiterate our earlier comment.** The definition of anonymisation needs to protect privacy while enabling scientific research and innovation. There are multiple ways this can be achieved. For example, the term “irreversible” from the definition of anonymisation can be removed, in order to make provisions for the advancement in technology and research. This would also account for the challenges that exist with anonymization and the ability to re-identify individuals, as has been called out by many experts including the Sri Krishna Committee. In the current form, there are various exemptions tied to anonymised data, therefore, a high threshold is appropriate and may be applicable at a later stage if anonymisation procedures do in fact assure irreversibility in the future. Alternately, we can choose to borrow from the definition of anonymisation from the Brazilian data protection bill which defines anonymised data as “data related to a data subject who cannot be identified, considering the use of reasonable and available technical means at the time of the processing.” Another approach could be to require anonymisation through aggregation and once aggregated, personal data would no longer be protected under the Act. Aggregated data falls within the ambit of anonymised data, but could still raise community privacy concerns and thus fair and reasonable processing obligations would still need to apply.

CHAPTER 1
Preliminary

1. *Short title and commencement*

(1) This Act may be called the Personal Data Protection Act, 2019.

(2) It shall come into force on such date as the Central Government may, by notification 5 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. *Application of Act to processing of personal data.*

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.

3. *Definitions*

In this Act, unless the context otherwise requires,—

(1) “Adjudicating Officer” means the Adjudicating Officer appointed as such under sub-section (1) of section 62;

(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;

3(8)

COMMENTS

It is estimated that globally, one in three Internet users is a child under the age of 18.[19] As per the UNICEF Report on the State of the Children in 2017[20],persons between the ages of 15 to 24 are the most connected age group and that children are increasingly accessing the internet at a younger age.; in some countries children under 15 are as likely to use the internet as adults over 25. The White Paper published by the Justice Srikrishna Committee[21] recognised the fact that a substantial percentage of internet users in India are children below the age of 18 and so prescribing 18 as the age below which children would necessarily require parental consent would not be feasible and may actually have a chilling effect on the child's opportunity to freely use the Internet as a medium of self-expression, growth and education.

In this regard, **we reiterate our previous comments.** The Srikrishna report justifies making the age of consent the same as that of contract by stating that the provision of consent for data sharing is often intertwined with consent to contract. However while stating about the non consensual processing of data the report justifies it by stating that the relationship between a person and the state cannot be reduced to a contract. It is also important to note that in case of non consensual processing the report and the Bill is silent of the status of non consensual processing of the data of children.

RECOMMENDATIONS

We reiterate our previous recommendations. The provisions of parental consent allows the data fiduciary to implement services that will be used by children without ensuring that the data of children are processed with care. Such a responsibility should be reflected in the definition and under the 'privacy by design' principle found under chapter VII section 29. This would also provide children and parents with stronger grounds for redress- which are currently limited to the existence of consent. With this obligation in place, the age of mandatory consent could be reduced and the data fiduciary could have an added responsibility of informing the children in the simplest manner how their data will be used. Such an approach places a responsibility on data fiduciaires when implementing services that will be used by children and allows the children to be aware of data processing, when they are interacting with technology.

3(18)

COMMENTS

We reiterate our previous comments. This definition is restrictive in its scope including only a) number or other personal data used to identify an account, card or payment instrument; b) personal data regarding the relationship between a financial institution and a data principal including financial status and credit history.

(4) "Appellate Tribunal" means the Tribunal established under sub-section (1) or notified under sub-section (4) of section 67;

(5) "Authority" means the Data Protection Authority of India established under 35 sub-section (1) of section 41;

(6) "automated means" means any equipment capable of operating automatically in response to instructions given 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 behavioural 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) "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;

(12) "data auditor" means an independent data auditor referred to in section 29;

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

(14) "data principal" means the natural person to whom the personal data relates;

(15) "data processor" means any person, including the State, a company, any juristic entity or any individual, who processes personal data on behalf of a data fiduciary;

(16) "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;

(17) "disaster" shall have the same meaning as assigned to it in clause (d) of section 2 of the Disaster Management Act, 2005;

(18) "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;

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

(20) "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;

RECOMMENDATIONS

We reiterate our previous recommendations. The inclusive list in the second leg of the definition be expanded to include"financial statements, financial transactions and use of financial services offered by the financial institutions." We further recommend that the definition, without limitation, bring under its scope or refer to existing definitions of financial information such as that found in the "Master Direction Non-Banking Financial Company Account Aggregator (Reserve Bank) Directions, 2016" as it is connected to personal data."

(vi) any discriminatory treatment;

(vii) any subjection to blackmail or extortion;

(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal;

(ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled;

or

(x) any observation or surveillance that is not reasonably expected by the data principal;

(21) "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 5 for, or provision of health services, data associating the data principal to the provision

of specific health services;

(22) "intra-group schemes" means the schemes approved by the Authority under clause (a) of sub-section (1) of section 34;

(23) "in writing" includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000;

(24) "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;

(25) "notification" means a notification published in the Official Gazette and the expression "notify" shall be construed accordingly;

(26) "official identifier" means any number, code, or other identifier, assigned to 20 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;

(27) "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;

3 (28)

COMMENTS

Though this definition has been expanded from the definition specified in the 2018 Bill to include *"and shall include any inference drawn from such data for the purpose of profiling"*, **we reiterate our previous comment.** Data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information. The phrase 'having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person' qualifies the scope of data to be classified as personal data. Therefore, data through which a natural person may be identified or identifiable but does not relate to any characteristic, trait, attribute or any other feature of the identity of such personal would not be covered under this definition. This would exclude information like identity numbers or other identifiers as long as they are not in combination with features of the identity of a natural person. Identifiers and pseudo-identifiers can be used to track individuals and in doing so can reveal identifying information. Thus, identifiers and pseudo-identifiers should be covered by the definition. Further, there is a lack of clarity about the terms 'identified' and 'identifiable'. The Article 29 Working Party in the EU has made recommendations in this regard, which we find to be appropriate. "A natural person can be considered as "identified" when, within a group of persons, he or she is distinguished from all other members of the group. A natural person is "identifiable" when, although the person has not been identified yet, it is possible to do it by taking into account all the means likely reasonably to be used either by a data fiduciary or by any other person to identify the said person.

RECOMMENDATIONS

We reiterate our previous recommendations. The definition of "personal data" be expanded further to include identifiers meant to track natural persons. The current definition would not cover an identity number that is stored by a data fiduciary along with other non-identity information. While identity numbers would get covered by this definition at the point at which the identity number is combined with "any characteristic, trait, attribute, or any other feature of the identity of such natural person", since identity numbers are also "other information", it is important for persistent identifiers to be treated differently from other forms of information. It would also be useful to clarify that "any aspect" of the identity of the person is covered by the definition. We further recommend that the definition of personal data in the Bill reflects the understanding of 'identified' and identifiable' as articulated by the Article 29 Working Party.

We suggest the following alternate definition of personal data: *"Personal data is 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 any aspect of the identity of such natural person, any identifiers intended to be associated with such natural person, any combination of such features or identifiers, or any combination of such features or identifiers with any other information."*

(28) "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;

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

(30) "prescribed" means prescribed by rules made under this Act;

(31) "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;

(32) "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal;

(33) "regulations" means the regulations made by the Authority under this Act;

(34) "re-identification" means the process by which a data fiduciary or data processor may reverse a process of de-identification;

(35) "Schedule" means the Schedule appended to this Act;

(36) "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;

Terms that the Bill does not define or leaves for further defining by the Central Government or the Authority include:

(a) Data Trust Score

(b) Critical Personal Data

(c) Employer/Employee

(d) Non-personal data

These should be clearly defined.

(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;

(37) "significant data fiduciary" means a data fiduciary classified as such under sub-section (1) of section 26;

(38) "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;

(39) "State" means the State as defined under article 12 of the Constitution;

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

5

COMMENTS

The present Bill has removed language of any person processing personal data having a duty[22] towards data principals to process their data in a fair and reasonable manner and instead holds that "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."

RECOMMENDATIONS

In our previous comments we had supported using the framing of a 'duty' and had recommended that in order to make the import of this provision clearer and in order to align it with the intent of protecting against harm as explained in the Report and incorporated through the Bill, we believe that adding the word fiduciary will make it clear that it means processing in the interest of the data principal. We suggest the following alternate language: *"Any person processing personal data owes a fiduciary duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy and does not harm the interests of the data principal."*

5 (b)

COMMENTS

This provision has not been changed from the 2018 Bill and **we reiterate our previous recommendations.** The Bill provides guidance on the standards of 'clear', 'specific' and 'lawful' and that further the Authority has a responsibility to publish and provide guidance on the standards of 'clear', 'specific', and 'lawful' as clearer definition evolve through use cases the Authority evaluates in it functioning. For example: A purpose is specific if it is detailed enough to determine what kind of processing is and is not included within the specific purpose. Purposes such as "improving users' experience", "marketing purposes", "IT-security purposes' ' or "future research" will - without more detail - usually not meet the criteria of being 'specific'. A purpose is clear if it is expressed in such a way so as to be understood in the same way not only by the fiduciary (including all relevant staff) and any third party processors, but also by the data protection authority and the data principals concerned.

RECOMMENDATIONS

The incidental purpose condition of this section should be replaced with the compatible purpose standard where the processing is compatible with the purposes for which the personal data was initially collected. In order to reduce function creep the processing of data must be similar to the purpose for which it was collected. We further recommend that the assessment of compatibility be made on the basis of the following factors: (a) the relationship between the purposes for which the data have been collected and the purposes of further processing; (b) the context in which the data have been collected and the reasonable expectations of the data principals as to their further use; (c) the nature of the data and the impact of the further processing on the data principals; and (d) the safeguards applied by the data fiduciary to ensure fair and reasonable processing and to prevent any harm to the data subjects.

CHAPTER 2
Obligations of Data Fiduciary

4. ***Prohibition of processing of personal data.***

No personal data shall be processed by any person, except for any specific, clear and lawful purpose.

5. ***Limitation on purpose of processing of personal data.***

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 10 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

RECOMMENDATIONS

This provision has not been changed from the 2018 Bill and **we reiterate our previous recommendations.** The test of proportionality should also be added under this clause such that it reads as follows: The collection of personal data shall be limited to such data that is necessary and proportionate for the purposes of processing.

7

COMMENTS

The provision specified under clause 7(1) is substantially similar to the provisions in the 2018 Bill. However, the exceptions to the requirement of providing notice have been expanded. Under the 2018 Bill[23], the data fiduciaries were not required to provide notice in two circumstances, namely in situations identified as requiring prompt action under clause 15 and 21 including medical emergency, provision of services during a threat to public health, and provision of services during a disaster or breakdown of public order.

RECOMMENDATIONS

The exception to providing notice should be limited to the provisions specified in the 2018 Bill. In addition, **we reiterate our previous comments.** The provision of notice provides the data principal the right to be notified in order for her to provide informed consent. The notice should be transparent and must inform the data principal of not only her rights but also of the duties of the data fiduciary. Clause 12(4) of this Bill states that if the data principal withdraws her consent for the processing of any personal data necessary for the performance of a contract to which the data principal is a party, then all legal consequences of the effects of such withdrawal shall be borne by the data principal. Hence the notice should also communicate to the data principal the nature of the relationship between the two, and whether there is a statutory or contractual requirement. Additionally, the notice should communicate the possible consequences when she fails to provide such data, as well as withdrawal from processing. This is similar to Article 13(2)(e) of the GDPR. The data principal must also have the right to know if her data is being used to make automated decisions about her. The Report of the DP Bill justifies the absence of this right by stating that the Bill already has a provision to seek legal recourse in case of harm or a breach. However, we recommend that it is important to include this provision so that this remedy can be directly claimed from the data fiduciary without putting additional burden on the Authority. The data principal must be informed of the existence of automated decision making including profiling (as defined under Section 2(33) of this Bill).

6. ***Limitation on collection of personal data.***

The personal data shall be collected only to the extent that is necessary for the purposes of processing of such personal data.

7. ***Requirement of notice for collection or processing of personal data.***

(1) Every data fiduciary shall give to the data principal a notice, at the time of 15 collection of the personal data, or if the data is not collected from the data principal, as soon

as reasonably practicable, containing the following information, namely:—

(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 specified 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) 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 the regulations.

(2) The notice referred to in sub-section (1) shall be clear, concise and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.

(3) The provisions of sub-section (1) shall not apply where such notice substantially prejudices the purpose of processing of personal data under section 12.

8. *Quality of personal data processed.*

(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.

9. *Restriction on retention of personal data.*

(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.

10. *Accountability of data fiduciary.*

The data fiduciary shall be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf.

11

COMMENTS

The clause is substantially similar to the provisions in the 2018 Bill and **we reiterate our previous comments.** This clause states that consent needs to be sought no later than at the commencement of processing, however it might be difficult for a data principal to assess at the commencement of the processing in which all ways the data will be processed in the future. As the use of data to provide services becomes more pervasive and connected to other services the data might be processed by the fiduciary in ways that the data subject had not consented for. Clause 30(2) states that the data fiduciary shall notify the data principal of important operations in the processing of personal data through periodic notifications. However this provisions do not speak about seeking consent from the data principal for the new processing.

The system of blanket consent is problematic as it takes away the autonomy from the data principal. The report of the Data Protection Bill in 2018 proposed the formation of consent dashboards in order to reduce consent fatigue and to provide the data principal with information and autonomy over their data. The report also states that the dashboard would provide a system where the data fiduciary will be notified and consent be sought a new in the case of a processing that she had not consented to. However, the consent dashboard will be a time consuming process not only to implement but also to educate the data principals of its usage. Hence the Bill should provide minimum safeguards and measures to ensure that the data principal has autonomy over her data, and mere notice does not serve the purpose. The provision for withdrawal of consent can be justified as a reason, however if the principal wants to use the service offered by the data fiduciary but objects to the recent addition of processing she has only two options one to agree to the processing and two to withdraw from the service altogether.

RECOMMENDATIONS

We reiterate our previous comments. Clause 12 could state that the consent needs to be sought not just at the commencement of the processing but also at instances where the personal data is being processed for a purpose that was not stated at the time of consent. The report of the PDP Bill states about the importance of reducing consent fatigue however the choice needs to be on the data principal to know and consent to each new processing. The data principal must be allowed to enjoy the services for which she had consented for and given the choice to not consent for some processing that is not directly related to the service.

11. *Consent necessary for processing of personal data.*

(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.

Recommendation

At the outset, **we reiterate our previous comment:** necessity and proportionality need to be the two conditions that are imperative for non consensual data protection. We suggest the following alternative language for all the provisions that deals with non consensual processing in the Bill *"Personal data maybe processed if such processing is necessary and proportionate."*

12

COMMENTS

Clause 13 and 14 of the 2018 Bill provided for non-consensual processing of personal data have been condensed into Clause 12 (b) and (c) of this Bill. However, by virtue of Clauses 12 (c) to (f) it has also included the grounds for non-consensual processing of sensitive personal data provided under the 2018 Bill under the ambit of this clause. Under the 2018 Bill, the corresponding provisions for processing of sensitive personal data required compliance with a higher threshold. For instance, processing of sensitive personal data for prompt action[24] and for certain functions of the State[25] had to be *strictly necessary* and similarly, processing of sensitive personal data in compliance with law or any order of any court could be undertaken if such processing is *explicitly mandated* under any law made by Parliament or any State Legislature or is necessary for compliance with any order or judgement of any court or tribunal.

RECOMMENDATIONS

The provision of any and all public services or benefits should not be a blanket exemption to the consent requirement. Guidelines could be provided for the Authority/Central Government to identify and notify the specific delivery of public services permitting non-consensual processing of personal data of the data principal.

In addition, **we reiterate our previous comment.** The conditions for non-consensual processing of personal data should rely not only on necessity, but also on proportionality. The Puttaswamy judgement laid out the three pronged test of necessity, legitimacy and proportionality. The non- consensual use of data by the state for providing services for the benefit of the data principal needs to be not just necessary but also proportional to the exercise of the function of the state.

13

COMMENTS

We appreciate that this clause now requires consent for the processing of sensitive personal data by employers. However, it is unclear on what basis and by whom a determination will be reached 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 processing. Furthermore, the Bill

CHAPTER 3
Grounds for Processing Data Without Consent

12. *Grounds for processing of personal data without consent in certain cases.*

Notwithstanding anything contained in section 11, the personal data may be processed if such processing is necessary,—

(a) for the performance of any function of the State authorised by law 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 the Parliament or any State Legislature; or

(c) for compliance with any order or judgment of any Court 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. *Processing of personal data necessary for purposes related to employment, etc.*

(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.

does not define the term employment or employee nor does it refer to a specific definition in Indian law; leaving it unclear if the provisions will extend to all forms of work and types of people in the workforce.

14

Clause 14 establishes eight purposes for which personal data may be processed without consent. The list has been expanded from the 2018 Bill to include operation of search engines. For this, the processing must be necessary and the decision must be weighed against 5 considerations. The authority will also determine if notice under clause 7 is applicable or not.

COMMENT AND RECOMMENDATION

We recommend that the provision requires that processing of personal information without consent must be both **necessary** and **proportionate.** Furthermore, we recommend that 'credit scoring' and 'the operation of search engines' are removed from the list of purposes that may constitute 'reasonable purposes'. We also recommend removing 'prevention and detection of any unlawful activity including fraud' as we believe it is covered under the exception carved out in clause 36 (a). We finally recommend that standards be defined on which the authority makes a determination regarding the applicability of clause 7 (notice).

15

COMMENTS

This clause has been changed to empower the Central Government, in consultation with the Authority and the concerned sectoral regulators to notify further categories of personal data as sensitive personal data on the basis of four specified criteria. Under the 2018 Bill,[26] the Authority had the sole authority to classify further categorise personal data as sensitive personal data.

RECOMMENDATIONS

The rationale for authorising the Central Government, albeit in consultation with the Authority and the sectoral regulator to notify categories of personal data as sensitive personal data is unclear. We recommend that the provision as per the 2018 Bill should be reinstated and the Authority in consultation with the sectoral regulators should be empowered to determine further categories of personal data.

14. ***Processing of personal data for other reasonable purposes.***

(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.

15. ***Categorisation of personal data as sensitive personal data.***

(1) The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such 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 the processing of such category of personal data;

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

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

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

(2) The Authority may specify, by regulations, the additional safeguards or restrictions 5 for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.

16

COMMENTS

There is no provision for the data principal to withdraw her consent upon attaining the age of majority. In July 2019, the Central Government amended the Aadhar Act[27] permitting a child who has been enrolled in the Aadhar database by her parents/ guardian to seek cancellation of her Aadhar within six months of her attaining the age of 18.

RECOMMENDATIONS

We recommend that upon attaining the age of majority, the data principal should have the right to withdraw her consent to any further processing of her data. Further, **we reiterate our earlier recommendation.** The data principal on attaining majority (according to the Act) has the right to be informed about the personal data that has been collected of her. However as this would require the collection of data about the age of the child there needs to be added protection with respect to this data including additional safeguards to prevent the data being used for further processing and profiling. Additionally the data fiduciary should seek consent anew from the data principal on attaining majority and the data principal should have the right to withdraw from the processing if she chooses not to consent to further processing.

CHAPTER 4
Personal Data and Sensitive Personal Data of Children

16. *Processing of personal data and sensitive personal data of children.*

(1) Every data fiduciary shall process personal data of a child in such manner that 10 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 15 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 behaviouraly 25 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 35 sub-section (4).

17

COMMENTS

Under the 2018 Bill, the data principal had the right to obtain a brief summary of the personal data that had been processed or was being processed. This has now been amended to permit the data principal to access the actual personal data that has been processed. Further, it now also permits the data principal to have the right to access in one place the identities of the data fiduciaries with whom the data has been processed along with the categories of the personal data shared with them.

RECOMMENDATIONS

We appreciate the expanded right to access provided to the data fiduciary, however **we would also reiterate our previous comment.** It is also imperative that along with the right to confirmation, the data principals are also provided information justifying the ground under which the processing is being conducted. Further, we recommend the addition of sub clause (c) which states as follows: "*an explanation of how the processing is justified under one or more of the provisions under Chapters III and IV.*"

CHAPTER 5
Rights of Data Principal

17. *Right to confirmation and access.*

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

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

(b) 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.

18. *Right to correction and erasure.*

(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 updating 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 sub-section (1), such data fiduciary shall also take necessary 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, particularly where such action may have an impact on the rights and interests of the data principal or on decisions made regarding them.

19

COMMENTS

Clause 19(1) has been changed from the 2018 Bill where this right applied to all data and not only data processed through automated means.

RECOMMENDATIONS

We recommend that this right be applicable to all data and should not be limited to data processed through automated means.

19. *Right to data portability.*

(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.

20

RECOMMENDATIONS

We reiterate our previous recommendations. This Clause"s heading could be changed from "Right to be Forgotten" to "Right to Prevent Continuing Disclosures" and should include a right for the individual to request that information pertaining to them is de-indexed. The Bill also empowers an adjudicating officer for the acceptance of complaints and making the decision. The report of the data protection Bill justifies making a central adjudicating authority as the approving entity instead of the data fiduciary in order to prevent privatisation of regulation. However a singular authority to approve requests, to adjudicate over them puts a heavy burden on this authority that might not have the capacity to handle the flow of requests that will be coming in. Additionally, the authority will have to coordinate with the data fiduciary for each request making the process severely time consuming. With respect to personal data and sensitive personal data this can be crucial. The data fiduciary could be given the authority to erase the data based on the data principal's complaints, the data principal could also be accountable to an adjudicating authority including providing an account and reasoning for requesting each erasure and the reason thereof.

20. *Right to be forgotten.*

(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) 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 clause (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 of his personal data overrides the right to freedom of speech and expression and the right to information of any other citizen.

While we appreciate that the Bill has provided the data principal the right to seek erasure of personal data, **we also reiterate our previous recommendation:**

(a) There must be a **Right to restriction of processing**

The data principal shall have the right to obtain from the data fiduciary restriction of processing where one of the following applies:

(1) the accuracy of the personal data is contested by the data principal, for a period enabling the fiduciary to verify the accuracy of the personal data:

(2) the processing is unlawful and the data principal opposes the deletion of the personal data and requests the restriction of their use instead; or

(3) the fiduciary no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims.

(b) There must be a **Right to object to processing**

The data principal shall have the right to object to processing at any time being carried out under Clause 13, Clause 17 and Clause 19. Upon such objection, the fiduciary shall immediately stop processing the personal data unless they can demonstrate compelling grounds for processing for the establishment, exercise or defence of legal claims.

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

(a) the sensitivity of the personal data;

(b) the scale of disclosure and the degree of accessibility sought to be restricted 20

or prevented;

(c) the role of the data principal in public life;

(d) the relevance of the personal data to the public; and

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

(4) Where any person finds that personal data, the disclosure 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, 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.

21. *General conditions for the exercise of rights in this Chapter.*

(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.

22

COMMENTS

The provision is similar to the provision in the 2018 Bill and **we reiterate our previous comments:** the Bill should not only emphasise on privacy by design but also on privacy by default. The Bill could ideally also add these following policy measures to ensure purpose limitation and data minimisation.

1. The data fiduciary shall implement measures to ensure that only that personal is collected which is necessary for and proportional to each specific purpose of the processing.
2. The data fiduciary especially those that process sensitive personal data must practice data minimisation, and implement measures such as anonymisation.

Further, though it is welcome that the Bill requires that the privacy by design policy of each data fiduciary should be published on their website as well as the website of the Authority; this provision could be strengthened by creating a timeframe after certification by which the policy needs to be published and requiring that the policy is updated and re-certified if and when significant changes are made to the way in which personal data is handled.

23

COMMENTS

There has been a change in the wording from the 2018 Bill.[28] In the present Bill, the term "available in an easily accessible form" has been replaced with "*information available in such form and manner as may be specified by regulations.*"

RECOMMENDATIONS

The need to maintain some level of transparency by the data fiduciary is essential to allow the data principal to assert their rights provided by the Bill. Reports on the privacy policies of companies have provided how length and legalese make these essential policies inaccessible to individual users.[29] Hence we suggest that the earlier wording of the 2018 version be restored to ensure that the data principal is aware of the rights that they are entitled to.

CHAPTER 6
Transparency and Accountability Measures

22. *Privacy by design policy.*

(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) Subject to the regulations made by the Authority, the 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) 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. *Transparency in processing of personal data.*

(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;

24

COMMENTS

This clause requires data fiduciaries to develop security safeguards based on the associated risks and the likelihood and severity of harm including de-identification and encryption, steps to protect the integrity of data, and steps to prevent misuse, unauthorised access, and modification and disclosure/destruction of personal data. These practices need to be reviewed periodically in a manner specified by regulations. Though, it is welcome that the Bill includes provisions around security, given the importance of security in the digital age, there is no clear form of accountability or baseline standard for security. This could result in a vast range of security practices emerging in India and levels of enforcement and could overall weaken national cyber security.

RECOMMENDATION

We recommend that the text of the Bill require an annual review rather than a periodic review and require that the review involve an audit by an independent third party. The results of such an audit should be included in the data trust score that is assigned to a data fiduciary. We further recommend that the Bill require adherence to security standards that have been recognized and approved at the sectoral, national, or international level.

25

COMMENTS

The provision is similar to the provision specified the 2018 Bill and **we reiterate our previous comments:**

(a) The fiduciary must report the breach as soon as possible and no later than the time period specified by the Authority. It does not indicate what a reasonable time period may look like. Further, the responsibility to determine this time period is not included under 'Powers and Functions of the Authority' which have been charted out under clause 60. Note under the present Bill also the responsibility to determine the time period has not been included under the Powers and Functions of the Authority specified under Clause 49. It has also not been included under Clause 94; which provides the matters on which the Authority is empowered to make regulations.

(b) Section 32(5) states that the Authority may choose to compel the fiduciary to report the breach to the data principal depending on the severity of the breach, the harm likely to be caused to the data principal and any mitigating action the data principal may need to take. The Bill does not provide any clarification on the meanings or the thresholds envisaged by these terms and places absolute discretion on the Authority to determine whether the data principal should be made aware of a breach of his/her personal data. This is potentially problematic for two reasons. First, informing the data principal enables the individual to take context specific measures that would remedy the harms caused by the breach in his/her specific situation-something the Authority may be ill-equipped to

(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.

24. *Security safeguards.*

(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.

25. *Reporting of personal data breach.*

(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.

determine. Second, from an insurance industry perspective,if breaches are not reported, customers will not be concerned about cyber risk and therefore will be less inclined to buy insurance.

RECOMMENDATIONS

We reiterate our previous recommendations:

(a) Impose a reasonable time limit on the data fiduciary to report data breaches under clause 32(3) or empower the Authority to decide time limits under clause 60.

(b) Instead of enabling the Authority to decide when to notify the breach to the data principal, amend clause 32 (5) to make this disclosure mandatory. The Authority should be allowed to withhold this information only in the case of narrowly defined exceptions such as national security.

26 (4) and 28 (3)

COMMENTS

Clause 26 (4) empowers the Central Government in consultation with the Authority notify any social media intermediary as a significant social data fiduciary if (a) the social media intermediary has users above the threshold notified by the Central Government; and (b) the activities of the intermediary 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.**

Clause 28 (3) further states that every social media intermediary which has been notified as a significant data fiduciary shall enable the users who register their services from India, or use their services in India, to voluntarily verify their accounts.

As mentioned in the General Comments, the classification of social media intermediaries and the verification obligation are out of the scope of a data protection legislation. Additionally, the construct of social media intermediaries as significant data fiduciaries suffers from several issues:

(a) With respect to the conditions for social media intermediaries to be designated under clause 26, the numerical thresholds are to be set with respect to the number of 'users'. The term 'user' has not been defined in the Bill or elsewhere in this context, and the Bill is silent on the treatment given to non-registered users or the level of activity required to be counted as a user.

(b) The condition requiring assessment for 'significant impact on electoral democracy' is vague, which may incentivise social media intermediaries to implement overly-restrictive content moderation practices to avoid designation.

(c) The Authority, which has been tasked with notifying significant data fiduciaries in all other cases, has been relegated to a consultative role with respect to social media intermediaries. The rationale behind this differential treatment is not clear.

(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.

26. *Classification of data fiduciaries as significant data fiduciaries.*

(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:

(d) Regulation relating to voluntary verification of users is the subject matter of delegated legislation. The rules notified in this regard may dilute the 'voluntary' nature of verification, given the lack of a guiding framework in the parent Bill.

RECOMMENDATIONS

Provisions relating to social media intermediaries and the verification of the user's accounts should be deleted from the Bill.

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 on- line storage services.

27. *Data protection impact assessment.*

(1) Where the 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.

Classification of data fiduciaries as significant data fiduciaries.

(2) The Authority may, by regulations specify, such circumstances, or class of data fiduciary, 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 reason to believe that the processing is likely to cause harm to the data principals, the Authority may direct the data fiduciary to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.

28. *Maintenance of records.*

(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.

29. *Audit of policies and conduct of processing, etc.*

(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.

30. *Data protection officer.*

(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 fiduciary under 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.

31. *Processing by entities other than data fiduciaries.*

(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.

(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 confidential.

32. *Grievance redressal by data fiduciary.*

(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

32

COMMENTS

The clause is substantially similar to the provisions in the 2018 Bill. The provision while laying out the process for grievance redressal and the measures that are needed to be taken by the data fiduciary, does not lay out the mechanisms through which the grievance can be made.

RECOMMENDATIONS

We reiterate our earlier recommendations: We suggest the inclusion of a list of key mechanisms to be added to this clause and we suggest the following alternate language:*"The data principal may raise a grievance through online lodging, toll-free calling lines, e-mail, letter, fax or in person to the Data Protection Authority."*

(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, 15 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.

33

COMMENTS

This provision has changed from the 2018 Bill.[30] Instead of requiring the storage of one serving copy of personal data within India and a strict limitation on critical personal data and sensitive data, there is now no restriction on the transferring of personal data outside of India. However, sensitive personal data shall continue to be stored in India and critical personal data can only be processed in India. Though it is a welcome change that personal data can be transferred outside of India, we maintain our concerns with the government applying a 'one size fits all' data localization requirements in a data protection bill and would encourage the government to consider sectoral regulation around specific categories of data such as defense related data. We are also concerned with the creation of the undefined category of 'critical personal data' as it creates an uncertain environment for companies to operate in and could lead to enforcement and implementation issues if the category is frequently changed.

RECOMMENDATION

We recommend that this provision as well as the category of 'critical data' are removed from the Bill.

34

COMMENTS

Sensitive personal data can be transferred outside of India as per the conditions specified under this clause including if the transfer is pursuant to an approved contract or intra-group scheme or the Central Government allows such transfer. Critical personal data can be transferred outside India to an entity engaged in the provision of health services or emergency or where the Central Government has deemed the transfer permissible. This is a change from the 2018 Bill[31] which allowed for the transfer of personal data outside of India based on five conditions and only permitted the transfer of sensitive personal data outside India on two conditions while maintaining that critical personal data could only be processed in India.

RECOMMENDATION

We recommend the following with respect to this provision:

- It is assumed that the intra-group schemes referred to in this section are similar to the binding corporate rules found in the GDPR. Under the GDPR there are multiple tools for international data transfers including adequacy findings, binding corporate rules, explicit consent, standard contractual clauses, and approved codes of conduct/certification. Clause 34 appears to combine different mechanisms (consent, contract, and intra-group scheme) into one mechanism - with the only other mechanism for transfer being approval by the Central Government. The Government should create a set of multiple comprehensive mechanisms by which sensitive data can be transferred outside of India.

CHAPTER 7
Restriction on Transfer of Personal Data Outside India

33. *Prohibition on processing of sensitive personal data and critical personal data outside India*

(1) Subject to the conditions 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.

34. *Conditions for transfer of sensitive personal data and critical personal data.*

(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

- The Authority should be the sole entity responsible for assessing and approving such mechanisms.
- Personal data should be brought back into the scope of this provision as the current framing excludes personal data and thus would mean that it can be transferred outside of India without assurance that it is being processed inline with the requirements found in the Bill.
- The provision should clarify at a more granular level how each transfer mechanism will work and what criteria must be met for approval. For example, it is currently unclear if the provision will require each transfer to be approved by the government/authority or if the government/authority will approve an intra-group scheme - after which companies can transfer data freely.

(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.

Recommendation

Under the 2018 Bill, exemptions were provided to the data fiduciary from the various provisions of the Bill in cases of processing of (i) personal data required for the security of the State, (ii) Prevention, investigation, prosecution and contravention of law, (iii) Processing for the purpose of legal proceedings, (iv) Research, archiving or statistical purposes, (v) personal and domestic purposes, and (vi) Manual Processing by small entities. However, any data fiduciary processing personal data for such specified purposes was still required to comply with the provision of fair and reasonable processing. Under the present Bill, similar grounds have been provided for exemptions from the various provisions of the Bill, but unlike the 2018 Bill, under the present Bill, the exemptions from the applicability of the provisions of the Bill has been expanded to include exemption from fair and reasonable processing of personal data.

In addition, **we also reiterate our earlier comments:**

(a) The standard of necessary and proportionate for the security of state, or prevention, detection, investigation and prosecution of contraventions of law is too vague. While it may not be possible to exhaustively define what constitutes as necessary and proportionate, it would be extremely useful to include explanations which provide guidance about how these legal tests ought to be construed.

(b) In its current formulation, there is no obligation and clear procedure for the agencies involved to establish necessity and proportionality before a judicial or quasi-judicial body. We recommend that a commission be set up by the Authority to examine all requests for processing under Clause 42 and 43 and be subject to their determination.

(c) We recommend that duration limitation, that is, data will only be retained for a given period and destroyed after that, be specified under Clause 42 and 43;

(d) Exemption under Clauses 42 and 43 need not be as sweeping as they have been drafted currently. Requirements such as reporting personal data breaches to the Authority and data audits should continue to apply;

(e) We also recommend that user notifications rights be made available under both Clause 42 and 43. Such notification maybe withheld as long as it cannot be ruled out that informing the data subject might jeopardise the purpose of the processing or as long as any general disadvantages to the interest of purposes under Clause 42 and 43.

(f) Similarly, a limited right to confirmation, access and rectification must be made available to data principals where their personal data is being processed under Clause 42 and 43. These rights maybe limited to the extent such conformation,access and rectification jeopardises the purpose of processing.

35

COMMENTS

Under the 2018 Bill,[32] the exemption was granted for the security of the State, subject to such processing of personal data being (i) authorised by law; (ii) in accordance

CHAPTER 8
Exemptions

35. *Power of Central Government to exempt any agency of Government from application of Act.*

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.

with the procedure laid down by the law; (iii) necessary; and (iv) proportionate to the interests being achieved. This four stage process embed the principles laid down by the Supreme Court in Puttaswamy I. This was regarded as a first step towards determining the surveillance powers of the State, even though the other recommendation of the Srikrishna Committee regarding an ex-ante judicial approval of the process was not included in the Bill.

However, under the present Bill, this four stage process has been done away with. The provision now merely provides that the Central Government if it is satisfied that it is **necessary or expedient** to do so may by a written order exempt any agency of the Government from the application of all or any of the provisions of this Bill in respect of the processing of such personal data **subject to such procedure, safeguards and oversight mechanism as may be prescribed.** Further, the grounds for such an exemption has been expanded to include processing for the sovereignty and integrity of India, security of the State, friendly relations and public order. These are the restrictions on freedom of speech and expression provided under Article 19(2) of the Indian Constitution which have now been provided as a measure to exempt protection of personal data.

The present Bill grants a blanket exemption from all the provisions of the Bill to an agency of the Central Government- it is not specific to a particular function or specific purpose of the particular agency. Unlike, the 2018 Bill,[33] where the exemptions were granted from certain specific provisions, under the current Bill, power has been granted to exempt the agency from any or all the provisions of the Bill, thereby exempting it from the obligations specified under Chapter XIII (offences), Chapter X (Penalties and Compensation), Chapter IX (Data Protection Authority of India).

By doing away with the four pronged test, these provisions are not in consonance with test laid down by the Supreme Court in and are also incompatible with an effective privacy regulation. There is also no provision for either a prior judicial review of the order by a district judge as envisaged by the Justice Srikrishna Committee Report or post facto review by an oversight committee of the order as laid down under the Indian Telegraph Rules, 1951[34] and the rules framed under Information Technology Act.[35] The provision states that such processing of personal data shall be subject to the procedure, safeguard and oversight mechanisms that may be prescribed. However, there is no corresponding provision under Clause 93, which grants powers to the Central Government to make rules on specified grounds.

RECOMMENDATIONS

In addition to the recommendations made under the General comments, we recommend the following:

(a) The exemption should be subject to the four stage test specified under the 2018 Bill. i.e. (i) authorised by law; (ii) in accordance with procedure established by such law; (iii) necessity; and (iv) proportionate.

(b) The procedure and the safeguards should be provided for in the parent Bill and not be delegated to the rules to be framed by the Central Government.

(c) The exemptions should not be as sweeping as have been provided for currently. There is no need for exemptions from the Chapter XIII (Offences), Chapter IX (Data Protection Authority of India), security safeguard measures.

36. *Exemption of certain provisions for certain processing of personal data.*

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.

37. *Power of Central Government to exempt certain data processors.*

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 15 of data processors incorporated under Indian law.

(d) Requirements such as reporting personal data breaches to the Authority and data audits should continue to apply.

(e) Prior judicial review of the written order exempting the agency of the Central Government from the provisions of this Bill.

36

COMMENTS

Clause 36 (a) provides for exemptions of certain provisions where the 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. Under the 2018 Bill,[36] a condition precedent for this clause to come into effect was (a) a law made by Parliament or State Legislature authorising such exemptions and (b) it was necessary for and proportionate to the interests sought to be achieved. These requirements have been deleted from this Bill.

Further, under the 2018 Bill[37] such exemptions in relation to the processing of personal data would apply to a victim, witness or any person with information about the offence/contravention of law. This provision/requirement has also been deleted from this Bill. The 2018 Bill also stated that the personal data so processed shall not be retained once the purpose for which it was processed is competed.[38] This provision has also been deleted from this present Bill.

As per the current provision, personal data could be processed for the prevention, detection, prosecution of any offence. The term 'offence' has not been defined and therefore even a breach of a contractual provision could constitute an offence for the purposes of this provision.

RECOMMENDATIONS

In addition to the recommendations made under the General comments, we recommend the following:

(a) The personal data so processed should be deleted once the purpose for which it was processed under this clause has been completed.

(b) Re-introduction of provisions in the 2018 Bill specifying the persons to whom this provision would be applicable.

(c) Determining the scope of the term 'offence' to include only cognizable offences as defined under the Code of Criminal Procedure, 1973.

38

COMMENTS

Under the 2018 Bill,[39] the Authority could exempt a data fiduciary from the application of any provisions of the Bill in cases where the personal data is processed for research, archiving or statistical purposes. However, provisions regarding 'fair and reasonable processing', 'security safeguards' and 'data protection

38. *Exemption for research, archiving or statistical purposes.*

Where the processing of personal data is necessary for research, archiving, or statistical purposes, and the Authority is satisfied that—

(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. *Exemption for manual processing by small entities.*

(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 35 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.

impact assessment' still had to be complied with. Under the 2019 Bill, the requirement for compliance with these provisions has been deleted.

RECOMMENDATIONS

The exemptions should be narrowed down and the provisions specified in the 2018 Bill should be reinstated.

40

COMMENTS

The Authority for the purpose of encouraging innovation in artificial intelligence, machine learning or any other emerging technology in public interest, will create a sandbox.

Any data fiduciary whose privacy by design policy is certified by the Authority can apply. The sandbox will involve relaxing requirements that obligate specification of purpose, limitation of personal data, restrictions on retention of personal data, and requirements for the processing of data in a fair and reasonable manner with consent. As mentioned in the General Comments, data sandboxes have been envisioned as a secure area where only a copy of the company's or participant companies' data is located.[40] In essence, it refers to the scalable and creation platform which can be used to explore an enterprise's information sets. On the other hand, regulatory sandboxes are controlled environments where firms can introduce innovations to a limited customer base within a relaxed regulatory framework, after which they may be allowed entry into the larger market after meeting certain conditions.

Sandboxes are regulatory tools which may be used to permit companies to innovate in the absence of heavy regulatory burdens. However, these ordinarily refer to burdens related to high barriers to entry (such as capital requirements for financial and banking companies), or regulatory costs. In this Bill, however, the relaxing of data protection provisions for data fiduciaries would lead to restrictions of the privacy of individuals. Limitations to fundamental rights on grounds of 'fostering innovation' is not a constitutional tenable position, and contradict the primary objectives of a data protection law.

40. *Sandbox for encouraging innovation, etc.*

(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.

42 (2)

COMMENTS

The composition of the members of the Selection Committee for the selection of members to the Authority has been drastically changed from the 2018 Bill leading to a potential significant reduction in the independence of the Authority. As per the 2018 Bill,[41] the Selection Committee consisted of 3 members (i.e, the Chief Justice of India, the Cabinet Secretary and one expert of repute.) However, the present Bill has removed the judicial member and the expert from the composition of the Selection Committee and it now comprises entirely of members from the Executive.

RECOMMENDATIONS

An independent Authority is the basis for a strong and robust data protection regime in the country, and it is therefore essential that the Selection Committee responsible for appointing the Authority is also perceived to be independent and neutral. We recommend that the composition of the Selection Committee be resorted to the composition under the 2018 Bill. Additionally, **we also reiterate our previous comments:** one eminent person representing the private sector and one eminent person representing the civil society are also made members of the committee.

43

COMMENTS

The 2018 Bill[42] explicitly stated that the salaries, allowances and other terms and conditions of service of the chairperson and other members of the Authority would not be varied to their disadvantage during their term. This provision has been deleted from the current Bill.

CHAPTER 9
Data Protection Authority of India

41. *Establishment of Authority.*

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

(2) The Authority 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.

42. *Composition and qualifications for appointment of Members.*

(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.

43. *Terms and conditions of appointment.*

(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.

For an efficient and smooth functioning of the Authority, it is necessary that the members of the Authority are able to function in an independent manner and are insulated from government control. By deleting the provision which prevented the government from varying the salaries and terms and conditions of appointment, the Central Government now has the power to reduce the salary or amend the terms of appointment to the detriment of the members of the Authority, thereby giving it effective control over the functioning of the Authority.

RECOMMENDATIONS

The 2018 provision should be reinstated and it should be clearly specified that the terms of appointments, salaries and allowances of the chairperson and members will not be varied to their disadvantage during the term of their appointment.

44

COMMENTS

The Central Government has been conferred the powers to remove from office the chairperson and or other members of the Authority on the basis of the grounds specified in the Bill. Considering that the Authority is required to exercise power over the Central Government as well as the State Government in exercise of their role as a data fiduciary, it is necessary to ensure that the power of removal does not solely vest with the Central Government.

RECOMMENDATIONS

We reiterate our earlier recommendation: A committee similar to the one constituted for appointment of members must also be constituted to address any issues of removal of members.

(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. *Removal of Chairperson or other Members.*

(1) The Central Government may remove from office, the Chairperson or any Member of the Authority who—

(a) has been adjudged as an insolvent;

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

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

(d) has so abused their position as to render their continuation in office 35 detrimental to the public interest; or

(e) has acquired such financial or other interest as is likely to affect prejudicially their 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 reasonable opportunity of being heard.

45. *Powers of Chairperson.*

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.

46. *Meetings of Authority.*

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

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

49

COMMENTS

Unlike the 2018 Bill,[43] under the present Bill, the power of the Authority to specify the residuary categories of sensitive personal data has been removed. This power has now been conferred upon the Central Government in consultation with the sectoral regulators and the Authority.[44]

Further, the present Bill has reduced the powers and functions of the Authority from the powers specified under the 2018 Bill. Under the 2018 Bill, the functions of the Authority included (i) issuing guidance on provisions under the Bill either on its own or in response to a query from a data fiduciary; (ii) preparation and publication of reports setting out the result of any inspection or inquiry in public interest; and (iii) advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data. These functions of the Authority have been deleted from the present Bill. The rationale for deleting these functions is unclear.

RECOMMENDATIONS

We recommend that the provision as per the 2018 Bill should be reinstated and the Authority in consultation with the sectoral regulators should be empowered to determine further categories of personal data. Further, the deleted functions of the Authority should be reinstated and it should be required to publish the results of the inquiry which it deems to be in public interest. This is useful for[45] (a) data principals to identify how different data fiduciaries are approaching data protection; (b) the Authority to rectify if needed its rules and regulations; and (c) afford more trust and transparency to the Authority.

(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 member 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.

47. *Vacancies, etc., not to invalidate proceedings of Authority.*

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

(a) any vacancy or defect in the constitution of the Authority;

(b) any defect in the appointment of a person as a Chairperson or member; or

(c) any irregularity in the procedure of the Authority not affecting the merits of the case.

48. *Officers and other employees of Authority.*

(1) The Authority may appoint such officers, other employees, consultants and experts as it may consider necessary for effectively discharging of 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.

49. *Powers and functions of Authority.*

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

50. *Codes of practice.*

(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 an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory Authority, or any departments or ministries of the Central or State Government.

(3) The Authority shall ensure transparency 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 Act or 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;

50

COMMENTS

Under the 2018 Bill,[46] the Authority had the power to issue a code of practice regarding the mechanism for processing personal data of users who are incapable of providing valid consent. This power of the Authority has been removed from the present Bill. The rationale for the deletion of the power is unclear.

RECOMMENDATIONS

The power to issue a code of practice to develop an appropriate mechanism for processing of personal data of users who are incapable of providing valid consent should be reinstated. In addition, **we reiterate our previous comment:** The following categories of bodies be included in this provision as bodies who may submit codes of practices: academic and research organisation, particularly those working on issues of privacy, security and encryption; civil society bodies which are engaged in research or building awareness on privacy and data protection issues.

(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 personal 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 the view of the Authority, may be necessary 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.

52. *Power of Authority to issue directions.*

(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.

(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.

53. *Power of Authority to conduct inquiry.*

(1) he 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 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 Inquiry Officer.

(7) The Inquiry Officer may keep in its custody any books, registers, documents, records and other data produced under sub-section (5) for six months and thereafter shall return the same to the person by whom or on whose behalf such books, registers, documents, record and data are produced, unless an approval to retain such books, registers, documents, record and data for an additional period not exceeding three months has been obtained from the Authority.

(8) 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 and other documents, at such place and at such time as may be specified;

(b) summoning and enforcing the attendance of persons and examining them on oath;

(c) inspection of any book, document, register or record of any data fiduciary;

(d) issuing commissions for the examination of witnesses or documents; and

(e) any other matter which may be prescribed.

54. *Action to be taken by Authority pursuant to an inquiry.*

(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—

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

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

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

(d) require the data 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 flow of personal data; or

(h) require the data fiduciary or data processor to take any such action in respect of any matter arising out of the report as the Authority may deems fit.

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

55. *Search and seizure.*

(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.

55

COMMENTS

Clause 55(4) provides that the Inquiry Officer can keep in its custody the seized material for a period not later than the conclusion of the inquiry. Under the 2018 Bill,[47] the seized material could only be retained for six months (unless the Authority approved the retention for a longer period). Further, under the 2018 Bill,[48] the person from whom the material had been seized could make copies of such material. This provision has been deleted under the present Bill.

RECOMMENDATIONS

A time period should be specified beyond which the seized materials cannot be kept in the custody of the Inquiry Officer. The provision in the 2018 Bill should be reinstated. In addition, the right of person to make copies of the seized material should also be reinstated into the present Bill.

(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.

56. *Co-ordination between Authority and other regulators or authorities.*

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

CHAPTER 10
Penalties and Compensation

57. *Penalties for contravening certain provisions of the Act.*

(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 5 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 recognised in the profit and loss account or any other equivalent statement,

as applicable, from the sale, supply or distribution of goods or services or on account

of services rendered, or both, and where such revenue is generated within India and outside India.

(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.

58. *Penalty for failure to comply with data principal requests under Chapter V.*

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.

59. *Penalty for failure to furnish report, returns, information, etc.*

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 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.

60. *Penalty for failure to comply with direction or order issued by Authority.*

If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 51 or order issued by the Authority under section 54, such data fiduciary 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.

61. *Penalty for contravention where no separate penalty has been provided.*

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.

62. *Appointment of Adjudicating Officer.*

(1) For the purpose of adjudging the penalties under sections 57 to 61or awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed.

(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) number of Adjudicating Officers to be appointed under sub-section (1);

62

COMMENTS

Clause 62(2) provides that the Central Government shall be responsible for prescribing the number of adjudicating officers to be appointed, the manner and term of their appointment and the jurisdiction of such officers.

RECOMMENDATIONS

We reiterate our previous comment: Such powers should vest with the Authority instead of the Central Government.

(b) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;

(c) jurisdiction of Adjudicating Officers;

(d) other such requirements as the Central Government may deem fit.

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

63. *Procedure for adjudication by Adjudicating Officer.*

(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 reasonable opportunity of being heard:

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 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 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; and

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

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

64. *Compensation.*

(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 expressly applicable to it.

(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.

(3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any contravention by the same data fiduciary

or data processor, one complaint may be instituted on behalf of all such data principals seeking compensation for the harm suffered.

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

(a) nature, duration and extent of violation of the provisions of the Act, rules prescribed, or regulations specified thereunder;

(b) nature and extent of harm suffered by the data principal;

(c) intentional or negligent character of the violation;

(d) transparency and accountability measures implemented by the data fiduciary or the data processor, as the case may be, including adherence to any relevant code of practice relating to security safeguards;

(e) action taken by the data fiduciary or the data processor, as the case may be, to mitigate the damage suffered by the data principal;

(f) previous history of any, or such, violation by the data fiduciary or the data processor, as the case may be;

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

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

(5) Where more than one data fiduciary or data processor, or both a data fiduciary and a data processor are involved in the same processing activity and are found to have caused harm to the data principal, 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.

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

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

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

65. *Compensation or penalties not to interfere with other punishment.*

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

66. *Recovery of amounts.*

(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.

(2) All sums realised by way of penalties under this Act shall be credited to the Consolidated Fund of India.

CHAPTER 11
Appellate Tribunal

67. *Establishment of Appellate Tribunal.*

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

(a) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (5) of section 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 63; and

(d) hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 64.

(2) The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed.

(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 body is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such body to act as the Appellate Tribunal under this Act.

68. *Qualifications, appointment, term, conditions of service of Members.*

(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.

69. *Vacancies.*

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

70. *Staff of Appellate Tribunal.*

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

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

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

71. *Distribution of business amongst Benches.*

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

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

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

72. *Appeals to Appellate Tribunal.*

(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 to in 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.

73. *Procedure and powers of Appellate Tribunal.*

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

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

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

(b) requiring the discovery and production of documents;

(c) receiving evidence on affidavits;

(d) subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872, requisitioning any public record or document or a copy of such record or document, from any office;

(e) issuing commissions for the examination of witnesses or documents;

(f) reviewing its decisions;

(g) dismissing an application for default or deciding it, ex parte;

(h) setting aside any order of dismissal of any application for default or any order passed by it, ex parte; and

(i) any other matter which may be prescribed.

(3) Every proceeding before the Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of sections 193 and 228, and for the purposes of section 196 of the Indian Penal Code 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.

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

(1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of civil court, and for this purpose, the Appellate Tribunal shall have all the powers of a civil court.

(2) Notwithstanding anything contained in sub-section (1), the Appellate Tribunal may transmit any order made by it to a civil court having local jurisdiction and such civil court shall execute the order as if it were a decree made by that court.

75. *Appeal to Supreme Court.*

(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.

76. *Right to legal representation.*

The applicant or appellant may either appear in person or authorise one or more legal practitioners or any of its officers to present 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.

77. *Civil court not to have jurisdiction.*

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

CHAPTER 12
Finance, Accounts and Audit

78. *Grants by Central Government.*

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

79. *Data Protection Authority of India Funds.*

(1) There shall be constituted a Fund to be called the Data Protection Authority Fund to which the following shall be credited—

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

(b) all sums received by the Authority from such other source as may be decided upon by the Central Government.

(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.

80. *Accounts and Audit.*

(1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed in consultation with the Comptroller and Auditor-General of India.

(2) The accounts of the Authority shall be audited by the Comptroller and Auditor-General of India at such intervals as may be prescribed and any expenditure incurred by 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 the Comptroller and Auditor-General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.

81. *Furnishing of returns, etc., to Central Government.*

(1) he 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.

82

COMMENTS

Clause 82(1) restricts the offences to re-identification and re-identification and processing of personal data. The offences relating to intentionally or recklessly obtaining, transferring or selling either personal or sensitive personal data has been deleted.

RECOMMENDATIONS

We reiterate our earlier recommendations: This clause could specify that whenever the personal data of a data principal was re-identified or de-identified the authority conducting such process must notify the data principal of such processing. Secondly we suggest the addition of another subsection to provide exemptions for research. We suggest the following language for the proposed subsection 3:*"Notwithstanding anything contained subsection (1) and (2) research undertaken for a re-identification and de-identification after notification of authority shall be exempt from the above provision. Provided that the researchers do not disclose or share any re-identified or de-identified data without consent of the data principals."*

83

COMMENTS

Clause 83(2) provides that no court shall take cognizance of any offence under this Bill, save on a complaint made by the Authority. The 2018 Bill[49] had no such provision; it merely provided that the offences shall be cognizable and non-bailable. The rationale for the inclusion of such a provision is unclear. Prior to the 2019 amendment to the Aadhar Act, the courts could take cognizance of a complaint, only if the Unique Identification Authority of India filed a complaint. The 2019 amendment changed this and has now permitted concerned individuals to file a complaint with the court directly. It is pertinent to note that this was pursuant to the 2018 Supreme Court judgement in Puttaswamy II,[50] in which the Supreme Court had held that it would be appropriate if the Aadhar Act was amended and the concerned individual whose right is violated is permitted to file a complaint and initiate proceedings.

RECOMMENDATIONS

We recommend that this provision should be deleted. The power to file a complaint under the Bill should not be restricted to the Authority; the concerned person should also have the power to file a complaint directly without having to first approach the Authority.

CHAPTER 13
Offences

82. *Re-identification and processing of de- identified personal data.*

(1) Any person who, knowingly or intentionally—

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

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

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

83. *Offences to be cognizable and non- bailable.*

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

(2) No court shall take cognizance of any offence under this Act, save on a complaint made by the Authority.

84. *Offences by companies.*

(1) Where an offence under this Act has been committed by a company, every

person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

(2) Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if 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 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.

85

COMMENT

Clause 85 of the present Bill is different from the 2018 Bill such that it requires the offence to be "proved" in order to be held guilty under the Act. Under the 2018 Bill,[51] the provision came into force when an offence was committed.

The new requirement to "prove the offence" is ambiguous and unclear.

85. *Offences by State.*

(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.

86

COMMENT

Clause 86 gives the Central Government the power to issue directions to the Authority as necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order. Though the Authority has the ability to express views on any direction, the decision of the Central Government - whether policy or not will be final and binding. In effect this provision severely undermines the strength and powers of the Authority. Given that the binding directions will pertain to security of the State etc. - the provision opens up the scope of exceptions defined in clause 35 and the already limited safeguards to the same - to potential revision. This could have serious implications for human rights.

RECOMMENDATION

We recommend that this provision is deleted.

CHAPTER 14
Miscellaneous

86. *Power of Central Government to issue directions.*

(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.

87. *Members, etc., to be public servants.*

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

88. *Protection of action taken in good faith.*

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

89. *Exemption from tax on income.*

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.

90. *Delegation.*

The Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act, except the powers under section 94, as it may deem necessary.

92

COMMENTS

The clause prohibits data fiduciaries from processing such biometric as may be notified by the Central Government, unless such processing is permitted by law. It is unclear as to why such a bar has only been placed on processing of biometric data and not on processing of other forms of genetic and sensitive personal data.

RECOMMENDATIONS

We recommend that this provision be revised to lay out the circumstances under which the Central government may place a bar on any form of sensitive personal data and also specify the principles to guide the same.

93

RECOMMENDATION

This clause defines 25 instances in which the Central Government has the power to make rules to carry out the provisions of the Bili. Of these, we would recommend the deletion of:

(a) the methods of voluntary identification to identify users of social media under sub-clause (3) and the identifying mark of verification of a voluntarily verified user under sub-clause (4) of clause 28;

(b) the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-clause (1) of clause 34;

We suggest shifting the following to the Authority:

(a) any other categories of sensitive personal data under clause 15;

(b) other factors to be taken into consideration under clause (d) of sub-clause (3) of clause 16.

91. ***Act to promote framing of policies for digital economy, etc..***

(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.

92. ***Bar on processing certain forms of biometric data.***

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

93. ***Power to make rules.***

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

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

(a) any other categories of sensitive personal data under section 15;

(b) other factors to be taken into consideration under clause (d) of sub-section (3) of section 16;

(c) 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;

(d) the methods of voluntary identification to identify users of social media under sub-section (3) and the identifying mark of verification of a voluntarily verified user under sub-section (4) of section 28;

(e) the manner in which a complaint may be filed under sub-section (4) of section 32;

(f) the entity or class of entity in a country, or international organisations to which transfers may be permitted under clause (b) of sub-section (1) of section 34;

(g) the place of head office of the Authority under sub-section (3) of section 41;

(h) procedure to be followed by the selection committee under sub-section (3) of section 42;

(i) the salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority under sub-section (2) of section 43;

(j) the time and place for, and the rules and procedures in regard to, transaction of business at the meetings of the Authority under sub-section (1) of section 46;

(k) other functions of the Authority under clause (o) of sub-section (2) of section 49;

(l) 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;

(m) other matters under clause (e) of sub-section (8) of section 53, in respect of which the Authority shall have powers;

(n) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (2) of section 62;

(o) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (1) of section 63;

(p) the form and manner of making a complaint under sub-section (2), and the 10 procedure for hearing of a complaint under sub-section (8) of section 64;

(q) 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 68;

(r) the procedure of filling of vacancies in the Appellate Tribunal under section 69;

(s) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 70;

(t) the form, manner and fee for filing an appeal or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 72;

(u) other matters under clause (i) of sub-section (2) of section 73 in respect of 20 powers of the Appellate Tribunal;

(v) 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 80;

(w) the time in which and the form and manner in which the returns, statements, 25 and particulars are to be furnished to the Central Government under sub-section (1), and annual report under sub-section (2) of section 81;

(x) 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 91; or

(y) any other matter which is require to be, or may be, prescribed, or in respect of which provision is to be made, by rules.

94. *Power to make regulations.*

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

(2) In particular and without prejudice to the generality of the foregoing power, such 35 regulations may provide for all or any of the following matters, namely:—

(a) information required to be provided by the data fiduciary to the data principal in its notice under clause (n) of sub-section (1) of section 7;

(b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section 9;

(c) 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 under sub-section (2), the manner of verification of age of a child under sub-section (3), application of provision in modified form to data fiduciaries offering counselling or child protection services under sub-section (6) of section 16;

(f) 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;

(g) the manner for submission of privacy by design policy under sub-section (2) of section 22;

(h) the manner and the technical, operation, financial and other conditions for registration of the consent manager and its compliance under sub-section (5) of section 23;

(i) the manner of registration of significant data fiduciaries under sub-section (2) of section 26;

(j) the circumstances or classes of data fiduciaries or processing operations where data protection impact assessments shall be mandatory and instances where data auditor shall be appointed under sub-section (2), and 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;

(k) 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;

(l) 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); the manner of registration of auditors under sub-section (4); 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;

(m) the qualification and experience of a data protection officer under sub-section (1) of section 30;

(n) the period within which transfer of personal data shall be notified to the Authority under sub-section (3) of section 34;

(o) the provisions of the Act and the class of research, archival or statistical purposes which may be exempted under section 38;

(p) he 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;

(q) the code of practice under sub-section (1) of section 50;

(r) the form and manner for providing information to the Authority by the data fiduciary under sub-section (3) of section 52;

(s) 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.

95. *Rules and regulations to be laid before Parliament.*

Every rule and regulation made under this Act and notification issued under sub-section (4) of section 67 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.

96. *Overriding effect of this Act.*

Save as otherwise provided in this Act, the provisions of this Act shall have effect notwithstanding anything inconsistent therewith any other law for the time being in force or any instrument having effect by virtue of any law other than this Act.

97. *Power to remove difficulties.*

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

Provided that no such order shall be made under this section after the expiry of five years from the 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.

98. *Amendment of Act 21 of 2000.*

The Information Technology Act, 2000 shall be amended in the manner specified in the Schedule to this Act.

Endnotes

General Comments

1 (2017) 10 SCC 641 ("Puttaswamy I").

2 Clause 42(1) of the 2018 Bill states that "*Processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to such interests being achieved.*"

3 (2019) 1 SCC 1 ("Puttaswamy II")

4 *Puttaswamy I*, *supra*, para 180.

5 (1978) 1 SCC 248.

6 *Ibid* para 48.

7 Puttaswamy I *supra* para 180.

8 *State of W.B. v. Anwar Ali Sarkar*, 1952 SCR 284; *Satwant Singh Sawhney v A.P.O AIR* 1967 SC1836.

9 (2016)7 SCC 353.

10 Dvara Research "Initial Comments of Dvara Research dated 16 January 2020 on the Personal Data Protection Bill, 2019 introduced in Lok Sabha on 11 December 2019", January 2020, *https://www.dvara.com/blog/2020/01/17/our-initial-comments-on-the-personal-data-protection-bill-2019/* ("Dvara Research").

11 "A Data Sandbox for Your Company", Terrific Data, last accessed on January 31, 2019, *http://terrificdata.com/2016/12/02/3221/.*

12 *https://www.rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=48550*

13 *https://main.trai.gov.in/notifications/press-release/trai-releases-telecom-commercial-communication-customer-preference*

14 Clause 3(20) — "harm" includes (i) bodily or mental injury; (ii) loss, distortion or theft of identity; (ii) 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 service,benefit or good resulting from an evaluative decision about the data principal; (ix) any restriction placed or suffered directly or indirectly on speech, movement or any other action arising out of a fear of being observed or surveilled; or (x) any observation or surveillance that is not reasonably expected by the data principal.

15 Clause 3(38): "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."

16 Alex Hern "Anonymised data can never be totally anonymous, says study", July 23, 2019 *https://www.theguardian.com/technology/2019/jul/23/anonymised-data-never-be-anonymous-enough-study-finds*.

17 Clause 97 of the 2018 Bill states*"(1) For the purposes of this Chapter, the term 'notified date' refers to the date notified by the Central Government under sub-section (3) of section 1. (2)The notified date shall be any date within twelve months from the date of enactment of this Act. (3)The following provisions shall come into force on the notified date-(a) Chapter X; (b) Section 107; and (c) Section 108. (4)The Central Government shall, no later than three months from the notified date establish the Authority. (5)The Authority shall, no later than twelve months from the notified date notify the grounds of processing of personal data in respect of the activities listed in sub-section (2) of section 17. (6)The Authority shall no, later than twelve months from the date notified date issue codes of practice on the following matters-(a) notice under section 8; (b) data quality under section 9; (c) storage limitation under section 10; (d) processing of personal data under Chapter III; (e) processing of sensitive personal data under Chapter IV; (f) security safeguards under section 31; (g) research purposes under section 45; (h) exercise of data principal rights under Chapter VI; (i) methods of de-identification and anonymisation; (j) transparency and accountability measures under Chapter VII. (7)Section 40 shall come into force on such date as is notified by the Central Government for the purpose of that section.(8)The remaining provision of the Act shall come into force eighteen months from the notified date."*

Section-wise Comments and Recommendations

18 Section 79 (1) of the Information Technology Act states *"Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-section (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hosted by him."*

19 Sonia Livingstone *et al*, "One in Three: Internet Governance and Children's Rights", *Global Commission on Internet Governance Paper Series No. 22* (November 2015) *https://www.cigionline.org/sites/default/files/no22_2.pdf*

20 UNICEF, "State of the World's Children-Children in a Digital World", (2017) https://*www.unicef.org/publications/index_101992.html*

21 White Paper of the Committee of Experts on a Data Protection Framework for India (2017) (SrikrihnaReport) *https://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf*

22 Clause 4 of the 2018 Bill states *"Any person processing personal data owes a duty to the data principal to process such personal data in a fair and reasonable manner that respects the privacy of the data principal."*

23 Clause 11(3) of the 2018 Bill states *"sub-section (1) shall not apply where the provision of notice under this section would substantially prejudice the purpose of processing of personal data under Section 15 or 21 of this Act"*

24 Clause 21 of the 2018 Bill states *"Passwords, financial data, health data, official identifiers, genetic data and biometric data may be processed where such processing is strictly necessary-(a) to respond to any medical emergency involving a threat to life to the life or a severe threat to the health of the data principal;(b) to undertake any measure to provide medical treatment or health services to any individual during an epidemic, outbreak of disease or any other threat to public health;(c) to undertake any measure to ensure safety of, or provide assistance or services to, any individual during any disaster or any breakdown of public order."*

25 Clause 19 of the 2018 Bill states *"Sensitive personal data may be processed if such processing is strictly necessary for (a) any function of Parliament or any State Legislature. (b) the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal."*

26 Clause 22 (1) of the 2018 Bill states *"Such further categories of personal data as may be specified by the Authority shall be sensitive personal data and, where such categories of personal data have been specified the Authority may also specify any further grounds on which such specified categories of personal data may be processed."*

27 Insertion of Section 3A to the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 by virtue of Aadhaar and other Laws Amendment Act, 2019.

28 Clause 30(1) of the 2018 Bill states that *"The data fiduciary shall take reasonable steps to maintain transparency regarding its general practices related to processing personal data and shall make the following information available in an easily accessible form as may be specified."*

29 Rishabh Bailey et al "Disclosures in privacy policies: Does "notice and consent work? ", NIPFP Working paper series (2018), *https://www.nipfp.org.in/media/medialibrary/2018/12/WP_246.pdf*,
Aayush Rathi and Shweta Mohandas, "FinTech in India, A study of privacy and security commitments", (April 2019), *https://cis-india.org/internet-governance/files/Hewlett%20A%20study%20of%20FinTech%20companies%20and%20their%20privacy%20policies.pdf/view*

30 Clause 40 of the 2018 Bill states *"(1) Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.(2) The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or a data center located in India. (3) Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section(1) on the grounds of necessity or strategic interests of the State. (4) Nothing contained in sub-section (3) shall apply to sensitive personal data."*

31 Clause 41(3) of the 2018 Bill states *"Notwithstanding sub-section (2) of Section 40, sensitive personal data notified by the Central Government may be transferred outside the territory of India-(a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and (b) to a particular country, a prescribed sector within a country or to a particular international organisation that has been prescribed under clause (b) of sub-section (1), where the Central Government is satisfied that such transfer or class of transfer is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of this Act."*

32 Clause 42 (1) of the 2018 Bill states *"Processing of personal data in the interests of the security of the State shall not be permitted unless it is authorised pursuant to a law, and is in accordance with the procedure established by such law, made by Parliament and is necessary for, and proportionate to, such interests being achieved."*

33 Clause 42 (2) of the 2018 Bill states *"Any processing authorised by a law referred to in sub-section (1) shall be exempted from the following provisions of the Act- (a) Chapter II, except section 4; (b) Chapter III; (c) Chapter IV; (d) Chapter V; (e) Chapter VI; (f) Chapter VII, except section 31; and (g) Chapter VIII."*

34 Rule 419A (16): The Central Government or the State Government shall constitute a Review Committee.
Rule 419 A(17): The Review Committee shall meet at least once in two months and record its findings whether the directions issued under sub-rule (1) are in accordance with the provisions of sub-section (2) of Section 5 of the said Act. When the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above it may set aside the directions and orders for destruction of the copies of the intercepted message or class of messages.

35 Rule 22 of Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009: The Review Committee shall meet at least once in two months and record its findings whether the directions issued under rule 3 are in accordance with the provisions of sub-section (2) of section 69 of the Act and where the Review Committee is of the opinion that the directions are not in accordance with the provisions referred to above, it may set aside the directions and issue an order for destruction of the copies, including corresponding electronic record of the intercepted or monitored or decrypted information.

36 Clause 43 (1) of the 2018 Bill states *"Processing of personal data in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of law shall not be permitted unless it is authorised by a law made by Parliament and State Legislature is necessary for, and proportionate to, such interests being achieved."*

37 Clause 43 (3) of the 2018 Bill states *"Sub-section (1) shall apply in relation to the processing of personal data of a data principal who is a victim, witness, or any person with information about the relevant offence or contravention only if processing in compliance with the provisions of this law would be prejudicial to the prevention, detection, investigation or prosecution of any offence or other contravention of law."*

38 Clause 43 (4) of the 2018 Bill states *"Personal data processed under sub-section (1) shall not be retained once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete except where such personal data is necessary for the maintenance of any record or database which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence or class of offences in future."*

39 Clause 45(1) of the 2018 Bill states *"Where processing of personal data is necessary for research, archiving, or statistical purposes, such processing may be exempted from such provisions of this Act as the Authority may specify except section 4, section 31 and section 33."*

40 "A Data Sandbox for Your Company", Terrific Data, last accessed on January 31, 2019, *http://terrificdata.com/2016/12/02/3221/*

41 Clause 50 (2) of the 2018 Bill states *"The chairperson and the members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of- (a) the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, who shall be the chairperson of the selection committee; (b) the Cabinet Secretary; and (c) one expert of repute as mentioned in sub-section (6), to be nominated by the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India, in consultation with the Cabinet Secretary."*

42 Clause 51 (2) of the 2018 Bill states *"The salaries and allowances payable to, and other terms and conditions of service of the chairperson and the members shall be such as may be prescribed and shall not be varied to their disadvantage during their term."*

43 Clause 22 (1) of the 2018 Bill states *"Such further categories of personal data as may be specified by the Authority shall be sensitive personal data and, where such categories of personal data have been specified, the Authority may also specify any further grounds on which such specified categories of personal data may be processed".*

44 Clause 15(1) of the 2018 Bill states *"The Central Government shall, in consultation with the Authority and the sectoral regulator concerned, notify such categories of personal data as "sensitive personal data."*

45 Dvara Research, *supra*, page 10

46 Clause 44 (6) of the 2018 Bill states *"Without prejudice to sub-sections (1) or (2), or any other provision of this Act, the Authority may issue codes of practice in respect of (h) processing of personal data under any other ground for processing, including processing of personal data of children and development of age-verification mechanism under section 23 and mechanisms for processing personal data on the basis of consent of users incapable of providing valid consent under this Act."*

47 Clause 66(5) of the 2018 Bill states *"The books, registers, documents, records or data seized under sub-section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the reasons for retaining the same are recorded by her in writing and the approval of the Authority for such retention is obtained."*

48 Clause 66(7) of the 2018 Bill states "*The person from whose custody the books, registers, documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer or any other person appointed by her in this behalf at such place and time as the Authorised Officer may designated in this behalf."*

49 Clause 93 of the 2018 Bill states *"Notwithstanding anything contained in the Code of Criminal Procedure, 1973, an offence punishable under this Act shall be cognizable and non-bailable."*

50 Puttaswamy II, *supra*, page 427

51 Clause 96 (1) of the 2018 Bill states *"Where an offence under this Act has been committed by any department of the Central or State Government,or any authority of the State, the head of the department or authority shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly."*