To be introduced in Lok Sabha

Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

ARRANGEMENT OF CLAUSES

Clauses

CLAUSES

CLAUSES

CLAUSES

TO BE INTRODUCED IN LOK SABHA

Bill No. 373 of 2019

THE PERSONAL DATA PROTECTION BILL, 2019

A

BILL

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

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

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

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

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

CHAPTER I

PRELIMINARY

Short title and commencement.

1. (*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 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.

Application of Act to processing of personal data.

2. 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.

Definitions.

3. 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;

(*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 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; 53 of 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;

(*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 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;

21 of 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 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;

(*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;

(*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.

CHAPTER II

Obligations of Data Fiduciary

Prohibition of processing of personal data.

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

Limitation on purpose of processing of personal data.

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

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

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

Limitation on collection of personal data.

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

Requirement of notice for collection or processing of personal data.

7. (*1*) Every data fiduciary shall give to the data principal a notice, at the time of 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.

Quality of personal data processed.

8. (*1*) The data fiduciary shall take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

(*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.

Restriction on retention of personal data.

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

Accountability of data fiduciary.

10. 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.

Consent necessary for processing of personal data.

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

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

(*a*) free, having regard to whether it complies with the standard specified under section 14 of the Indian Contract Act, 1872; 9 of 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.

CHAPTER III

GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

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

12. 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.

Processing of personal data necessary for purposes related to employment, etc.

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

(*a*) recruitment or termination of employment of a data principal by the data fiduciary;

(*b*) provision of any service to, or benefit sought by, the data principal who is an employee of the data fiduciary;

(*c*) verifying the attendance of the data principal who is an employee of the data fiduciary; or

(*d*) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.

(*2*) Any personal data, not being sensitive personal data, may be processed under sub-section (*1*), where the consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing under the said sub-section.

Processing of personal data for other reasonable purposes.

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

(*a*) the interest of the data fiduciary in processing for that purpose;

(*b*) whether the data fiduciary can reasonably be expected to obtain the consent of the data principal;

(*c*) any public interest in processing for that purpose;

(*d*) the effect of the processing activity on the rights of the data principal; and

(*e*) the reasonable expectations of the data principal having regard to the context of the processing.

(*2*) For the purpose of sub-section (*1*), the expression "reasonable purposes" may include—

(*a*) prevention and detection of any unlawful activity including fraud;

(*b*) whistle blowing;

(*c*) mergers and acquisitions;

(*d*) network and information security;

(*e*) credit scoring;

(*f*) recovery of debt;

(*g*) processing of publicly available personal data; and

(*h*) the operation of search engines.

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

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

(*b*) determine where the provision of notice under section 7 shall apply or not apply having regard to the fact whether such provision shall substantially prejudice the relevant reasonable purpose.

Categorisation of personal data as sensitive personal data.

15. (*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 for the purposes of repeated, continuous or systematic collection of sensitive personal data for profiling of such personal data.

CHAPTER IV

PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

Processing of personal data and sensitive personal data of children.

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

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

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

(*a*) the volume of personal data processed;

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

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

(*d*) such other factors as may be prescribed.

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

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

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

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

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

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

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

CHAPTER V

RIGHTS OF DATA PRINCIPAL

Right to confirmation and access.

17. (*1*) The data principal shall have the right to obtain from the data fiduciary—

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

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

(*c*) a brief summary of processing activities undertaken by the data fiduciary with respect to the personal data of the data principal, including any information provided in the notice under section 7in relation to such processing.

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

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

Right to correction and erasure.

18. (*1*) The data principal shall where necessary, having regard to the purposes for which personal data is being processed, subject to such conditions and in such manner as may be specified by regulations, have the right to—

(*a*) the correction of inaccurate or misleading personal data;

(*b*) the completion of incomplete personal data;

(*c*) the 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.

Right to data portability.

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

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

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

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

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

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

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

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

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

Right to be forgotten.

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

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

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

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

(*2*) 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.

(*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 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.

General conditions for the exercise of rights in this Chapter.

21. (*1*) The data principal, for exercising any right under this Chapter, except the right under section 20, shall make a request in writing to the data fiduciary either directly or through a 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.

CHAPTER VI

Transparency and accountability measures

Privacy by design policy.

22. (*1*) Every data fiduciary shall prepare a privacy by design policy, containing—

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

(*b*) the obligations of data fiduciaries;

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

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

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

(*f*) the processing of personal data in a transparent manner; and

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

(*2*) 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.

Transparency in processing of personal data.

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

(*a*) the categories of personal data generally collected and the manner of such collection;

(*b*) the purposes for which personal data is generally processed;

(*c*) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;

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

(*e*) the right of data principal to file complaint against the data fiduciary to the Authority;

(*f*) where applicable, any rating in the form of a data trust score that may be accorded to the data fiduciary under sub-section (*5*) of section 29;

(*g*) where applicable, information regarding cross-border transfers of personal data that the data fiduciary generally carries out; and

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

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

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

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

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

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

Security safeguards.

24. (*1*) Every data fiduciary and the data processor shall, having regard to the nature, scope and purpose of processing personal data, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, implement necessary security safeguards, including—

(*a*) use of methods such as de-identification and encryption;

(*b*) steps necessary to protect the integrity of personal data; and

(*c*) steps necessary to prevent misuse, unauthorised access to, modification, disclosure or destruction of personal data.

(*2*) Every data fiduciary and data processor shall undertake a review of its security safeguards periodically in such manner as may be specified by regulations and take appropriate measures accordingly.

Reporting of personal data breach.

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

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

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

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

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

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

(*3*) The notice referred to in sub-section (*1*) shall be made by the data fiduciary to the Authority as soon as possible and within such period as may be specified by regulations, following the breach after accounting for any period that may be required to adopt any urgent measures to remedy the breach or mitigate any immediate harm.

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

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

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

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

Classification of data fiduciaries as significant data fiduciaries.

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

(*a*) volume of personal data processed;

(*b*) sensitivity of personal data processed;

(*c*) turnover of the data fiduciary;

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

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

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

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

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

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

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

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

shall be notified by the Central Government, in consultation with the Authority, as a significant data fiduciary:

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

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

(*a*) enable commercial or business oriented transactions;

(*b*) provide access to the Internet;

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

Data protection impact assessment.

27. (*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.

(*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.

Maintenance of records.

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

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

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

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

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

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

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

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

Audit of policies and conduct of processing, etc.

29. (*1*) The significant data fiduciary shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor under this Act.

(*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.

Data protection officer.

30. (*1*) Every significant data fiduciary shall appoint a data protection officer possessing such qualification and experience as may be specified by regulations for carrying out the following functions—

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

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

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

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

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

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

(*g*) maintaining an inventory of records to be maintained by the data 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.

Processing by entities other than data fiduciaries.

31. (*1*) The data fiduciary shall not engage, appoint, use or involve a data processor to process personal data on its behalf without a contract entered into by the data fiduciary and such data processor.

(*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.

Grievance redressal by data fiduciary.

32. (*1*) Every data fiduciary shall have in place the procedure and effective mechanisms to redress the grievances of data principals efficiently and in a speedy manner.

(*2*) A data principal may make a complaint of contravention of any of the provisions of this Act or the rules or regulations made thereunder, which has caused or is likely to cause harm to such data principal, to—

(*a*) the data protection officer, in case of a significant data fiduciary; or

(*b*) an officer designated for this purpose, in case of any other data fiduciary.

(*3*) A complaint made under sub-section (*2*) shall be resolved by the data fiduciary in an expeditious manner and not later than thirty days from the date of receipt of the complaint by such data fiduciary.

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

CHAPTER VII

Restriction on transfer of personal data outside India

Prohibition on processing of sensitive personal data and critical personal data outside India

33. (*1*) Subject to the conditions in sub-section (*1*) of section 34, the sensitive personal data may be transferred outside India, but such sensitive personal data shall continue to be stored in India.

(*2*) The critical personal data shall only be processed in India.

Explanation.—For the purposes of sub-section (*2*), the expression "critical personal data" means such personal data as may be notified by the Central Government to be the critical personal data.

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

34. (*1*) The sensitive personal data may only be transferred outside India for the purpose of processing, when explicit consent is given by the data principal for such transfer, and where—

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

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

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

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

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

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

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

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

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

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

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

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

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

CHAPTER VIII

EXEMPTIONS

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

35. 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;

2 of 1974.

(*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.

Exemption of certain provisions for certain processing of personal data.

36. 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.

Power of Central Government to exempt certain data processors.

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

Exemption for research, archiving or statistical purposes.

38. 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.

Exemption for manual processing by small entities.

39. (*1*) The provisions of sections 7, 8, 9, clause (*c*) of sub-section (*1*) of section 17 and sections 19 to 32 shall not apply where the processing of personal data by a small entity is not automated.

(*2*) For the purposes of sub-section (*1*), a "small entity" means such data fiduciary as may be classified, by regulations, by Authority, having regard to—

(*a*) the turnover of data fiduciary in the preceding financial year;

(*b*) the purpose of collection of personal data for disclosure to any other individuals or entities; and

(*c*) the volume of personal data processed by such data fiduciary in any one day in the preceding twelve calendar months.

Sandbox for encouraging innovation, etc.

40. (*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.

CHAPTER IX

DATA PROTECTION AUTHORITY OF INDIA

Establishment of Authority.

41. (*1*) The Central Government shall, by notification, establish, for the purposes of this Act, an Authority to be called the Data Protection Authority of India.

(*2*) The Authority referred to in sub-section (*1*) shall be a body corporate by the name aforesaid, having perpetual succession and a common seal, with power, subject to the provisions of this Act, to acquire, hold and dispose of property, both movable and immovable, and to contract and shall, by the said name, sue or be sued.

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

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

Composition and qualifications for appointment of Members.

42. (*1*) The Authority shall consist of a Chairperson and not more than six whole-time Members, of which one shall be a person having qualification and experience in law.

(*2*) The Chairperson and the Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of—

(*a*) the Cabinet Secretary, who shall be Chairperson of the selection committee;

(*b*) the Secretary to the Government of India in the Ministry or Department dealing with the Legal Affairs; and

(*c*) the Secretary to the Government of India in the Ministry or Department dealing with the Electronics and Information Technology.

(*3*) The procedure to be followed by the Selection Committee for recommending the names under sub-section (*2*) shall be such as may be prescribed.

(*4*) The Chairperson and the Members of the Authority shall be persons of ability, integrity and standing, and shall have qualification and specialised knowledge and experience of, and not less than ten years in the field of data protection, information technology, data management, data science, data security, cyber and internet laws, public administration, national security or related subjects.

(*5*) A vacancy caused to the office of the Chairperson or any other member of the Authority shall be filled up within a period of three months from the date on which such vacancy occurs.

Terms and conditions of appointment.

43. (*1*) The Chairperson and the Members of the Authority shall be appointed for a term of five years or till they attain the age of sixty-five years, whichever is earlier, and they shall not be eligible for re-appointment.

(*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.

Removal of Chairperson or other Members.

44. (*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 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.

Powers of Chairperson.

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

Meetings of Authority.

46. (*1*) The Chairperson and Members of the Authority shall meet at such times and places and shall observe such rules and procedures in regard to transaction of business at its meetings including quorum at such meetings, as may be prescribed.

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

(*3*) All questions which come up before any meeting of the Authority shall be decided by a majority of votes of the Members present and voting, and in the event of an equality of votes, the Chairperson or in his absence, the 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.

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

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

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

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

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

Officers and other employees of Authority.

48. (*1*) The Authority may appoint such officers, other employees, consultants and experts as it may consider necessary for effectively discharging 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.

Powers and functions of Authority.

49. (*1*) It shall be the duty of the Authority to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of this Act, and promote awareness about data protection.

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

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

(*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.

Codes of practice.

50. (*1*) The Authority shall, by regulations, specify codes of practice to promote good practices of data protection and facilitate compliance with the obligations under this Act.

(*2*) Notwithstanding anything contained in sub-section (*1*), the Authority may approve any code of practice submitted by 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;

(*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.

Power of Authority to issue directions.

51. (*1*) The Authority may, for the discharge of its functions under this Act, issue such directions from time to time as it may consider necessary to any data fiduciary or data processor who shall be bound to comply with such directions.

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

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

Power of Authority to call for information.

52. (*1*) Without prejudice to the other provisions of this Act, the Authority may require a data fiduciary or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.

(*2*) If the Authority requires a data fiduciary or a data processor to provide any information under sub-section (*1*), it shall provide a notice in writing to the data fiduciary or the data processor stating the reasons for such requisition.

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

Power of Authority to conduct inquiry.

53. (*1*) The Authority may, on its own or on a complaint received by it, inquire or cause to be inquired, if it has reasonable grounds to believe that—

(*a*) the activities of the data fiduciary or data processor are being conducted in a manner which is detrimental to the interest 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— 5 of 1908.

(*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.

Action to be taken by Authority pursuant to an inquiry.

54. (*1*) On receipt of a report under sub-section (*2*) of section 53, the Authority may, after giving such opportunity to the data fiduciary or data processor to make a representation in connection with the report as the Authority deems reasonable, by an order in writing—

(*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.

Search and seizure.

55. (*1*) Where in the course of inquiry under section 53, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such designated court, as may be notified by the Central Government, for an order for the seizure of such books, registers, documents and records.

(*2*) The Inquiry Officer may require the services of any police officer or any officer of the Central Government, or of both, to assist him for the purposes specified in sub-section (*1*) and it shall be the duty of every such officer to comply with such requisition.

(*3*) After considering the application and hearing the Inquiry Officer, if necessary, the designated court may, by order, authorise the Inquiry Officer—

(*a*) to enter, with such assistance, as may be required, the place or places where such books, registers, documents and records are kept;

(*b*) to search that place or those places in the manner specified in the order; and

(*c*) to seize books, registers, documents and records it considers necessary for the purposes of the inquiry.

(*4*)The Inquiry Officer shall keep in its custody the books, registers, documents and records seized under this section for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person, from whose custody or power they were seized and inform the designated court of such return.

(*5*) Save as otherwise provided in this section, every search or seizure made under this section shall be carried out in accordance with the provisions of the Code of Criminal Procedure, 1973 relating to searches or seizures made under that Code.

2 of 1974.

Co-ordination between Authority and other regulators or authorities.

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

CHAPTER X

Penalties and compensation

Penalties for contravening certain provisions of the Act.

57. (*1*) Where the data fiduciary contravenes any of the following provisions,—

(*a*) obligation to take prompt and appropriate action in response to a data security breach under section 25;

(*b*) failure to register with the Authority under sub-section (*2*) of section 26,

(*c*) obligation to undertake a data protection impact assessment by a significant data fiduciary under section 27;

(*d*) obligation to conduct a data audit by a significant data fiduciary under section 29;

(*e*) appointment of a data protection officer by a significant data fiduciary under section 30,

it shall be liable to a penalty which may extend to five crore rupees or two per cent. of its total worldwide turnover of the preceding financial year, whichever is higher;

(*2*) Where a data fiduciary contravenes any of the following provisions,—

(*a*) processing of personal data in violation of the provisions of Chapter II or Chapter III;

(*b*) processing of personal data of children in violation of the provisions of Chapter IV;

(*c*) failure to adhere to security safeguards as per section 24; or

(*d*) transfer of personal data outside India in violation of the provisions of Chapter VII,

it shall be liable to a penalty which may extend to fifteen crore rupees or four per cent. of its total worldwide turnover of the preceding financial year, whichever is higher.

(*3*) For the purposes of this section,—

(*a*) the expression "total worldwide turnover" means the gross amount of revenue 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.

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

58. Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter V, such data fiduciary shall be liable to a penalty of five thousand rupees for each day during which such default continues, subject to a maximum of ten lakh rupees in case of significant data fiduciaries and five lakh rupees in other cases.

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

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

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

60. If any data fiduciary or data processor fails to comply with any direction issued by the Authority under section 51or 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.

Penalty for contravention where no separate penalty has been provided.

61. Where any person fails to comply with any provision of this Act or the rules or regulations made thereunder applicable to such person, for which no separate penalty has been provided, then, such person shall be liable to a penalty which may extend to a maximum of one crore rupees in case of significant data fiduciaries, and a maximum of twenty five lakh rupees in other cases.

Appointment of Adjudicating Officer.

62. (*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*);

(*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.

Procedure for adjudication by Adjudicating Officer.

63. (*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.

Compensation.

64. (*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.

Compensation or penalties not to interfere with other punishment.

65. 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.

Recovery of amounts.

66. (*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 XI

Appellate Tribunal

Establishment of Appellate Tribunal.

67. (*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.

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

68. (*1*) A person shall not be qualified for appointment as the Chairperson or a member of the Appellate Tribunal unless he—

(*a*) in the case of Chairperson, is, or has been a Judge of the Supreme Court or Chief Justice of a High Court;

(*b*) in the case of a member, has held the post of Secretary to the Government of India or any equivalent post in the Central Government for a period of not less than two years or a person who is well versed in the field of data protection, information technology, data management, data science, data security, cyber and internet laws or any related subject.

(*2*) The Central Government may prescribe the manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the Chairperson and any member of the Appellate Tribunal.

Vacancies.

69. 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.

Staff of Appellate Tribunal.

70. (*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.

Distribution of business amongst Benches.

71. (*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.

Appeals to Appellate Tribunal.

72. (*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.

Procedure and powers of Appellate Tribunal.

73. (*1*) The Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.

5 of 1908.

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

5 of 1908.

(*a*) summoning and enforcing the attendance of any person and examining 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;

1 of 1872.

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

(*f*) reviewing its decisions;

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

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

(*i*) any other matter which may be prescribed.

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

45 of 1860.
2 of 1974.

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

74. (*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.

Appeal to Supreme Court.

75. (*1*) Notwithstanding anything contained in the Code of Civil Procedure, 1908 or in any other law, an appeal shall lie against any order of the Appellate Tribunal, not being an interlocutory order, to the Supreme Court on any substantial question of law.

5 of 1908.

(*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.

Right to legal representation.

76. 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.

Civil court not to have jurisdiction.

77. 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 XII

FINANCE, ACCOUNTS AND AUDIT

Grants by Central Government.

78. 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.

Data Protection Authority of India Funds.

79. (*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.

Accounts and Audit.

80. (*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.

Furnishing of returns, etc., to Central Government.

81. (*1*) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements (including statement on enforcement action taken) and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require.

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

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

(*4*) A copy of the report prepared under sub-section (*2*) shall also be made publicly available by the Authority.

CHAPTER XIII

OFFENCES

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

82. (*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.

Offences to be cognizable and non-bailable.

2 of 1974.

83. (*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.

Offences by companies.

84. (*1*) Where an offence under this Act has been committed by a company, every person who, at the time the offence was committed was in charge of, and was responsible to, the company for the conduct of the business of the company, as well as the company, shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

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

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

Explanation.—For the purpose of this section—

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

(*i*) a firm; and

(*ii*) an association of persons or a body of individuals whether incorporated or not.

(*b*) "director" in relation to—

(*i*) a firm, means a partner in the firm;

(*ii*) an association of persons or a body of individuals, means any member controlling affairs thereof.

Offences by State.

85. (*1*) Where it has been proved that an offence under this Act has been committed by any department or authority or body of the State, by whatever name called, the head of such department or authority or body shall be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

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

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

(*4*) Notwithstanding anything in this section, the provisions of the Code of Criminal Procedure, 1973 relating to public servants shall continue to apply. 2 of 1974.

CHAPTER XIV

MISCELLANEOUS

Power of Central Government to issue directions.

86. (*1*) The Central Government may, from time to time, issue to the Authority such directions as it may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order.

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

Provided that the Authority shall, as far as practicable, be given an opportunity to express its views before any direction is given under this sub-section.

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

Members, etc., to be public servants.

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

Protection of action taken in good faith.

88. 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.

Exemption from tax on income.

89. 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. 43 of 1961.

Delegation.

90. 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.

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

91. (*1*) Nothing in this Act shall prevent the Central Government from framing of any policy for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policy do not govern personal data.

(*2*) The Central Government may, in consultation with the Authority, direct any data fiduciary or data processor to provide any personal data anonymised or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government, in such manner as may be prescribed.

Explanation.—For the purposes of this sub-section, the expression "non-personal data" means the data other than personal data.

(*3*) The Central Government shall disclose annually the directions, made by it under sub-section (*2*), in such form as may be prescribed.

Bar on processing certain forms of biometric data.

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

Power to make rules.

93. (*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 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 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, 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.

Power to make regulations.

94. (*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 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*) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (*2*) of section 48;

(*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.

Rules and regulations to be laid before Parliament.

95. 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.

Overriding effect of this Act.

96. 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.

Power to remove difficulties.

97. (*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.

Amendment of Act 21 of 2000.

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

THE SCHEDULE
(*See* section 98)

AMENDMENTS TO THE INFORMATION TECHNOLOGY ACT, 2000
(21 OF 2000)

Omission of section 43A.

1. Section 43A of the Information Technology Act, 2000 (hereafter in this Schedule referred to as the principal Act) shall be omitted.

Amendment of section 87.

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

STATEMENT OF OBJECTS AND REASONS

In the matter of Justice K.S. Puttaswami and another *Vs*. Union of India [WP 494 of 2012], a nine Judge Constitutional Bench of the Supreme Court, while delivering its judgment on 24th August, 2017, declared "privacy" as a fundamental right under article 21 of the Constitution. Subsequently, on 26th September, 2018, a five Judge Constitutional Bench of the Supreme Court while delivering its final judgment in the above case impressed upon the Government to bring out a robust data protection regime.

2. The Government on 31st July, 2017 constituted a "Committee of Experts on Data Protection" chaired by Justice B.N. Srikrishna to examine the issues relating to data protection. The said Committee examined the issues on data protection and submitted its Report on 27th July, 2018. On the basis of the recommendations made in the said Report and the suggestions received from various stakeholders, it is proposed to enact a legislation, namely, the Personal Data Protection Bill, 2019.

3. The proposed Legislation seeks to bring a strong and robust data protection framework for India and to set up an Authority for protecting personal data and empowering the citizens' with rights relating to their personal data ensuring their fundamental right to "privacy and protection of personal data".

4. The salient features of the Data Protection Bill, 2019, *inter alia*, are as under—

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

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

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

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

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

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

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

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

(*ix*) to empower the Authority to specify the "code of practice" to promote good practices of data protection and facilitate compliance with the obligations under this legislation;

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

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

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

5. The Notes on Clauses explain in detail the various provisions contained in the Bill.

6. The Bill seeks to achieve the above objectives.

NEW DELHI;
The 5*th December*, 2019.

RAVI SHANKAR PRASAD.

Notes on Clauses

Clause 1.—This clause seeks to provide for short title and commencement of the Act.

Clause 2.—This clause seeks to clarify the application of the Act with regard to personal data of Indians and save for clause 91 would not be applicable to processing of anonymised data.

Clause 3.- This clause seeks to define certain expressions occurring in the Act.

Clause 4.—This clause seeks to prohibit processing of personal data without any specific, clear and lawful purpose.

Clause 5.—This clause seeks to limit the processing of personal data to the purpose consented to by the data principal or which is incidental or connected thereto.

Clause 6.—This clause seeks to lay down limitation on collection of personal data specifying that it should be only to the extent that is necessary.

Clause 7.—This clause seeks to lay down the requirement of notice for collection or processing of personal data and lists the various types of information that should be contained in the notice given to the data principal.

Clause 8.—This clause seeks to lay down that the data fiduciary should ensure the quality of the personal data processed.

Clause 9.—This clause seeks to lay down restriction on retention of personal data beyond what is necessary.

Clause 10.—This clause seeks to lay down the responsibility for complying with the provisions of this Act on the data fiduciary.

Clause 11.—This clause seeks to expound the various aspects of consent which are necessary for processing of personal data.

Clause 12.—This clause seeks to list out certain cases which provide for processing of personal data without consent.

Clause 13.—This clause seeks to provide for processing of personal data necessary for purposes related to employment.

Clause 14.—This clause seeks to provide for other reasonable purposes for which personal data may be processed.

Clause 15.—This clause seeks to provide for categorisation of personal data as sensitive personal data and lists out criteria for such categorisation.

Clause 16.—This clause seeks to provide for obligations on data fiduciaries who processed personal data of children.

Clause 17.—This clause seeks to provide the data principal with the right to confirmation and access to his personal data.

Clause 18.—This clause seeks to provide the data principal with a right to correct and erase his personal data.

Clause 19.—This clause seeks to provide the data principal the right to port personal data to any data fiduciary.

Clause 20.—This clause seeks to provide the data principal the right to be forgotten.

Clause 21.—This clause seeks to lay down the general conditions for the exercise of the rights in clauses 17 to 20.

Clause 22.—This clause seeks to list out the constituents of privacy by design policy.

Clause 23.—This clause seeks to require transparency in processing of personal data by requiring the fiduciary to inform the data principal and making information available.

Clause 24.—This clause seeks to require the data fiduciary to implement necessary security safeguards.

Clause 25.—This clause seeks to require the data fiduciary to report to the Authority about breach of any personal data.

Clause 26.—This clause seeks to provide for classification of certain data fiduciaries as significant data fiduciaries including certain social media intermediaries.

Clause 27.—This clause seeks to require significant data fiduciaries to undertake data protection impact assessment.

Clause 28.—This clause seeks to require significant data fiduciaries to maintain accurate and up-to-date records, including requiring significant social media intermediaries to provide for voluntary verification mechanism.

Clause 29.—This clause seeks to require significant data fiduciaries to have their policies and conduct audited by data auditors.

Clause 30.—This clause seeks to require significant data fiduciaries to appoint a Data Protection Officer.

Clause 31.—This clause seeks to require data fiduciaries to ensure a contract for processing by other data processors.

Clause 32.—This clause seeks to require every data fiduciary to have a grievance redressal mechanism.

Clause 33.—This clause seeks to prohibit processing of sensitive personal data and critical personal data outside India.

Clause 34.—This clause seeks to list out conditions under which sensitive personal data and critical personal data could be transferred outside India.

Clause 35.—This clause seeks to empower the Central Government to exempt any agency of the Government from application of the Act.

Clause 36.—This clause seeks to provide for exemption of certain provisions of the Act for certain processing of personal data.

Clause 37.—This clause seeks to clarify that the Government could exempt certain data processors who are processing data of foreigners, from the application of this Act.

Clause 38.—This clause seeks to provide for exemption when personal data is processed for research, archival or statistical purposes.

Clause 39.—This clause seeks to provide for exemption for small entities who are engaged in manual processing of personal data.

Clause 40.—This clause seeks to provide for a Sandbox which can facilitate new ideas and approaches without any regulatory violations.

Clause 41.—This clause seeks to establish a regulator namely the Data Protection Authority of India (the Authority).

Clause 42—This clause seeks to lift the compositions and qualifications for appointment of Chairperson and Members of the Authority and their method of selection.

Clause 43.—This clause seeks to list the terms and conditions of appointment for the Chairperson and Members of the Authority.

Clause 44.—This clause seeks to list the conditions under which a Chairperson or other Members of the Authority can be removed.

Clause 45.—This clause seeks to lay down that the powers of the Authority rests with the Chairperson

Clause 46.—This clause seeks to provide for the matters relating to meetings of the Authority.

Clause 47.—This clause seeks to provide that the proceedings of the Authority would not be invalidated due to vacancy, procedural irregularity, etc.

Clause 48.—This clause seeks to empower the Authority to appoint officers and other employees.

Clause 49.—This clause seeks to list the powers and functions of the Authority.

Clause 50.—This clause seeks to require the Authority to specify codes of practice to promote good practices of data protection.

Clause 51.—This clause seeks to empower the Authority to issue directions to any data fiduciary for the discharge of its functions.

Clause 52.—This clause seeks to empower the Authority to call for information from any data fiduciary

Clause 53.—This clause seeks to empower the Authority to conduct an inquiry into the affairs of a data fiduciary.

Clause 54.- This clause seeks to list out various actions that can be taken by the Authority pursuant to an inquiry

Clause 55.—This clause seeks to empower the Inquiry Officer of the Authority to order for search and seizure of documents, records, etc.

Clause 56.—This clause seeks to provide for coordination between the Authority and other regulators.

Clause 57.—This clause seeks to list out penalties for contravening certain provisions of the Act.

Clause 58.—This clause seeks to list out penalties for failure to comply with request made by data principal.

Clause 59.—This clause seeks to list out penalty for failure of the data fiduciary to furnish report, return, information to the Authority.

Clause 60.—This clause seeks to list out penalty for failure of the data fiduciary to comply with direction or order issued by the Authority.

Clause 61.—This clause seeks to list out penalty for contravention of any provision of this Act or rules or regulations made thereunder for which no separate penalty has been provided.

Clause 62.—This clause seeks to provide for appointment of Adjudicating Officer for adjudging penalties.

Clause 63.—This clause seeks to lay down the procedure for adjudication by Adjudicating Officer.

Clause 64—This clause seeks to provide for data principal's right to seek compensation from the data fiduciary in case of suffering harm.

Clause 65.—This clause seeks to ensure that compensation or penalties under this Act would not interfere with any other penalty or punishment.

Clause 66.—This clause seeks to lay down that penalties or compensation awarded under this Act may be recovered as arrear of land revenue.

Clause 67.—This clause seeks to lay down provisions relating to establishment of Appellate Tribunal.

Clause 68.—This clause seeks to list out qualifications, appointment, term, conditions of service of Chairperson and Members of Appellate Tribunal.

Clause 69.—This clause seeks to provide for filling up vacancies in the office of Chairperson and Members of Appellate Tribunal.

Clause 70.—This clause seeks to provide for staffing of Appellate Tribunal.

Clause 71.—This clause seeks to provide for distribution of business to different benches of the Appellate Tribunal.

Clause 72.—This clause seeks to provide for appeal to the Appellate Tribunal against any decision of the Authority.

Clause 73.—This clause seeks to lay down the procedure and powers of the Appellate Tribunal.

Clause 74.—This clause seeks to provide that the Appellate Tribunal shall have all the powers of a civil court.

Clause 75.—This clause seeks to provide for an appeal to the Supreme Court against any order of the Appellate Tribunal.

Clause 76.—This clause seeks to provide for the applicant or appellant to appear in person or authorise legal representative.

Clause 77.—This clause seeks to lay down that no civil court would have jurisdiction to entertain any suit on any matter which falls within the ambit of Appellate Tribunal.

Clause 78.—This clause seeks to provide for the Central Government to make grants to the Authority.

Clause 79. —This clause seeks to provide for constitution of the Data Protection Authority Fund.

Clause 80.—This clause seeks to require the Authority to maintain proper accounts which are to be audited by the Comptroller and Auditor-General of India.

Clause 81.—This clause seeks to require the Authority to furnish returns, statements, etc., to the Central Government.

Clause 82.—This clause seeks to list out punishment for the offence of reidentifying of deidentified personal data.

Clause 83.—This clause seeks to lays out that offence in Clause 82 to be cognizable and non-bailable.

Clause 84.—This clause seeks to list out provisions relating to commission of offence by companies.

Clause 85.—This clause seeks to list out provisions relating to commission of offence by any State Government or Central Government Department or agency.

Clause 86.—This clause seeks to empower the Central Government to issue directions to the Authority.

Clause 87.—This clause seeks to deem Members, officers etc. of the Authority to be public servants when acting pursuant to any provisions of the Act.

Clause 88.—This clause seeks to protect the Authority, Member, employee in case of action done under this Act in good faith.

Clause 89.—This clause seeks to exempts Authority from tax on income in respect of its income, profits.

Clause 90.—This clause seeks to empower the Authority to delegate its powers or functions to any Member or officer.

Clause 91.—This clause seeks to empower the Central Government to frame policies for digital economy in respect of non-personal data.

Clause 92.—This clause seeks to ban processing of certain forms of biometric data unless permitted by law.

Clause 93.—This clause seeks to empowers the Central Government to make rules to carry out the provisions of the Act.

Clause 94.—This clause seeks to empowers the Authority to make regulations consistent with the Act and rules made there under.

Clause 95.—This clause seeks to require that rules and regulations made under this Act are to be laid before the Parliament.

Clause 96.—This clause seeks to provide for the overriding effect of this Act notwithstanding anything inconsistent with any other law.

Clause 97.—This clause seeks to provide for power of Central Government to remove difficulties.

Clause 98.—This clause seeks to provide for related amendments to the Informations Technology Act, 2000.

FINANCIAL MEMORANDUM

Sub-clause (2) of clause 43 provides for the payment of salaries and allowances to the Chairperson, Members of the Authority.

2. Sub-clause (2) of clause 48 provides for the payment of salaries and allowances to the officers and employees of the Authority.

3. Sub-clause (2) of clause 68 provides for the payment of salaries and allowances to the Chairperson and Members of the Appellate Tribunal.

4. Sub-clause (3) of clause 70 provides for the payment of salaries and allowances to the officers and employees of the Appellate Tribunal.

5. For the aforesaid provisions, it would involve an expenditure of (recurring or non-recurring) one hundred crore rupees from the Consolidated Fund of India.

MEMORANDUM REGARDING DELEGATED LEGISLATION

Clause 93 of the Personal Data Protection Bill 2019 seeks to empower the Central Government to make rules for—(*a*) categorization of sensitive personal data under section 15; (*b*) verification of the age of child under sub-section (*3*) of section (*3*); (*c*) the form and manner in which an application to enforce the right to be forgotten can be exercised under sub-section (*2*) of section 20 and the manner of review of 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 regarding grievance redressal 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 procedure for conducting any inquiry under sub-section (*2*) of section 44; (*k*) 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; (*l*) other functions of the Authority under clause (*o*) of sub-section (*2*) of section 49; (*m*) 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; (*n*) other matters under clause (*e*) of sub-section (*8*) of section 53 in respect of which the Authority shall have powers; (*o*) the number of Adjudicating Officers, manner and terms of their appointment, their jurisdiction and other requirements under sub-section (*2*) of section 62; (*p*) the manner in which the Adjudicating Officer shall conduct an inquiry under sub-section (*1*) of section 63; (*q*) the form and manner of making a complaint under sub-section (*2*), and the procedure for hearing of a complaint under sub-section (*8*) of section 64; (*r*) 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; (*s*) the procedure of filling of vacancies in the Appellate Tribunal under section 69; (*t*) 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; (*u*) 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; (*v*) other matters under clause (*i*) of sub-section (*2*) of section 73 in respect of powers of the Appellate Tribunal; (*w*) 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; (*x*) the time in which and the form and manner in which the returns, statements, and particulars are to be furnished to the Central Government under sub-section (*1*) and annual report under sub-section (*2*) of section 81; (*y*) 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; (*z*) any other matter which is required to be, or may be, prescribed, or in respect of which provision is to be made, by rules.

2. Clause 94 of the Bill empowers the Authority, with the previous approval of the Central Government, by notification, to make regulations consistent with the provisions of the Act and the rules made thereunder to provide for—(*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*) the remuneration, salary or allowances and other terms and conditions of service of such officers, employees, consultants and experts under sub-section (*2*) of section 48; (*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; and (*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.

3. The matters in respect of which the aforementioned rules and regulations may be made are matters of procedure and administrative detail, and as such, it is not practicable to provide for them in the proposed Bill itself. The delegation of legislative power is, therefore, of a normal character.

ANNEXURE

EXTRACTS FROM THE INFORMATION TECHNOLOGY ACT, 2000

(21 OF 2000)

* * * * * *

Compensation for failure to protect data.

43A. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.—For the purposes of this section,—

(*i*) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;

(*ii*) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;

(*iii*) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

* * * * * *

Power of Central Government to make rules.

87. (*1*) * * * * * *

(*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:—

* * * * * *

(*ob*) the reasonable security practices and procedures and sensitive personal data or information under section 43A;

* * * * * *

LOK SABHA

A

BILL

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

(Shri Ravi Shankar Prasad, Minister of Law and Justice, Communications and Electronics and Information Technology)

MGIPMRND—4173LS(S3)—06-12-2019.