

THE PERSONAL DATA PROTECTION BILL, 2019

ARRANGEMENT OF CLAUSES
[Note: Table of Contents Not Redlined]

CHAPTER I: PRELIMINARY

1. Short title and commencement.
2. Application of Act to processing of personal data.
3. Definitions.

CHAPTER II: OBLIGATIONS OF DATA FIDUCIARY

4. Prohibition of processing of personal data.
5. Limitation on purpose of processing of personal data.
6. Limitation on collection of personal data.
7. Requirement of notice for collection or processing of personal data.
8. Quality of personal data processed.
9. Restriction on retention of personal data.
10. Accountability of data fiduciary.
11. Consent necessary for processing of personal data.

CHAPTER III: GROUNDS FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

12. Grounds for processing of personal data without consent in certain cases.
13. Processing of personal data necessary for purposes related to employment, etc.
14. Processing of personal data for other reasonable purposes.
15. Categorisation of personal data as sensitive personal data.

CHAPTER IV: PERSONAL DATA AND SENSITIVE PERSONAL DATA OF CHILDREN

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

CHAPTER V: RIGHTS OF DATA PRINCIPAL

17. Right to confirmation and access.
18. Right to correction and erasure.
19. Right to data portability.
20. Right to be forgotten.
21. General conditions for the exercise of rights in this Chapter.

CHAPTER VI: TRANSPARENCY AND ACCOUNTABILITY MEASURES

22. Privacy by design policy.
23. Transparency in processing of personal data.
24. Security safeguards.
25. Reporting of personal data breach.
26. Classification of data fiduciaries as significant data fiduciaries.
27. Data protection impact assessment.

28. Maintenance of records.
29. Audit of policies and conduct of processing, etc.
30. Data protection officer.
31. Processing by entities other than data fiduciaries.
32. Grievance redressal by data fiduciary.

CHAPTER VII: RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

33. Prohibition of processing of sensitive personal data and critical personal data outside India.
34. Conditions for transfer of sensitive personal data and critical personal data. CHAPTER VIII

CHAPTER VIII: EXEMPTIONS

35. Power of Central Government to exempt any agency of Government from application of the Act.
36. Exemption of certain provisions for certain processing of personal data.
37. Power of Central Government to exempt certain data processors.
38. Exemption for research, archiving or statistical purposes.
39. Exemption for manual processing by small entities.
40. Sandbox for encouraging innovation, etc.

CHAPTER IX: DATA PROTECTION AUTHORITY OF INDIA

41. Establishment of Authority.
42. Composition and qualifications for appointment of Members.
43. Terms and conditions of appointment.
44. Removal of Chairperson or other Members.
45. Powers of Chairperson.
46. Meetings of Authority.
47. Vacancies, etc., not to invalidate proceedings of Authority.
48. Officers and other employees of Authority.
49. Powers and functions of Authority.
50. Codes of practice.
51. Power of Authority to issue directions.
52. Power of Authority to call for information.
53. Power of Authority to conduct inquiry.
54. Action to be taken by Authority pursuant to an inquiry.
55. Search and seizure.
56. Co-ordination between Authority and other regulators or authorities.

CHAPTER X: PENALTIES AND COMPENSATION

57. Penalties for contravening certain provisions of the Act.
58. Penalty for failure to comply with data principal requests under Chapter V.
59. Penalty for failure to furnish report, returns, information, etc.
60. Penalty for failure to comply with direction or order issued by Authority.
61. Penalty for contravention where no separate penalty has been provided.
62. Appointment of Adjudicating Officer.
63. Procedure for adjudication by Adjudicating Officer.
64. Compensation.
65. Compensation or penalties not to interfere with other punishment.
66. Recovery of amounts.

CHAPTER XI: APPELLATE TRIBUNAL

67. Establishment of Appellate Tribunal.
68. Qualifications, appointment, term, conditions of service of Members.
69. Vacancies.
70. Staff of Appellate Tribunal.
71. Distribution of business amongst Benches.
72. Appeals to Appellate Tribunal.
73. Procedure and powers of Appellate Tribunal.
74. Orders passed by Appellate Tribunal to be executable as a decree.
75. Appeal to Supreme Court.
76. Right to legal representation.
77. Civil court not to have jurisdiction.

CHAPTER XII: FINANCE, ACCOUNTS AND AUDIT

78. Grants by Central Government.
79. Data Protection Authority of India Funds.
80. Accounts and Audit.
81. Furnishing of returns, etc., to Central Government.

CHAPTER XIII: OFFENCES

82. Re-identification and processing of de-identified personal data.
83. Offences to be cognizable and non-bailable.
84. Offences by companies.
85. Offences by State.

CHAPTER XIV: MISCELLANEOUS

86. Power of Central Government to issue directions.
87. Members, etc., to be public servants.
88. Protection of action taken in good faith.
89. Exemption from tax on income.
90. Delegation.
91. Act to promote framing of policies for digital economy, etc.
92. Bar on processing certain forms of biometric data.
93. Power to make rules.
94. Power to make regulations.
95. Rules and regulations to be laid before Parliament.
96. Overriding effect of this Act.
97. Power to remove difficulties.
98. Amendment of Act 21 of 2000. THE SCHEDULE.

THE PERSONAL DATA PROTECTION BILL, ~~2018~~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 ~~meant~~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.

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

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

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

CHAPTER I PRELIMINARY

Short title, ~~extent and~~ and commencement.—

1. (1) This Act may be called the Personal Data Protection Act, ~~2018~~2019.

~~(1)— It extends to the whole of India.~~

~~The provisions of Chapter XIV of this Act~~ (2) It shall come into force on such date, as the Central Government may, by notification ~~appoint and the remaining provisions of the~~ 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 ~~come be~~ construed as a reference to the coming into force ~~in accordance with the provisions in of that Chapter~~ provision.

Application of ~~the~~ Act to processing of personal data.—

This 2. The provisions of this Act ~~applies,~~—

(A) shall apply to—

(2)—(a) the following—

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

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

~~Notwithstanding anything contained in sub-section (1), the Act shall apply to~~ (c) the processing of personal data by data fiduciaries or data processors not present within the territory of India, ~~only~~ 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.

~~Notwithstanding anything contained in sub-sections (1) and (2), the Act~~ (B) shall not apply to ~~the~~ processing of ~~anonymised~~ of anonymised data, other than the anonymised data referred to in section 91.

Definitions:—

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

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

~~“(1) “Adjudicating Officer” means an officer of the adjudication wing~~ Adjudicating Officer appointed as such under sub-section 68(1) of section 62;

~~“Anonymisation”~~ (2) “anonymisation” in relation to personal data, means ~~the~~ such irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, ~~meeting which meets~~ the standards of irreversibility specified by the Authority;

~~“Anonymised”~~ (3) “anonymised data” means data which has undergone the process of anonymisation ~~under sub-clause (3) of this section;~~

~~“(4) “Appellate Tribunal” means the tribunal~~ Tribunal established under sub-section (1) or notified under Chapter XII of this Act sub-section (4) of section 67;

~~“(5) “Authority” means the Data Protection Authority of India established under Chapter X~~ sub-section (1) of this Act section 41;

~~“Automated”~~ (6) “automated” means any equipment capable of operating automatically in response to instructions given for the purpose of processing data;

~~“Biometric”~~ (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;

~~“Child”~~ (8) “child” means a data principal below the age of person who has not completed eighteen years of age;

~~“Code”~~ (9) “code of Practice” practice” means a code of practice issued by the Authority under section ~~64~~ 50;

~~“Consent” means~~ (10) “consent under” means the consent referred to in section 12 11;

~~“Data” means and~~ (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;

~~“(Data(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;~~

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

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

~~“(De(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;~~

~~“(Disaster”(17) “disaster” shall have the same meaning as assigned to it under clause (d) of section 2 of the Disaster Management Act, 2005 (53 of 2005);”;~~

~~(4)(2) “Explicit consent” means consent under section (18;~~

~~“(Financial) “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;~~

~~“(Genetic(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;~~

~~“(Harm”(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;”;~~

~~“(Health(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;”;~~

~~(5)(3) “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.~~

“Intra(22) ~~“intra-group schemes”~~ means the schemes approved by the Authority under clause (a) of sub-section 4(1) of section 34;

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

(24) ~~“journalistic purpose”~~ means any activity intended towards the dissemination through print, electronic or any other media of factual reports, analysis, opinions, views or documentaries regarding—

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

“Notification”(25) ~~“notification”~~ means a notification published in the Official Gazette and the term ~~“expression “notify”~~ shall be construed accordingly;

“Official(26) ~~“official identifier”~~ means any number, code, or other identifier, ~~including Aadhaar number~~, assigned to a data principal under a law made by Parliament or any State Legislature which may be used for the purpose of verifying the identity of a data principal;

~~(6)(4) “Person” means—~~

~~(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;~~

“Personal(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 any combination of such features 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;~~

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

“Prescribed”(30) ~~“prescribed”~~ means prescribed by rules made ~~by the Central Government~~ under this Act;

“Processing”(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;

“Profiling”(32) **“profiling”** means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or ~~interest~~interests of a data principal;

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

(34) **“re-identification”**~~meansthe~~ **means the** process by which a data fiduciary or data processor may reverse a process of de-identification;

“Sensitive Personal Data”~~means~~(35) **“Schedule”** means the Schedule appended to this Act;

(36) **“sensitive personal data-revealing,”** **means such personal data, which may, reveal, be related to, or** ~~constituting, as may be applicable~~constitute—

(i) ~~—~~passwords;

(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;

~~religious or~~ (xi) religious or political belief or affiliation; or

(ii)(i) (xii) any other category of data specified by the Authority under section 22.

“Significant data fiduciary”~~means a~~categorised as sensitive personal data fiduciary notified by the Authority under section 38;15.

(7)(5) **“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;~~

(8)(6) **“Specified”** ~~means specified by regulations made by the Authority under this Act and the term “specify” shall be construed accordingly;~~

(9)(7) **“State”** ~~shall, unless the context otherwise requires, have the same meaning assigned to it under Article 12 of the Constitution;~~

(10)(8) **“Systematic activity”** ~~means any structured or organised activity that involves an element of planning, method, continuity or persistence;~~

“Transgender status”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

DATA PROTECTION OBLIGATIONS OF DATA FIDUCIARY

~~Fair and reasonable~~ Prohibition of processing.—Any 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 that respects and ensure the privacy of the data principal;

2. Purpose limitation.—

Personal data shall be processed only and

(1) (b) for purposes that are clear, specific and lawful.

Personal data shall be processed only for purposes specified or for any other incidental the purpose that 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 specified purposes purpose, and in the context and circumstances in which the personal data was collected.

~~Collection limitation.—Collection~~ Limitation on collection of personal data.

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

3. Lawful Requirement of notice for collection or processing.—

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

Sensitive personal data.

(2) 7. (1) Every data fiduciary shall be processed only on the basis of one or a combination of grounds of processing in Chapter IV.

4. Notice.—

~~The data fiduciary shall provide to~~ the data principal ~~with the following information, no later than 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 ~~is~~ 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 ~~such~~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 ~~section~~sections 12 to ~~section 17, and section 18 to section 22~~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 ~~will~~shall be retained in terms of section 109 or where such period is not known, the criteria for determining such period;
- (j) the existence of and procedure for the exercise of ~~data principal~~ rights mentioned in Chapter ~~IV~~ and any related contact details for the same;
- (k) the procedure for grievance redressal under section 3932;
- (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~~assigned to the data fiduciary under ~~sub-section 35(5) of section 29;~~ and
- (n) any other information as may be specified by the ~~Authority~~regulations.

~~The data fiduciary shall provide the information as required under this (2)~~ The notice referred to in sub-section ~~to the data principal in a~~(1) shall be clear and, concise manner that is and easily comprehensible to a reasonable person and in multiple languages where necessary and practicable.

~~Sub(3) The provisions of sub-section (1) shall not apply where the provision of such notice under this section would substantially prejudice~~ the purpose of processing of personal data under sections 15 or 21 of this Act section 12.

5. Data quality.—

The data Quality of personal data processed.

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

In considering whether which it is processed.

(2) While taking any reasonable step is necessary under 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 individualsindividual or entitiesentity, including other data fiduciariesfiduciary or processorsprocessor, and the data fiduciary subsequently finds that such data does not comply with e requirement of sub-section (1), the data fiduciary shall take reasonable steps to notify suchindividualssuch individual or entitiesentity of thisfactthis fact.

6. ~~Data storage limitation.—~~

~~The data fiduciary shall retain Restriction on retention of personal data only as long as may be reasonably.~~

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 of time if such retention is explicitly mandated, consented to by the data principal, or necessary to

comply with any obligation, under a lawany law for the time being in force.

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

(4) Where it is not necessary for personal data to be retained by the data fiduciary under sub-sectionsection (1) and/or sub-section (2), then, such personal data mustshall be deleted in asuch manner as may be specified by regulations.

Accountability.— of data fiduciary.

10. The data fiduciary shall be responsible for complying with all obligations set out inthe provisions of this Actact in respect of any processing undertaken by it or on its behalf.

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

~~CHAPTER III~~

~~GROUNDS FOR PROCESSING OF PERSONAL DATA~~

~~Processing of Consent necessary for processing of personal data.~~

7. 11. (1) ~~The personal data on the basis of consent.—~~

~~Personal data mayshall not be processed on, except on the consent given by the data principal at the basiscommencement of theits processing.~~

(1) (2) ~~The consent of the data principal, given no later than at the commencement of the processing.~~

~~For the consent of the data principal to shall not be valid, it must beunless such consent is—~~

(a) free, having regard to whether it meetscomplies 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 87;

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

~~The data fiduciary shall not make the~~(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 data fiduciary shall bear the burden of proof to establish that the consent has been given by the data principal for processing of the personal data in accordance with sub-section (2); shall be on the data fiduciary.

(6) Where the data principal withdraws his consent for from the processing of any personal data necessary for the performance of a contract to which the data principal is a party without any valid reason, all legal consequences for the effects of such withdrawal shall be borne by the such data principal.

CHAPTER III

~~Processing~~ GROUND FOR PROCESSING OF PERSONAL DATA WITHOUT CONSENT

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

8. ~~12.~~ Notwithstanding anything contained in section 11, the State.—

~~Personal~~personal data may be processed if such processing is necessary, —

(1) (a) for any function of Parliament or any State Legislature.

~~Personal data may be processed if such processing is necessary for the exercise of 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, ~~license~~licence or permit for any action or activity of the data principal by the State.;

9. ~~Processing of personal data in compliance with law or any order of any court or tribunal.—~~

~~Personal data may be processed if such processing is—~~

~~explicitly mandated~~ (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;~~

10. ~~Processing of personal data necessary for prompt action.—~~

~~Personal data may be processed if such processing is necessary—~~

~~(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;~~

~~(a) 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~~

~~(b)(a) 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.~~

11. ~~Processing of personal data necessary for purposes related to employment.—~~

~~(1) 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)(a) any other activity relating to the assessment of the performance of the data principal who is an employee of the data fiduciary.~~

~~(2) Sub-section (1) shall apply only where processing on the basis of consent of the data principal is not appropriate having regard to the employment relationship between the data fiduciary and the data principal, or would involve a disproportionate effort on the part of the data fiduciary due to the nature of the processing activities under this section.~~

12. ~~Processing of data for reasonable purposes.—~~

~~(1) In addition to the grounds for processing contained in section 12 to section 16, personal data may be processed if such processing is necessary for such reasonable purposes as may be specified after taking into consideration—~~

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

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

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

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

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

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

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

~~(b) whistle blowing;~~

~~(c) mergers and acquisitions;~~

- ~~(d) network and information security;~~
- ~~(e) credit scoring;~~
- ~~(f) recovery of debt;~~
- ~~(g)(a) processing of publicly available personal data;~~
- (3) ~~Where the Authority specifies a reasonable purpose under sub-section (1), it shall:~~
 - ~~(a) lay down such safeguards as may be appropriate to ensure the protection of the rights of data principals; and~~
 - ~~(b)(a) determine where the provision of notice under section 8 would not apply having regard to whether such provision would substantially prejudice the relevant reasonable purpose.~~

CHAPTER IV

GROUND FOR PROCESSING OF SENSITIVE PERSONAL DATA

13. ~~Processing of sensitive personal data based on explicit consent.—~~
- ~~(1) Sensitive personal data may be processed on the basis of explicit consent.~~
 - ~~(2)(1) For the purposes of sub-section (1), consent shall be considered explicit only if it is invalid as per section 12 and is additionally:~~
 - ~~(a) informed, having regard to whether the attention of the data principal has been drawn to purposes of operations in processing that may have significant consequences for the data principal;~~
 - ~~(b) clear, having regard to whether it is meaningful without recourse to inference from conduct in a context; and~~
 - ~~(c)(a) specific, having regard to whether the data principal is given the choice of separately consenting to the purposes of, operations in, and the use of different categories of sensitive personal data relevant to processing.~~
14. ~~Processing of sensitive personal data for certain functions of the State.—~~
- ~~Sensitive personal data may be processed if such processing is strictly necessary for:~~
- ~~(a) any function of Parliament or any State Legislature.~~
 - ~~(b)(a) the exercise of any function of the State authorised by law for the provision of any service or benefit to the data principal.~~
15. ~~Processing of sensitive personal data in compliance with law or any order of any court or tribunal.—~~
- ~~Sensitive personal data may be processed if such processing is —~~
- ~~(a) explicitly mandated under any law made by Parliament or any State Legislature;~~
~~or~~
 - ~~(b)(a) necessary for compliance with any order or judgment of any Court or Tribunal in India.~~
16. ~~Processing of certain categories of sensitive personal data for prompt action.—~~

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

~~(a) — to respond to any medical emergency involving a threat to the life or a severe threat to the health of the data principal;~~

~~(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.~~

~~Further categories Processing of sensitive personal data.— necessary for purposes related to employment, etc.~~

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

~~(a) — recruitment or termination of employment of a data principal by the Authority shall be 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 and, may be processed under sub-section (1), where such categories 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 have been specified, the Authority may also specify any further for other reasonable purposes.~~

~~14. (1) In addition to the grounds on which such specified categories of 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—~~

~~The (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 specify—

(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 under sub-section (1) as "sensitive personal data", having regard to—

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

CHAPTER ~~V~~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 ~~children~~ a child in asuch manner that protects ~~and advances~~ the rights of, and ~~is in the~~ best interests of, the child.

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

(2) ~~Appropriateness of an age verification mechanism incorporated by a data fiduciary shall be determined on the basis of—~~

(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/ren/child;
- (c) possibility of harm to child/ren/child arising out of processing of personal data; and
- (d) such other factors as may be specified by the Authority/prescribed.

(3) (4) The Authority shall ~~notify the following, by regulations, classify any data fiduciary~~, as guardian data fiduciaries—

data fiduciaries/fiduciary, who—

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

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

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

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

Where a (7) A guardian data fiduciary ~~notified under sub-section (4) exclusively provides counseling/providing exclusive counselling~~ or child protection services to a child, ~~as under sub-section (6), then such guardian data fiduciary will shall~~ not be ~~required/require~~ to obtain ~~parental/the~~ consent ~~as set out 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 VI

V RIGHTS OF DATA PRINCIPAL—RIGHTS

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;

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

abrief (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 8 in 7 in relation to such processing activities.

(2) The data fiduciary shall provide the information ~~as required~~ under ~~this 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, etc.— and erasure.

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

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

(b) the completion of incomplete personal data; ~~and~~

(c) the updating of personal data that is out-of-date; ~~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 ~~the need for~~ such correction, completion, updatation or updating ~~having erasure having~~ regard to the purposes of processing, ~~the such~~ data fiduciary shall provide the data principal with adequate ~~justification in~~ justification in writing for rejecting the application.

(3) Where the data principal is not satisfied with ~~the justification~~ the justification provided by the data fiduciary under sub-section (2), the data ~~principal may~~ 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, ~~or~~ updates or erases any personal data in accordance with sub-section (1), ~~the such~~ data fiduciary shall also take ~~reasonable~~ necessary steps to notify all relevant entities or individuals to whom such personal data may have been disclosed regarding the relevant correction, completion, updatation or updating ~~erasure~~, particularly where such action ~~would~~ may have an impact on the rights and interests of the data principal or on decisions made regarding them.

17. Right to ~~Data Portability.~~—

~~The data principal portability.~~

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

~~reecive~~ (a) receive the following personal data ~~related to the data principal~~ in a structured, commonly used and machine-readable format—

~~which such~~ (i) the personal data ~~principal has~~ 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~~ 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.

~~Sub-section (1) shall only apply where the processing has been carried out through automated means, and~~ (2) The provisions of sub-section (1) shall not apply where—

(a) ~~(a)~~ processing is necessary for functions of the State ~~under section 13;~~

~~processing is or~~ in compliance of law ~~as referred to in or order of a court under~~ section 14; ~~or~~ 12;

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

Right to ~~Be Forgotten.~~—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 related to the data principal where~~fiduciary where such disclosure—

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

(b) _____ was made ~~on~~with the ~~basis of~~ consent of the data principal under section ~~12~~11 and such consent has since been withdrawn; or

(c) _____ was made contrary to the provisions of this Act or any other law ~~made by Parliament or any State Legislature~~for the time being in force.

~~Sub(2) The rights under sub-section (1) shall~~may be enforced only ~~apply where~~on an order of the Adjudicating Officer ~~under section 68~~determines the applicability of ~~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 (a), (b) or (c) of sub-section (1) and that the rights and interests of~~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 ~~override~~overrides the right to freedom of speech and expression and the right to information of any other citizen.

~~In determining whether the condition in sub-section (2) is satisfied, the~~(3) _____ The Adjudicating Officer shall ~~have, 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~~systematically~~fiduciary systematically facilitates access to personal data and whether the activities ~~would~~shall be significantly impeded if disclosures of the relevant nature were to be restricted or prevented.

~~(2)(1) The right under sub-section (1) shall be exercised by filing an application in such form and manner as may be prescribed.~~

(4) _____ Where any person finds that personal data, the disclosure of which has been restricted or prevented by an order of the Adjudicating ~~Officer~~Officer under sub-section (2), does not satisfy the conditions referred to in that sub-section ~~any longer, they, he~~ may apply for the review of that order to the Adjudicating Officer in such manner as may be prescribed, and ~~such~~the Adjudicating Officer shall review ~~her~~his order ~~on the basis of the considerations referred to in sub-section (3).~~

(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 ~~exercise of~~data principal, for exercising any right under this Chapter, except the right ~~under section 27,~~under section 20, shall ~~only be on the basis of~~make a request ~~made~~ in writing to the data ~~fiduciary~~with reasonable~~fiduciary either directly or through a consent manager with the necessary information to satisfy the data fiduciary of the~~as regard to his identity ~~of the data principal making the~~

~~request~~, and the data fiduciary shall acknowledge the receipt of such request within such period ~~of time~~ as may be specified by regulations.

~~The data fiduciary may charge a reasonable fee to be paid for (2) For complying with requests the request made under this Chapter, except for requests made under clauses (a) and 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.~~

~~(1) of section 24 and section 25 which shall be complied with by the (3) The data fiduciary without charging any fee.~~

~~The Authority may specify a reasonable time period within which the data fiduciary shall shall comply with the requests request under this Chapter, and such time period shall be communicated communicate the same to the data principal along with the acknowledgement referred to in sub-section (1), 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 making such request with adequate the reasons for such refusal as per the provisions of this Chapter 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.~~

~~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 made under this Chapter where such compliance would shall harm the rights of any other data principal under this Act.~~

~~(3)(2) The manner of exercise of rights under this Chapter shall be in such form as may be provided by law or in the absence of such law, in a reasonable format to be followed by each data fiduciary.~~

~~CHAPTER VII~~

CHAPTER VI

TRANSPARENCY AND ACCOUNTABILITY MEASURES

Privacy by ~~Design~~.—design policy.

22. (1) Every data fiduciary shall implement policies and measures to ensure that prepare a privacy by design policy, containing—

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

~~(a) the obligations mentioned in Chapter II are embedded in organisational and business practices;~~

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

(f) the processing of personal data is carried out in a transparent manner; and
(g) the interest of the data principal is accounted for at every stage of processing of personal data.

(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.

~~The 23.~~ (1) Every data fiduciary shall take reasonable necessary steps to maintain transparency regarding its general practices related to in processing personal data and shall make the following information available in an easily accessible 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 the exercise of rights of data principal rights mentioned in under Chapter VI, V and any related contact details for the same;

(e) the existence of a right of data principal to file complaints 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 35(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 the Authority regulations.

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

~~Having~~^{24.} (1) Every data fiduciary and the data processor shall, ~~having~~ regard to the nature, scope and purpose of processing personal data ~~undertaken~~, the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing, ~~the data fiduciary and the data processor shall~~ implement ~~appropriate~~^{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~~^{as periodically in such manner as} may be specified ~~by regulations~~ and ~~may~~ take appropriate measures accordingly.

18. ~~Personal Data Breach.~~—

~~The Reporting of personal data breach.~~

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

(2) The ~~notification~~^{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
- ~~measures~~(d) ~~action~~ being taken by the data fiduciary to remedy the breach.

(3) The ~~notification~~^{notice} referred to in sub-section (1) shall be made by the data fiduciary to the Authority as soon as possible and ~~not later than the time~~^{within such} period ~~as may be~~ specified by ~~the Authority~~^{regulations}, following the breach after accounting for any ~~time~~^{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 ~~as set out~~^{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 ~~notification~~^{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~~^{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 ~~own~~ 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.—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, in addition, by regulations specify those, such circumstances, or classesclass of data fiduciariesfiduciary, or processing operationsoperation where such data protection impact assessment shall be mandatory, and may also specify those 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, ~~at~~—

(1) ~~(a minimum—~~
) 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 ~~prepared~~ and ~~shall~~ submit the ~~same~~ assessment with his finding to the ~~Authority in~~ 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~~ processing or direct that such processing shall be subject to such conditions as ~~may be issued by~~ the Authority may deem fit.

19. ~~Record-Keeping.—~~

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 ~~11~~ 10;

(b) periodic review of security safeguards under section ~~31~~ 24;

~~data protection~~ (c) data protection impact assessments under section ~~33~~ 27; and

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

(1) ~~The records in sub-section (1) shall be maintained in such form as specified by the Authority.~~

(2) Notwithstanding anything contained in this Act, this section shall also apply to the ~~Central or State Government, departments of the Central and State Government, and any agency instrumentality or authority.~~

(3) Every social media intermediary which is “~~the State~~” notified as a significant data fiduciary under Article 12 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 the Constitution~~ verification, which shall be visible to all users of the service, in such manner as may be prescribed.

20. ~~Data Audits.—~~

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 ~~will~~shall evaluate the compliance of the data fiduciary with the provisions of this Act, including—

(a) clarity and effectiveness of notices under section ~~87~~;

(b) effectiveness of measures adopted under section ~~2922~~;

(c) transparency in relation to processing activities under section ~~3023~~;

(d) security safeguards adopted pursuant to section ~~3124~~;

(e) instances of personal data breach and response of the data fiduciary, including the promptness of ~~notification~~notice to the Authority under section ~~32~~and 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, ~~manner~~ and procedure for conducting audits under this section ~~including any civil penalties on data auditors for negligence~~.

(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, ~~with~~possessing such qualifications, experience and eligibility having regard to factors such as independence, integrity and ability, as it may ~~specify~~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 ~~asuch~~ manner that is likely to cause harm to a data principal, the Authority may ~~order~~direct the data fiduciary to conduct an audit and shall appoint a data auditor for that purpose.

Data ~~Protection Officer~~.—protection officer.

~~The~~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 ~~where required~~ on carrying out the ~~manner in which~~ data protection impact assessments ~~must be carried out~~, and carry out ~~the~~its review ~~of such assessment as~~ under sub-section (4) of section ~~3327~~;

(d) providing advice to the data fiduciary, ~~where required~~ on the ~~manner in which~~ development of internal mechanisms ~~may be developed in order~~ to satisfy the principles ~~set out~~specified under section ~~2922~~;

(e) providing assistance to and ~~cooperating~~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 raising grievances to the data fiduciary pursuant to redressal under section 39 of this Act~~³²; and

(g) ~~maintaining an inventory of all records to be maintained by the data fiduciary pursuant to under section 34~~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, in addition to the functions provided in sub-section (1) above.~~

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

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

Processing by entities other than data fiduciaries.—

31. (1) ~~The data fiduciary shall only not engage, appoint, use or involve a data processor to process personal process personal data on its behalf through a valid 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 further engage, appoint, use, or involve another data processor in the relevant processing on its behalf, except with the authorisation of the data fiduciary, and unless permitted through 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 unless they are required to do otherwise under law and shall treat any personal data that comes within their knowledge as and treat it confidential.~~

21. ~~Grievance redressal by Classification of data fiduciaries as significant data fiduciaries.—~~

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

(a) ~~volume of personal data processed;~~

(b) ~~sensitivity of personal data processed;~~

~~turnover of the data fiduciary;~~

(c) ~~risk of harm resulting from any processing or any kind of processing undertaken by the fiduciary;~~

(d) ~~use of new technologies for processing; and~~

(e)(a) ~~any other factor relevant in causing harm to any data principal as a consequence of such processing.~~

(2) ~~The notification of a data fiduciary or classes of data fiduciaries as significant data fiduciaries by the Authority under sub-section 32. (1) shall require such data fiduciary or class of data fiduciaries to register with the Authority in such manner as may be specified.~~

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

~~(a) — data protection impact assessments under section 33;~~

~~(b) — record keeping under section 34;~~

~~(c) — data audits under section 35; and~~

~~(d)(a) data protection officer under section 36.~~

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

22. ~~Grievance Redressal.~~ —

Every data fiduciary shall have in place ~~proper procedures~~ the procedure and effective mechanisms to ~~address~~ redress the grievances of data principals efficiently and in a speedy manner.

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

(4) ~~_____~~ Where, ~~a grievance under sub-section (2)~~ a complaint is not resolved within the ~~time~~ time period ~~mentioned~~ specified under sub-section (3), or where the data principal is not satisfied with the manner in which the ~~grievance~~ complaint is resolved, or the data fiduciary has rejected the ~~grievance raised~~ complaint, the data principal ~~shall have the right to~~ may file a complaint ~~with~~ to the ~~adjudication wing under section 68 of the Act~~ Authority in ~~the~~ such manner ~~as may be~~ prescribed.

CHAPTER VII

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

CHAPTER VIII

RESTRICTION ON TRANSFER OF PERSONAL DATA OUTSIDE INDIA

23. ~~Restrictions~~ Prohibition on ~~Cross-Border~~ Transfer of Personal Data. —

- (1) ~~Every data fiduciary shall ensure the storage, on a server or data centre located in India, of at least one serving copy of personal data to which this Act applies.~~
- (2) ~~The Central Government shall notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.~~
- (3) ~~Notwithstanding anything contained in sub-section (1), the Central Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the State.~~

~~Nothing contained in sub-section (3) shall apply to processing of sensitive personal data and critical personal data outside India~~

24. ~~Conditions for Cross-Border Transfer of Personal Data.—~~

~~Personal data other than those categories of 33. (1) Subject to the conditions in sub-section (1) of section 34, the sensitive personal data notified under sub-section (2) of section 40 may be transferred outside the territory of India where—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 subject to standard contractual clauses pursuant to a contract or intra-group schemes that have been 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 prescribed that transfers allowed the transfer to a particular country, or to a sector within or, such entity or class of entity in a country or to a particular, an international organisation is permissible; or on the basis of its finding that—~~

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

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

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

~~(2) The Central Government may only prescribe the permissibility of transfers under clause~~

~~(b) of sub-section (1) where it finds that the relevant (i) such sensitive personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section; 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 40, sensitive section 33, any critical personal data notified by the Central Government may be transferred outside the territory of India, only where such transfer is—

(a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under section 16; and 12; or

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

transfers is necessary for any class of data fiduciaries or data principals and does not hamper the effective enforcement of this Act.

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

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

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

CHAPTER IX

CHAPTER VIII EXEMPTIONS

25. Security of the State.—

Processing of personal data—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 interests of interest of sovereignty and integrity of India, the security of the State shall not be permitted unless it is authorised pursuant to a law, and is in accordance with the, 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 established by such law, made, safeguards and oversight mechanism to be followed by Parliament and is necessary for, and proportionate to, such interests being achieved the agency, as may be prescribed.~~

~~Any Explanation.—For the purposes of this section,—~~

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

~~(ii) the expression "processing authorised of such personal data" includes sharing by a law referred to in sub-section (1) shall be exempted from the following or sharing with such agency of the Government by any data fiduciary, data processor or data principal.~~

~~Exemption of certain provisions of the Act—for certain processing of personal data.~~

~~(a)—36. The provisions of Chapter II, except section 4;~~

~~(b)—Chapter, Chapters III;~~

~~(c)—Chapter IV;~~

~~(d)—Chapter to V;~~

~~(e)—, Chapter VI;~~

~~Chapter VII, except section 31; and 24, and Chapter VII shall not apply where—~~

~~(f)(a) Chapter VIII.~~

26. ~~Prevention, detection, investigation and prosecution of contraventions of law.—~~

~~(1) Processing of (a) personal data is processed in the interests of prevention, detection, investigation and prosecution of any offence or any other contravention of any law shall not be permitted unless~~

~~it is authorised by a law made by Parliament and State Legislature and is necessary for, and proportionate to, such interests the time being achieved.~~

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

~~(a)—Chapter II, except section 4;~~

~~(b)—Chapter III;~~

~~(c)—Chapter IV;~~

~~(d)—Chapter V;~~

~~(e)—Chapter VI;~~

~~(f)—Chapter VII except section 31; and~~

~~(g)(a) Chapter VIII.~~

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

~~(3)(2) Personal data processed under sub-section (1) shall not be retained once the purpose of prevention, detection, investigation or prosecution of any offence or other contravention of law is complete except where such personal data is necessary for the maintenance of~~

~~any record or database which constitutes a proportionate measure to prevent, detect or investigate or prosecute any offence or class of offences in future.~~

27. ~~Processing for the purpose of legal proceedings.—~~

~~Where (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 such processing shall be exempted from the following provisions of this Act—;~~

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

~~Where (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 following provisions 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.~~

- ~~(g) Chapter II, except section 4;~~
- ~~(h) Chapter III;~~
- ~~(i) Chapter IV;~~
- ~~(j) Chapter V;~~
- ~~(k) Chapter VI; and~~
- ~~(l)(b) Chapter VII, except section 31.~~

28. ~~Research, archiving or statistical purposes.—~~

~~Where processing of personal data is necessary Exemption for research, archiving or statistical purposes.~~

~~38. Where the processing of personal data is necessary for research, archiving, or statistical purposes, such processing may be exempted from such and the Authority is satisfied that—~~

- (1) ~~(a) the compliance with the provisions of this Act as the Authority may specify except section 4, section 31 and section 33.~~

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

(3) ~~Sub-section (1) shall apply only where—~~

~~compliance with the provisions of this Act will disproportionately divert resources from the such purpose referred to in sub-section (1);~~

~~(b) the purposes of processing cannot be achieved if the personal data is anonymised;~~

~~(c) the data fiduciary has carried out de-identification ~~meeting in accordance with the standard contained in any~~ code of practice specified under section 61, ~~where~~ 50 and the purpose of processing can be achieved if the personal data is in a de-identified form;~~

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

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

29. ~~Personal or domestic purposes.—~~

~~Personalit 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 a natural person such data fiduciary in any one day in the ~~course~~ preceding twelve calendar months.~~

~~Sandbox for encouraging innovation, etc.~~

~~40. (1) The Authority shall, for the purposes of a purely personal encouraging innovation in artificial intelligence, machine-learning or domestic purpose, 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 exempted from 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

(1) (c) that the following provisions of this Act—

(a) Chapter II, except section 4;

(b) Chapter III;

(c) Chapter IV;

(d) Chapter V;

(e) Chapter VI;

(f) Chapter VII; and

(g)(a) Chapter VIII.

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

(a) involves disclosure to the public; or

(b)(a) is undertaken in connection with any professional or commercial activity.

30. Journalistic purposes.—

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

(a) Chapter II, except section 4;

(b) Chapter III;

(c) Chapter IV;

(d) Chapter V;

(e) Chapter VI;

(f) Chapter VII except section 31; and

(g)(a) Chapter VIII.

Sub-section (1) shall or apply only where it can be demonstrated that the processing is in compliance with any code of ethics issued by— 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

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

31. ~~Manual processing by small entities.—~~

- ~~(1) Subject to any law for the time being in force, where personal data is processed through means other than automated means by a small entity, the following provisions of the Act shall not apply—~~
 - ~~(a) Sections 8, 9 and 10 in Chapter II;~~
 - ~~(b) Clause (c) of sub-section (1) of section 24, and sections 26 and 27 in Chapter VI; and~~
 - ~~(c)(a) Section 29 to section 36, and sections 38 and 39 in Chapter VII.~~
- ~~(2) For the purposes of sub-section (1), a small entity shall be any data fiduciary which—~~
 - ~~(a) did not have a turnover of more than twenty lakh rupees or such other lower amount as may be prescribed by the Central Government in the preceding financial year;~~
 - ~~(b) does not collect personal data for the purpose of disclosure to any other individuals or entities, including other data fiduciaries or processors; and~~
 - ~~(c)(a) did not process personal data of more than one hundred data principals in any one day in the preceding twelve calendar months.~~

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

CHAPTER X

~~DATA PROTECTION AUTHORITY OF INDIA~~

~~Establishment and incorporation of Authority.—~~

~~41. (1) The Central Government shall, by notification, establish₂ 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.—Members.~~

~~42. (1) The Authority shall consist of a chairperson and six whole-time members 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~~Chairperson and the ~~members~~Members of the Authority shall be appointed by the Central Government on the recommendation made by a selection committee consisting of—

~~the Chief Justice of India or a judge of the Supreme Court of India nominated by the Chief Justice of India~~ (a) the Cabinet Secretary, who shall be ~~the chairperson~~Chairperson of the selection committee;

~~(d)—the Cabinet~~(b) the Secretary; and

~~one expert of repute as mentioned in sub-section (6), to be nominated by the Chief Justice Government of India or a judge of the Supreme Court of India nominated by in the Chief Justice of India, in consultation Ministry or Department dealing with the Cabinet Secretary. 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~~Selection Committee for recommending the names under sub-section (2) shall be such as may be prescribed.

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

(5) A vacancy caused to the office of the ~~chairperson~~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.

(3) ~~The Central Government shall maintain a list of at least five experts who have specialised knowledge of, and professional experience in the field of data protection, information technology, data management, data science, cyber and internet laws, and related subjects.~~

Terms and conditions of appointment.—

43. (1) The ~~chairperson~~Chairperson and the ~~members~~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~~Chairperson and the ~~members~~Members of the Authority shall be such as may be prescribed and shall not be varied to their disadvantage during their term.

(3) The ~~chairperson~~Chairperson and the ~~members~~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~~Chairperson or a ~~member~~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 ~~members~~.—Chairperson or other Members.

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

(a) has been adjudged ~~as~~ an insolvent;

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

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

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

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

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

Powers of ~~the chairperson.~~—Chairperson.

45. The ~~chairperson~~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 ~~the~~this Act.

Meetings of ~~the~~Authority.—

46. (1) The ~~chairperson~~Chairperson and ~~members~~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~~Chairperson is unable to attend any meeting of the Authority, ~~any~~ other member chosen by the ~~members~~Members present at the meeting, shall preside ~~at~~ the meeting.

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

(4) Any ~~member~~Member who has any direct or indirect pecuniary interest in any matter coming ~~up~~ for consideration at a meeting of the Authority shall disclose the nature of ~~her~~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 ~~the~~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~~Chairperson or member; or;

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

Officers and ~~Employees~~other employees of ~~the~~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~~

32. ~~Grants by Central Government.—~~

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

33. ~~Accounts and Audit—~~

- ~~(1) The Authority shall maintain proper accounts and other relevant records and prepare an annual statement of accounts in such form as may be prescribed by the Central Government in consultation with the Comptroller and Auditor General of India.~~
- ~~(2) The accounts of the Authority shall be audited by the Comptroller and Auditor General of India at such intervals as may be prescribed and any expenditure incurred by her in connection with such audit shall be reimbursed to her by the Authority.~~
- ~~(3) The Comptroller and Auditor General of India and any other person appointed by her in connection with the audit of the accounts of the Authority shall have the same rights and privileges and authority in connection with such audit as the Comptroller and Auditor General of India generally has in connection with the audit of the Government accounts and, in particular, shall have the right to demand the production of books, accounts, connected vouchers and other documents and papers, and to inspect any of the offices of the Authority.~~
- ~~(4) The accounts of the Authority as certified by the Comptroller and Auditor General of India or any other person appointed by the Comptroller and Auditor General of India in this behalf together with the audit report thereon shall be forwarded annually to the Central Government and the Central Government shall cause the same to be laid before each House of the Parliament.~~

34. ~~Furnishing of returns, etc. to Central Government.—~~

- ~~(1) The Authority shall furnish to the Central Government at such time and in such form and manner as may be prescribed or as the Central Government may direct, such returns and statements and such particulars in regard to any proposed or existing programme for the promotion and development of protection of personal data, as the Central Government from time to time, require.~~
- ~~(2) The Authority shall prepare once every year in such form and at such time as may be prescribed, an annual report giving a summary of its activities during the previous year and copies of the report shall be forwarded to the Central Government.~~
- ~~(3) A copy of the report received under sub-section (2) shall be laid, as soon as may be after it is received, before each House of the Parliament.~~

Powers and ~~Functions~~functions of the 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 ~~of/about~~ data protection.

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

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

(a) specifying reasonable purposes for which personal data may be processed under

~~section 17 of this Act;~~

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

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

~~(c) specifying the circumstances where a data protection impact assessment may be required to be undertaken in accordance with section 33 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) specifying the criteria for assigning a rating in the form of a data trust score by a data auditor having regard to the factors mentioned in sub-section (2) of section 35;~~

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

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

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

~~(f) classification of data fiduciaries;~~

~~(g) monitoring cross-border transfer of personal data under section 41 of this Act;~~

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

(i) promoting ~~public~~ awareness and understanding of the risks, rules, safeguards and rights in respect of protection of personal data, ~~including issuance of any public statement setting out trends in, or specific instances of, contravention of the amongst data fiduciaries and data principals;~~

~~provisions of this Act by a data fiduciary or a class of data fiduciaries, as the case may be;~~

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

(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 ~~Parliament,~~ Central Government, State Government and any ~~regulatory or statutory other~~ authority on measures ~~that must required to be undertakentaken~~ to promote protection of personal data and ensuring consistency of application and enforcement of this Act;

~~(g) issuing guidance on any provision under this Act either on its own or in response to any query received from a data fiduciary where the Authority considers it necessary;~~

subject always to the provisions of this Act;

~~(h) advising the Central Government on the acceptance of any relevant international instrument relating to protection of personal data;~~

~~(m) specifying fees and other charges for carrying out the purposes of this Act;~~

~~(n) receiving and handling inquiring complaints under the provisions of this Act; and~~

~~(v) calling for information from, conducting inspections and inquiries into the affairs of data fiduciaries in accordance with the provisions of this Act;~~

~~(w) preparation and publication of reports setting out the result of any inspection or inquiry and any other comments that the Authority deems to be in public interest; and~~

~~(o) performing such other functions, including maintaining, updating and submitting any records, documents, books, registers or any other data, as may be prescribed.~~

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

~~(a) the discovery and production of books of account and other documents, at such place and at such time as may be specified;~~

~~summoning and enforcing the attendance of persons and examining them on (3) oath;~~

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

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

~~(d)(a) any other matter which may be prescribed.~~

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 as per under any law to do so, or where it is required to carry out its function under clause (w) of sub-section (2).

Codes of ~~Practise.~~ practice.

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

(2) ~~Notwithstanding anything contained in~~ sub-section (1), the Authority may ~~also~~ approve, ~~and issue codes~~ any code of practice ~~submitted by~~ submitted by an industry or trade association, an association representing the interest of data principals, any sectoral regulator or statutory ~~authority~~ Authority, or any departments or ministries of the Central or State Government.

(5) (3) The Authority shall ensure transparency ~~while~~ and compliance with the obligations of data fiduciary and the rights of the data principal under this Act while specifying or approving ~~or issuing any code of practice under this section in accordance with sub-section (4).~~

~~Any~~ code of practice, ~~whether under this section.~~

(4) A code of practice under sub-section (1) or sub-section (2), shall not be issued unless the Authority has ~~undertaken a requisite~~ made consultation ~~process~~ with ~~relevant~~ the sectoral regulators and

~~other~~ stakeholders including the public and has followed ~~the such~~ procedure ~~for issuance of such code of practice~~, as may be prescribed.

(6) ~~(5)~~ A code of practice issued under this section shall not derogate ~~from the~~ ~~from the~~ provisions of this ~~Act or any applicable law~~.

~~Without prejudice to sub-sections (1) or (2), Act or any other provision of law for the time being in force.~~

~~(6)~~ The code of practice under this Act, ~~the Authority~~ may ~~issue codes of practice in respect of~~ include the following matters—, namely:—

~~(a)~~ requirements for notice ~~under section 8 of this Act~~ ~~under section 7~~ including any model forms or guidance relating to notice;

~~(b)~~ measures for ensuring quality of personal data processed under section ~~9 of this Act~~ ~~8~~;

~~(c)~~ measures pertaining to the retention of personal data under section ~~10 of this Act~~ ~~9~~;

~~conditions~~ ~~(d)~~ manner for ~~obtaining~~ valid consent under section ~~12 of this Act~~ ~~11~~;

~~(e)~~ processing of personal data under section ~~15 of this Act~~ ~~12~~;

~~(f)~~ activities where processing of personal data may be undertaken ~~under section 17~~ ~~under section 14~~;

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

~~(h)~~ processing of personal data under any other ground for processing, including processing of personal data of children and ~~development of appropriate age-verification mechanisms under section 23 and mechanisms for processing personal data on the basis of consent of users incapable of providing valid consent under this Act~~; ~~under this Act~~;

~~(i)~~ exercise of any right by data principals under Chapter ~~VI of this Act~~ ~~V~~;

~~(j)~~ the standards and means by which a data principal may avail the right to data portability under section ~~26 of this Act~~ ~~19~~;

~~(k)~~ transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under Chapter ~~VII of this Act~~ ~~VI~~;

~~(l)~~ standards for security safeguards to be maintained by data fiduciaries and data processors under section ~~31 of this Act~~ ~~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 ~~32 of this Act~~ ~~25~~;

~~(p)~~ manner in which data protection impact assessments may be carried out by the data fiduciary or a class thereof under section ~~33 of this Act~~ ~~27~~;

~~cross-border~~ ~~(q)~~ transfer of personal data ~~outside India~~ pursuant to section ~~41 of this Act~~ ~~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 ~~45 of this Act~~ ~~38~~; and

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

- (7) ~~Non-compliance by the data fiduciary or data processor with any code of practice issued under this section and applicable to it may be considered by the Authority, or any court, tribunal or statutory body, while determining whether such data fiduciary or data processor has violated the provisions of this Act.~~
- (8) ~~Nothing contained in sub-section (7) shall prevent a data fiduciary or data processor from demonstrating before the Authority, or any court, tribunal or statutory body, that it has adopted an equivalent or a higher standard than that stipulated under the relevant code of practice.~~

(7) The Authority may review, modify or revoke a code of practice issued under this section in ~~thesuch~~ manner as may be prescribed.

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

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 ~~data fiduciaries or data processors generally, or to any data fiduciary or data processor in particular, and such data fiduciaries or data processors, as the case may be, any data fiduciary or data processor who~~ shall be bound to comply with such directions.

(2) No ~~such~~ direction shall be issued under sub-section (1) unless the Authority has given a reasonable opportunity of being heard to the data fiduciaries or data ~~processors-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 ~~thinks~~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~~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 ~~as per~~under sub-section (1), it ~~must~~shall provide a ~~written~~ notice in writing to the data ~~fiduciary or~~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~~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, ~~time~~ frame~~the period~~ within which such information is ~~required~~ to be furnished and the form in which such information may be provided.

Power of Authority to conduct inquiry.—

53. (1) The Authority may ~~conduct an inquiry where, 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~~fiduciary or data processor are being conducted in a manner which is detrimental to the interest of data principals; or

any data fiduciary or (b) any data fiduciary or data processor has ~~violated~~contravened any of the provisions of this Act or the rules ~~prescribed~~, or ~~the~~ regulations ~~specified~~made thereunder, or ~~directions issued by any direction of~~ the Authority ~~thereunder~~.

(2) For the ~~purpose~~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~~fiduciary or data processor and to report to the Authority on any inquiry made.

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

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

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

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

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

(8) Notwithstanding anything contained in any other law for the time being in force, while exercising the powers under this section, the Authority or the Inquiry Officer, as the case may be, shall have the same powers as are vested in a civil court under the Code of Civil Procedure, 1908 while trying a suit, in respect of the following matters, namely—

(a) the discovery and production of books of account and other documents, at such place and at such time as may be specified;

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

~~(10) Without prejudice to any other power set out in this Act or under any other law, any Inquiry Officer directed to make an inquiry may examine on oath, any officer, employee or other person acting under the direct authority of the data fiduciary or the data processor, or a service provider, or a contractor where services are being obtained by or provided to the data fiduciary or data processor, as the case may be, in relation to the business or activity of the data fiduciary or data processor.~~

(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 64~~53~~, the Authority may, after giving such opportunity to the data ~~fiduciary or~~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~~ 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~~ 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 ~~think~~ deems fit.

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

Search and ~~Seizure.~~ seizure.

(11) ~~55.~~ (1) Where ~~in the Authority~~ course of inquiry under section 53, the Inquiry Officer has reasonable ~~grounds~~ ground to believe that—

~~(a) any person who has been required under sub-section (5) of section 64 to produce, or cause to be produced, any books, registers, documents, records or data in her custody or power is likely to omit or fail, or has omitted or failed, to do so; or~~

~~(b) any books, registers, documents, records or data belonging to any person as mentioned in clause (a) of sub-section (1) therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed; or~~

~~(c) a contravention of any provision of this Act has been committed or is likely to be committed by a data fiduciary;~~

~~it may authorise any officer of, the Authority not below the rank equivalent to that of a Gazetted Officer of the Central Government (hereinafter referred to as “Authorised Inquiry Officer”) may make an application to—~~

~~(i) enter and search any building or place where she has reason to suspect that such books, registers, documents, records or data are kept;~~

~~(ii) break open designated court, as may be notified by the lock of any box, locker, safe, almirah or other receptacle Central Government, for exercising an order for the powers conferred by clause (i) where the keys thereof are not available;~~

~~(iii) access any computer, computer resource, or any other device containing or suspected to be containing data;~~

~~seize all or any~~ seizure of such books, registers, documents, and records ~~or data found as a result of such search;~~

~~(iv) (i) place marks of identification on such books, registers, documents, records or databases or make extracts or copies of the same.~~

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

~~The Authorised (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 it is not practicable to seize any such book, register, document, record or data such books, registers, documents and records are kept;~~

~~(b) to search that place or those places in the manner specified in sub-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 (1), serve an order on the for such period not later than the conclusion of the inquiry as it considers necessary and thereafter shall return the same to the person who is in immediate possession or control thereof that such person shall not remove, part with, from whose custody or power they were seized and inform the designated court of such return.~~

- ~~(12) (5) Save as otherwise deal with it except with the previous permission of such officer and such officer may take such steps as may be necessary for ensuring compliance with this sub-provided in this section.~~
- ~~(13) The Authorised Officer may, during the course of the, every search or seizure, examine on oath any person who is found to be in possession or control of any books, registers, documents, records or data, and any statement made by such person during such examination may thereafter be used in evidence in any proceeding under this Act.~~
- ~~(14) The books, registers, documents, records or data seized under sub-under this section (1) shall not be retained by the Authorised Officer for a period exceeding six months from the date of the seizure unless the reasons for retaining the same are recorded by her in writing and the approval of the Authority for such retention is obtained.~~
- ~~(15) The Authority shall not authorise the retention of the books, registers, documents, records or data for a period exceeding thirty days after all the proceedings under this Act, for which the said books, registers, documents, records or data are relevant, are completed.~~
- ~~(16) The person from whose custody the books, registers, documents, records or data are seized under sub-section (1) may make copies thereof, or take extracts therefrom, in the presence of the Authorised Officer or any other person appointed by her in this behalf at such place and time as the Authorised Officer may designate in this behalf.~~
- ~~(17) If a person legally entitled to the books, registers, documents, records or data seized under sub-section (1) objects for any reason to the approval given by the Authority under sub-section (5), such person may make an application to the Appellate Tribunal stating therein the reason for such objection and requesting for the return of the books, registers, documents, records or data.~~
- ~~(18) On receipt of the application under sub-section (8), the Appellate Tribunal may, after giving the parties an opportunity of being heard, pass such order as it thinks fit including any order prohibiting the destruction or alteration of such books, registers, documents, records or data.~~

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

- (19) ~~Without prejudice to the generality of the foregoing, rules may be prescribed in relation to the process for search and seizure under this section and in particular may provide for—~~
- ~~(a) obtaining ingress into such building or place to be searched where free ingress thereto is not available;~~
 - ~~(b) obtaining access to a computer, computer resource, or any other device containing or suspected to be containing data, where such access is not available;~~
 - ~~(c)(a) ensuring safe custody of any books, registers, documents, records or data seized under this section.~~

~~Coordination~~ Co-ordination between ~~the~~ 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.

35. Appointment of Adjudicating Officer.—

- ~~(1) Without prejudice to any other provision of this Act and for the purpose of imposing of penalties under section 69 to section 73 or awarding compensation under section 75, the Authority shall have a separate adjudication wing.~~
- ~~(2) The Central Government shall, having regard to the need to ensure the operational segregation, independence, and neutrality of the adjudication wing, prescribe—~~
 - ~~(a) number of Adjudicating Officers;~~
 - ~~(b) qualification of Adjudicating Officers;~~
 - ~~(c) manner and terms of appointment of Adjudicating Officers ensuring independence of such officers;~~
 - ~~(d) jurisdiction of Adjudicating Officers;~~
 - ~~(e) procedure for carrying out an adjudication under this Act; and~~
 - ~~(f)(a) other such requirements as the Central Government may deem fit.~~
- ~~(3) The Adjudicating Officers shall be persons of ability, integrity and standing, and must have specialised knowledge of, and not less than seven years professional experience in the fields of constitutional law, cyber and internet laws, information technology law and policy, data protection and related subjects.~~

CHAPTER XIX PENALTIES AND REMEDIES COMPENSATION

Penalties.— for contravening certain provisions of the Act.

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

(a) obligation to take prompt and appropriate action in response to a data security breach under section ~~32 of this Act~~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 ~~33 of this Act~~27;

(d) obligation to conduct a data audit by a significant data fiduciary under section ~~35 of this Act~~29;

~~(a) — (c) appointment of a data protection officer by a significant data fiduciary under section 36 of this Act;~~

~~failure to register with the Authority significant data fiduciary under sub-section (2) of section 38.30.~~

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

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

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

~~(c) — processing of sensitive personal data in violation of the provisions of Chapter IV of this Act;~~

~~(b) processing of personal data of children in violation of the provisions of Chapter ~~VIV~~;~~

~~(c) failure to adhere to security safeguards as per section ~~31 of this Act~~24; or~~

~~(d) transfer of personal data outside India in violation of ~~section 41 the provisions~~ of this Act. Chapter VII.~~

~~Explanation I. 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.

~~Explanation II. For the purposes of this section,— (b) it is hereby clarified that total that total~~ worldwide turnover in relation to a data ~~fiduciary is~~ 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—

~~the alignment~~ (i) the alignment of the overall economic interests of the data fiduciary and the group entity;

~~the relationship~~ (ii) the relationship between the data fiduciary and the group entity specifically in relation to the processing activity undertaken by the data fiduciary; and

~~the degree~~ (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 ~~VI.~~V.

58. Where, any data fiduciary, without any reasonable explanation, fails to comply with any request made by a data principal under Chapter ~~VI of this Act~~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 ~~prescribed~~ or regulations ~~specified~~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 ~~the~~ Authority.~~—.~~

60. If any data ~~fiduciary or~~fiduciary or data processor fails to comply with any direction issued by the Authority under section ~~62 or~~51 or order issued by the Authority under section ~~65, as applicable~~54, such data ~~fiduciary or~~fiduciary or data processor shall be liable to a penalty which, ~~in case of a data fiduciary~~ may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two ~~crore rupees, and~~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 ~~prescribed~~ or regulations ~~specified~~made thereunder ~~as~~ applicable to such person, for which no separate penalty has been provided, then, such person shall be liable to a penalty ~~subject~~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 ~~all~~ other cases.

Adjudication~~Appointment~~ of Adjudicating Officer.

62. (1) For the purpose of adjudging the penalties under sections 57 to 61 or 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 ~~conducting~~ an inquiry made in such manner as may be prescribed, and the data fiduciary or data ~~processor or 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 ~~violation~~contravention of the provisions of this Act, ~~which a penalty may be imposed under section 69 to section 73,~~ the Adjudicating Officer may impose such penalty ~~in accordance with the provisions of the appropriate specified under relevant~~ section.

(4) While deciding whether to impose a penalty under sub-section (3) ~~of this section~~ and in determining the quantum of penalty under ~~section 69 to section 73~~sections 57 to 61, the Adjudicating Officer shall have due regard to the following factors, ~~as may be applicable—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 prescribed~~ or regulations ~~specified hereunder~~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 37~~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 ~~31~~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 ~~pursuant to by making~~ a complaint ~~instituted to the Adjudicating Officer~~ in such form and manner as may be prescribed ~~before an Adjudicating Officer~~.

(3) Where there are one or more data principals or any identifiable class of data principals who have suffered harm as a result of any ~~violation~~ ~~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 ~~whether~~ to award compensation and the amount of compensation under this section, the Adjudicating Officer shall have ~~due~~ regard to the following factors, namely:—

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

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

(c) intentional or negligent character of the violation;

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

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

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

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

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

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

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

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

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

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.

36. Data Protection Funds.—

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

~~all Government grants, fees and charges received by the Authority~~ Recovery of amounts.

- (a) ~~66. (1) The amount of any penalty imposed or compensation awarded under this Act; and~~
- (b) ~~(a) all sums received by the Authority from such other source as, if not paid, may be decided upon by the Central Government, but which shall not include the sums mentioned in sub-section (3).~~
- (c) ~~The Data Protection Authority Fund shall be applied for meeting—~~
- (i) ~~the salaries, allowances and other remuneration of the chairperson, members, officers, employees, consultants and experts appointed by the Authority; and~~

~~the other expenses of the Authority in connection with the discharge~~ recovered as if it were an arrear of its functions and for the purposes of this Act and revenue.

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

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

37. Recovery of Amounts.—

- (1) ~~The Authority shall, by an order in writing, appoint at least one officer or employee as a Recovery Officer for the purpose of this Act.~~
- (2) ~~Where any person fails to comply with—~~
- (a) ~~an order of the Adjudicating Officer imposing a penalty under the provisions of this Act; or~~
- (b) ~~(a) an order of the Adjudicating Officer directing payment of compensation under the provisions of this Act,~~

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

- (i) ~~attachment and sale of the person's movable property;~~
- (ii) ~~attachment of the person's bank accounts;~~
- (iii) ~~attachment and sale of the person's immovable property;~~
- (iv) ~~arrest and detention of the person in prison;~~
- (v) ~~(i) appointing a receiver for the management of the person's movable and immovable properties.~~
- (3) ~~For the purpose of such recovery, the provisions of section 220 to section 227, and sections 228A, 229 and 232, the Second and Third Schedules of the Income Tax Act, 1961 (43 of 1961) and the Income Tax (Certificate Proceedings) Rules, 1962, as in force from time to time, in so far as may be, shall apply with necessary modifications as if the~~

~~said provisions and rules—~~

~~(a) were the provisions of this Act; and~~

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

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

~~(a) property or monies transferred by the person without adequate consideration;~~

~~(b) such transfer is made:~~

~~(i) on or after the date on which the amount in the certificate drawn up under section 222 of the Income Tax Act, 1961 (43 of 1961) had become due; and~~

~~(ii)(i) to the person's spouse, minor child, son's wife or son's minor child.~~

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

~~(5)(4) The Recovery Officer shall be empowered to seek the assistance of the local district administration while exercising the powers under this section.~~

CHAPTER ~~XHXI~~ 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 39;63; and~~

~~(a)—(d) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 65;~~

~~(b) hear and dispose of an application under sub-section (9) of section 66;~~

~~(c) hear and dispose of any appeal from an order of the an Adjudicating Officer under sub-section (5) of section 74; and~~

~~hear and dispose of any appeal from an order of an Adjudicating Officer under sub-section (7) of section 7564.~~

~~(2) The Appellate Tribunal shall consist of a chairpersonChairperson and such number of not more than members as mayto be notified by the Central Governmentappointed.~~

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

~~Where(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 ~~as envisaged~~ under this Act, then, the Central Government may notify such ~~existing~~ body to act as the Appellate Tribunal under this Act.

Qualifications, appointment, term, conditions of service of ~~members~~.—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 qualifications, manner of appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairpersonChairperson and any member of the Appellate Tribunal.

~~(6)(5) Neither the salary and allowances nor the other terms and conditions of service of the chairperson or member of the Appellate Tribunal may be varied to her disadvantage after her appointment.~~

Vacancies.—

69. If, for reason other than temporary absence, any vacancy occurs in the office of the chairpersonChairperson 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 chairpersonChairperson.

(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~~.—Benches.

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

(2) Where benchesBenches of the Appellate Tribunal are constituted under sub-section (1), the chairpersonChairperson may, from time to time, by notification, make provisions as to the distribution of the business of the Appellate Tribunal amongst the benchesBenches, transfer of membersMembers between benchesBenches, 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 chairpersonChairperson may desire to be heard, or on the chairperson'sChairperson's own motion without such notice, the chairpersonChairperson of the Appellate Tribunal may transfer any case pending before one benchBench, for disposal, to any other benchBench.

Appeals to Appellate Tribunal.—

72. (1) Any person aggrieved by the decision of the Authority, may fileprefer an appealor application, as the case may be, withappeal 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:-

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

Notwithstanding sub-section (2), Provided that the Appellate Tribunal may entertain any appeal-or application, as the case may be, after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period.

(2) On receipt of an appealor application, as the case may be, 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 thinksdeems 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 or application preferred under this section, on its own motion or otherwise, call for the records relevant to disposing of such appeal or application and make such orders as it thinks fit.

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 (5 of 1908),, but shall be guided by the principles of natural justice and, subject to the other provisions of this Act, the Appellate Tribunal shall have powers to regulate its own procedure.

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

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

(b) requiring the discovery and production of documents;

(c) receiving evidence on affidavits;

(d) subject to the provisions of section 123 and section 124 of the Indian Evidence Act, 1872 (1 of 1872),, requisitioning any public record or document or a copy of such record or document, from any office;

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

(f) reviewing its decisions;

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

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

(i) any other matter which may be prescribed.

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

Penal Code, ~~1860 (45 of 1860)~~ and the Appellate Tribunal shall be deemed to be a civil court for the purposes of section 195 and Chapter XXVI of the Code of Criminal Procedure, 1973 ~~(2 of 1974)~~.

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 ~~of India~~.—

75. (1) Notwithstanding anything contained in the Code of Civil Procedure, 1908 ~~(5 of 1908)~~ or in any other law, an appeal shall lie against any order of the Appellate Tribunal, not being an interlocutory order, to the Supreme Court ~~of India~~ on any substantial question of law.

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

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

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

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 ~~her~~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

38. ~~Obtaining, transferring or selling of personal data contrary to the Act.—~~

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

~~(a) obtains personal data; or~~

~~(b) discloses personal data; or~~

~~(c) transfers personal data to another person; or~~

~~(d)(a) sells or offers to sell personal data to another person,~~

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

39. ~~Obtaining, transferring or selling of sensitive personal data contrary to the Act.—~~

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

~~(a) obtains sensitive personal data; or~~

~~(b) discloses sensitive personal data; or~~

~~(c) transfers sensitive personal data to another person; or~~

~~(d) sells or offers to sell sensitive personal data to another person,~~

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

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

82. (1) Any person who, knowingly or intentionally ~~or recklessly~~—

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

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

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

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

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

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

Offences to be cognizable and non-bailable.—

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

40. ~~Power to investigate offences.—~~

~~Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), a police officer not below the rank of Inspector~~(2) No court shall investigate 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.

~~(1)~~ ~~(2)~~ Nothing contained in sub-section (1) shall render any such person liable to any punishment provided in this Act, if ~~shehe~~ proves that the offence was committed without ~~her his~~ knowledge or that ~~shehe~~ 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 ~~Central or State Government departments.~~—

~~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 ~~Central or State Government, or any authority of the State, by whatever name called,~~ the head of ~~thesuch~~ 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 ~~shehe~~ proves that the offence was committed without ~~herhis~~ knowledge or that ~~shehe~~ had exercised all due diligence to prevent the commission of such offence.

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

CHAPTER XIV TRANSITIONAL PROVISIONS

41. ~~Transitional provisions and commencement.~~—

~~(1) For the purposes of (4) Notwithstanding anything in this Chapter, the term „notified date” refers to the date notified by the Central Government under sub-section (3), the provisions of the Code of section 1.~~

~~The notified date Criminal Procedure, 1973 relating to public servants shall be any date within twelve months from the date of enactment of this Act continue to apply.~~

~~(2) The following provisions shall come into force on the notified date—~~

~~(a) Chapter X;~~

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

CHAPTER ~~XV~~XIV MISCELLANEOUS

Power of Central Government to issue directions ~~in certain circumstances.—~~.

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:

~~Any direction issued by the Central Government~~ Provided that the Authority shall, as far as practicable, be given, ~~after providing~~ an opportunity to ~~the Authority to~~ express its views ~~in~~ before any direction is given under this ~~regards~~ sub-section.

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

Members, etc., to be public servants.—

87. The ~~chairperson, members~~ Chairperson, Members, officers and employees of the Authority and the Appellate Tribunal shall be deemed, when acting or purporting to act in pursuance of

any of the provisions of this Act, to be public servants within the meaning of section 21 of the Indian Penal Code, ~~1860 (45 of 1860)~~.

Protection of action taken in good faith.—

~~88.~~ 88. No suit, prosecution or other legal proceedings shall lie against the Authority or its ~~chairperson~~ 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.~~ 89. Notwithstanding anything contained in the Income Tax Act, 1961 ~~(43 of 1961)~~ or any other enactment for the time being in force relating to tax on income, profits or gains, as the case may be, the Authority shall not be liable to pay income tax or any other tax in respect of its income, profits or gains derived.

Delegation.—

~~90.~~ 90. The ~~chairperson of the~~ Authority may, by general or special order in writing delegate to any member or officer of the Authority subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act, except the powers under section ~~10894~~, as it may deem necessary.

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

~~42.~~ 42. 91. (1) Nothing in this Act shall prevent the Central Government from framing of any policy ~~Power to remove difficulties.—~~

- ~~(1) If any difficulty arises in giving effect to the provisions of this Act, the Central Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty.~~
- ~~(2) No such order shall be made under this section after the expiry of five years from the commencement of this Act.~~
- ~~(3) Every order made under this section shall be laid, as soon as may be after it is made, before each House of Parliament.~~

~~43.~~ 43. Power to exempt certain data processors.—

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

~~44.~~ 44. No application to non-personal data

~~Nothing contained in this Act shall affect the power of the Central Government to formulate appropriate policies for the digital economy, including measures for its growth, security, integrity, prevention of misuse, insofar as such policies~~ 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 ~~purposes~~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;

~~(a)—(c)~~ (c) the form and manner in which an application may be made to exercise the right under sub-section

~~(4) of Section 27;~~

(2), and the manner of review of the order passed by the Adjudicating Officer under sub-section ~~(54)~~ of section 2720;

(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 ~~with the adjudication wing~~ may be filed under sub-section (4) of section 3932;

~~the countries, sectors within~~ (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 4134;

~~(b)—the time period of notification to the Authority under sub-section (4) of section 41 of the transfer of personal data to a particular country as permitted under clause (b) of sub-section (3) of section 41;~~

~~(c)—the amount of turnover for a data fiduciary to qualify as a small entity under clause (a) of sub-section (2) of section 48;~~

(g) the place of ~~establishment and incorporation of the~~ head office of the Authority ~~as~~ under sub-section (3) of section 4941;

(h) procedure to be followed by the selection ~~committee under~~ committee under sub-section (3) of section 5042;

(i) the salaries and allowances payable to, and other terms and conditions of service of the ~~chairperson~~ Chairperson and the ~~members~~ Members of the Authority under sub-section (2) of section 5143;

(j) the ~~time~~ time and ~~places~~ 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 5446;

(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;

~~(d)—(v) the form of accounts, other relevant records and annual statement of accounts under sub-section (1) of section 58;~~

~~), the intervals at which the accounts of the Authority ~~will~~shall be audited under sub-section (2) of section 5880;~~

~~(w) the time in which, and the form and manner in ~~whichthe~~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 5981;~~

~~(e)—(x) the ~~time~~manner in which, and the form in which an annual report is to be prepared by the Authority and forwarded to the Central Government ~~may issue a direction, including the specific purposes for which data is sought~~ under sub-section (2) and the form of section 59;~~

~~(f)—other functions~~disclosure~~ of the Authority~~such directions~~ under clause (x) of sub-section (2) of section 60;~~

~~other matters under clause (e) of sub-section (3) of section 60 in respect of which the Authority shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit;91; or~~

~~(g)—the procedure of issuance of a code of practice under sub-section (4) of section 61;~~

~~(h)—the manner in (y) any other matter which the Authority may review, modify or revoke a code of practice under sub-section (9) of section 61;~~

~~(i)—the manner in which the Authority shall maintain a register containing details of the codes of practice under sub-section (10) of section 61;~~

~~(j)—the process for search and seizure under sub-section (11) of section 66;~~

- ~~(k) the number of Adjudicating Officers that the adjudication wing will consist of under sub-section (2) of section 68;~~
- ~~(v) the qualification, manner and terms of appointment, and jurisdiction of Adjudicating Officers is require to ensure their independence, and the procedure for carrying out adjudication under this Act and other such requirements as deemed fit by the Central Government under sub-section (2) of section 68;~~
- ~~(w) the manner in which the Adjudicating Officer will conduct an inquiry under sub-section (1) of section 74;~~
- ~~(x) the form and manner of instituting a complaint under sub-section (2) of section 75;~~
- ~~(y) the procedure for hearing of a complaint and the limit on the amount of compensation under sub-section (8) of section 75;~~
- ~~(z) the qualifications, appointment, term of office, salaries and allowances, resignation, removal and the other terms and conditions of service of the chairperson and any member of the Appellate Tribunal under sub-section (1) of section 80;~~
- ~~(aa) the procedure of filling of vacancies in the Appellate Tribunal under section 81;~~
- ~~(bb) the salaries and allowances and other conditions of service of the officers and employees of the Appellate Tribunal under sub-section (3) of section 82;~~
- ~~(cc) the form, manner and fee for filing an appeal be, or may be, prescribed, or application, as the case may be, with the Appellate Tribunal under sub-section (1) of section 84; and~~
- ~~(dd) other matters under clause (i) of sub-section (2) of section 85 in respect of which the Appellate Tribunal shall have powers under the Code of Civil Procedure, 1908 (5 of 1908) that are vested in a civil court while trying a suit 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 ~~prescribed~~made thereunder to carry out the ~~purposes~~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 ~~87~~;

(b) manner in which the personal data retained by the data fiduciary must be deleted under sub-section (4) of section ~~109~~;

~~(l) reasonable purposes for which personal data may be processed in accordance with sub-section (2) of section 17;~~

(c) ~~the safeguards as may be appropriate~~ for protecting the rights of data principals under sub-section (3) of ~~section 17~~section 14;

~~(m) any further categories of sensitive personal data and further grounds on which such data may be processed under sub-section (1) of section 22;~~

such (d) the additional safeguards or restrictions ~~applicable to processing~~ under sub-section (2) of section 15;

~~(e) the manner of obtaining consent of the parent or guardian of sensitive personal data and any further categories of personal data where there is repeated, continuous, systematic collection for the purposes of profiling and such additional safeguards required a child under sub-section (2), the manner of verification of age of a child under sub-section (3) of section 22;~~

~~(n) the additional factors necessary for determining the appropriateness of age verification mechanisms to be incorporated by a data fiduciary processing the personal data and sensitive personal data of children under sub-section (3) of section 23;~~

~~practices that may be undertaken by application of provision in modified form to data fiduciaries offering counseling or child protection services under sub-section (6) of section 23~~

~~(f) the time period within which a data fiduciary must comply with a acknowledge the receipt of request made 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) of section 28;~~

~~), and the time manner and the period within which a data principal may file a complaint under sub-section (4) of section 28~~

~~(p) the form in which the data fiduciary is required to make available to the data principal information under sub-section (1) of section 30;~~

~~(g) the manner for submission of privacy by which a data fiduciary shall notify the data principal regarding important operations in the processing of personal data design policy under sub-section (2) of section 30~~

~~(h) the manner of periodic review of security safeguards to be undertaken by the data fiduciary and the data processor 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 31~~

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

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

~~), and the manner in which the data fiduciary protection officer shall submit review the data protection impact assessment and submit to the Authority under sub-section (4) of section 33~~

~~any (k) the form and manner for maintaining the records, and any other aspect of processing for which records shall be maintained under clause (d) of sub-section (1) of section 34~~

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

~~(t) the (1) the other factors to be taken into consideration while evaluating the compliance of data fiduciaries with the provisions of this Act under clause (g) of sub-section (2) of section 35;~~

~~(u)); the form, manner and procedure by which data for conducting audits shall be conducted under sub-section (3); the manner of registration of auditors under sub-section (3) of section 35;~~

~~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 ~~3529~~;

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

~~(m) — the eligibility and qualification and experience of a data protection officer under sub-section (31) of section 3630;~~

~~(w) — the registration requirements of significant data fiduciaries under sub-section (2) of section 38;~~

~~the manner of certification and time(n) —~~ the period within which transfer of personal data shall be notified to the Authority under sub-section (~~63~~) of section ~~4134~~;

~~(o) — the provisions of the Act which may be exempted for different categories and the class of research, archival or statistical purposes which may be exempted under sub-section (1) of section 4538;~~

~~(aa-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 ~~5648~~;

~~(bb) any other fees and charges for carrying out purposes(q) —~~ the code of this Act practice under ~~clause (t) of~~ sub-section (~~21~~) of ~~Section 60~~ section ~~50~~;

~~(ee-r) —~~ the form and manner in which for providing information shall be provided to the authority Authority by the data fiduciary under sub-section (3) of ~~Section 63; and~~ section ~~52~~;

~~(dd-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~~ 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 ~~expressly~~ provided ~~under~~in this Act, the provisions of this Act shall have ~~an overriding effect to the extent that such provisions are notwithstanding anything~~ inconsistent ~~with therewith~~ any other law for the time being in force or any instrument having effect by virtue of any ~~such 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 (~~21 of 2000~~) shall be amended in the manner ~~set out~~specified in the ~~First Schedule to this Act~~.

45. ~~Amendment of Act 22 of 2005.—~~

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

THE ~~FIRST~~ SCHEDULE

(See ~~Section 11~~section 98)

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

~~Deletion~~Omission of section 43A.—

1. Section 43A of the Information Technology Act, 2000 (~~hereinafter~~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; RAVI SHANKAR PRASAD.

The 5th December, 2019.

[Note: Annexes Not Included]