REGULATION ON THE USAGE OF ARTIFICIAL INTELLIGENCE BILL, 2022

ARRANGEMENT OF SECTIONS

REGULATION ON THE USAGE OF ARTIFICIAL INTELLIGENCE BILL, 2022

An Act to provide legal recognition for the placing on the market, the putting into services of Artificial Intelligence systems intended to interact with the natural person, used to generate or manipulate images, audio or video content, remedies for unauthorised and harmful processing and to protect the privacy of individuals, to establish an Artificial Intelligence Protection Authority of India for the said purposes and for matters connected therewith or incidental thereto;

WHEREAS the General Conference of the United Nations Educational, Scientific and Cultural Organization, dated the 24th November 2021 has adopted the recommendation on the ethics of artificial intelligence;

AND WHEREAS the said recommendation states *inter alia*, that all States give favourable consideration to the said draft to ensure assumption of responsibility by all the stakeholders, including private sector companies in artificial intelligence technologies and bring the recommendation to the attention of the authorities, bodies, research and academies organisation, institutions and organisation in public, private and civil society sectors involved in artificial intelligence technologies in order to guarantee that the development and use of artificial intelligence are guided by both sound scientific research as well as ethical analysis, evolution and in support of the sustainable development goals;

AND WHEREAS it is considered necessary to give effect to the said recommendation and to promote efficient delivery of Government services by means of reliable artificial intelligence technologies.

BE it enacted by Parliament in the Seventy-third Year of the Republic of India as follows:–

CHAPTER I

PRELIMINARY

1. Short title, extent, commencement.—

(1) This Act may be called the Regulation on the Usage of Artificial Intelligence Act, 2022.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.

(3) It shall come into force on such date as the Central Government may, by notification, in the Official Gazette appoint.

2. Application of Act. —

(1) This Act applies to the following—

(a) Artificial intelligence system that is developed with a single or a constellation of technologies that enable machines to act with higher levels of intelligence and emulate the human capabilities of sense, comprehend and act;

(b) Artificial intelligence system that is used on a stand-alone basis or as a component of a product, irrespective of whether embedded or non-embedded; and

(c) Artificial intelligence system that is used for the processing of personal data by the State, any Indian company, any citizen of India or any person or body of persons incorporated or created under Indian law.

(2) Notwithstanding anything contained in sub-section (1), the Act shall apply to the artificial intelligence system that is used for processing of personal data by individual, company or data processors not present within the territory of India, if such processing is in connection with any business carried on in India, or any systematic activity of offering services within the territory of India.

Explanation.—In this clause,—

a) the expression “embedded” means the system which is physically integrated into the product.

b) the expression “non-embedded” means serving the functionality of the product without being integrated therein.

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

(1) "adjudicating officer" means the Adjudicating Officer appointed as such under sub-section (1) of section 45;

(2) “appellate tribunal” means the tribunal notified under Chapter VI of this Act;

(3) "authority" means the Artificial Intelligence Protection Authority of India established under sub-section (1) of section 19;

(4) "artificial intelligence" means software that is developed with one or more of the programming techniques for simulation of human intelligence, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with;

(5) “company” means as defined under Companies Act, 2013;

(6) "consent" means the consent referred to in section 9;

(7) "data" means as defined in sub-section (o) of section 2 of the Information Technology Act, 2000;

(8) "data auditor" means an independent data auditor referred to in section 15;

(9) "data principal" means the natural person or artificial person to whom the personal data relates;

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

(11) "de-identification" means the process by which a provider 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;

(12) "harm" includes—

(i) bodily or mental injury;

(ii) loss, distortion or theft of identity;

(iii) financial loss, loss of property;

(iv) loss of reputation, humiliation or any discriminatory treatment;

(v) loss of employment;

(vi) any subjection to blackmail or extortion, assault, criminal intimidation;

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

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

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

(13) "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;

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

(15) "person" means as defined in sub-section (31) of section 2 of the Income Tax Act, 1960;

(16) "personal data" means data about or relating to a natural or artificial person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such person, whether online or offline, or any combination of such features with any other information, any inference drawn from such data for the purpose of profiling and shall include which may reveal, be related to, or constitute—

(i) financial data;

(ii) health data;

(iii) official identifier;

(iv) sex life;

(v) sexual orientation;

(vi) biometric data;

(vii) genetic data;

(viii) transgender status;

(ix) intersex status;

(x) caste or tribe;

(xi) religious or political belief or affiliation;

Explanation.— For the purposes of this clause, the expressions,—

(a) "biometric data" means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operation;

(b) "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;

(c) "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;

(d) "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;

(e) "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;

(f) "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;

(17) “placing on the market” means the first making available of an artificial intelligence system on the market;

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

(19) "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;

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

(21) “provider” means a natural or legal person, public authority, agency or other body that, namely —

(a) develops an artificial intelligence system or that has an artificial intelligence system developed with a view to placing it on the market or putting it into service under its own name or trademark, whether for payment or free of charge; and

(b) determines the purpose and means of the processing of personal data;

(22) “putting into service” means the supply of an Artificial Intelligence system for first use directly to the user or for own use on the market for its intended purpose;

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

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

(25) "Sandbox" means an isolated virtual machine to test innovative technologies ;

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

(27) "State" means the State as defined under Article 12 of the Constitution of India, 1950 ;

(28) "user" means any natural or legal person, public authority, agency or other body using an Artificial Intelligence system under its authority, except where the Artificial Intelligence system is used in the course of personal non-professional activity.

CHAPTER II

OBLIGATIONS OF PROVIDER

4. Prohibiting high-risk Artificial Intelligence system. —

(1) The placing on the markets, putting into services, processing or use of an artificial intelligence system shall be considered prohibited when the following conditions are fulfilled, namely:—

a) the system deploys subliminal techniques beyond a person's consciousness in order to materially distort a person's behaviour in a manner that causes or is likely to cause that person or another person any harm;

b) the system exploits any of the vulnerabilities of a specific group of persons due to their age, physical or mental disability, in order to materially distort the behaviour of a person pertaining to that group in a manner that causes or is likely to cause that person or another person any harm;

c) the system violates the right to education and perpetuate patterns of discrimination to any person under Article15 of the Constitution of India or is likely to cause that person or another person any harm;

d) the system impact future prospects and livelihood to any person in employment, workers management and access to self-employment, notably for the recruitment and selection of persons, for making decisions on promotion and termination and for task allocation, monitoring or evaluation of persons in work-related contractual relationships;

e) the system collects or attempts to use personal data of natural persons without consent specified under sub-section(2) of section 9 except for the purpose specified in section 27.

(2) The provider shall be responsible under sub-section(1) with the provisions of this Act in respect of any processing, placing on the markets, or putting into services Artificial Intelligence system undertaken by it or on its behalf.

5. Limitation on the purpose of the processing of personal data.— Every person processing personal data of a data principal shall process such personal data—

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

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

6. Limitation on the collection of personal data.— The personal data of a data principal shall be collected only to the extent that is necessary for the purposes of processing such personal data.

7. Notice for collection or processing of personal data.—

(1) Every provider shall give to the data principal a notice, at the time of collection of the personal data, or if the data is not collected from the data principal, as soon as reasonably practicable, containing the following information, namely:—

(a) the purposes for which the personal data is to be processed;

(b) the nature and categories of personal data being collected;

(c) the identity and contact details of the provider and the contact details of the artificial intelligence protection officer, if applicable;

(d) the right of the data principal to withdraw his consent, and the procedure for such withdrawal, if the personal data is intended to be processed on the basis of consent;

(e) the source of such collection if the personal data is not collected from the data principal;

(f) the individuals or entities including other provider, with whom such personal data may be shared, if applicable;

(g) information regarding any cross-border transfer of the personal data that the provider intends to carry out, if applicable;

(h) the period for which the personal data shall be retained in terms of section 8 or where such period is not known, the criteria for determining such period;

(i) the procedure for grievance redressal under section 18;

(j) the existence of a right to file complaints to the Authority;

(k) any other information as may be specified by the regulations.

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

8. Restriction on retention of personal data.–

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

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

(3) The provider shall undertake a periodic review to determine whether it is necessary to retain the personal data in its possession.

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

9. Consent is necessary for processing personal data. —

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

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

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

(b) informed, having regard to whether the data principal has been provided with the information required under section 7;

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

(d) clear, having regard to whether it is indicated through an affirmative action that is meaningful in a given context; and capable of being withdrawn, having regard to whether the ease of such withdrawal is comparable to the ease with which consent may be given.

CHAPTER III

TRANSPARENCY AND ACCOUNTABILITY MEASURES

10. Privacy by design policy.—

(1) Every provider shall prepare privacy by design policy, containing—

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

b) the technology used in the placing on the markets, putting into services or processing of personal data is in accordance with commercially accepted or certified standards;

c) the protection of privacy throughout processing from the point of collection to deletion of personal data; and

d) the placing on the markets or putting into services and processing of personal data in a transparent manner prescribed under section 12.

(2) Subject to the regulations made by the Authority, the provider 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 subsection (1).

(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the provider and the Authority.

11. Artificial Intelligence regulatory sandboxes.—

(1) The Authority shall, for the purposes of encouraging innovation in artificial intelligence in the public interest create a Sandbox.

(2) Any provider whose privacy by design policy is certified by the Authority under sub-section (3) of section 10 shall be eligible to apply, in such manner as may be specified by regulations, for inclusion in the Sandbox created under sub-section (1).

(3) Any provider 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 provider in the Sandbox, specify—

(a) the term of the inclusion in the Sandbox, which may be renewed not more than twice, subject to a total period of thirty-six months;

(b) the safeguards including terms and conditions in view of the obligations under clause (c) including the requirement of consent of data principals participating under any licensed activity, compensation to such data principals and penalties in relation to such safeguards; and

(c) that the following obligations shall not apply or apply with a modified form to such provider, 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 8.

12. Transparency obligations for certain Artificial Intelligence System.—

(1) Every provider ensures that artificial intelligence systems intended to interact with natural persons are designed and developed in such a way that natural persons are informed that they are interacting with an artificial intelligence system unless this is obvious from the circumstances and the context of use.

(2) Artificial intelligence systems shall be accompanied by instructions for use in an appropriate digital format or otherwise that include concise, complete, correct and clear information that is relevant, accessible and comprehensible to users.

(3) Users of an artificial intelligence system that generates or manipulates images, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful(‘deep fakes’), shall disclose that the content has been artificially generated and manipulated.

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

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

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

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

(d) the right of data principal to file a complaint against the provider to the Authority;

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

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

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

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

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

(8) 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 provider which enables a data principal to gain, withdraw, review and manage his consent through an accessible, transparent and interoperable platform.

13. Security safeguards. —

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

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

(b) steps necessary to protect the integrity of personal data or artificial intelligence system ; and

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

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

14. Reporting of the personal data breach. —

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

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

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

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

(c) possible consequences of the breach; and

(d) action being taken by the provider to remedy the breach.

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

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

(5) Upon receipt of a notice, the Authority shall determine whether such breach should be reported by the provider or data processor 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.

15. Data protection impact assessment.—

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

(2) The Authority may, by regulations specify, such circumstances, or class of providers, or processing operation where such data protection impact assessment shall be mandatory, and also specify the instances where a data auditor shall be engaged by the providers to undertake a data protection impact assessment.

(3) A data protection impact assessment shall, *inter alia*, contain—

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

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

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

(4) Upon completion of the data protection impact assessment, the artificial intelligence protection officer shall review the assessment and submit the assessment with his finding to the Authority in such a 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 provider to cease such processing or direct that such processing shall be subject to such conditions as the Authority may deem fit.

16. Maintenance of records.—

(1) The significant provider 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 7;

(b) periodic review of security safeguards under section 13;

(c) data protection impact assessments under section 15; and

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

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

17. Processing by entities other than provider.—

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

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

(3) The provider, and any employee of the provider or the data processor, shall only process personal data in accordance with the instructions of the provider and treat it confidential.

18. Grievance redressal by the provider.—

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

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

(a) the authority, in case of a significant provider; or

(b) an officer designated for this purpose, in the case of any other provider.

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

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

CHAPTER IV

ARTIFICIAL INTELLIGENCE PROTECTION AUTHORITY OF INDIA

19. Establishment of Authority. —

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

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

20. Composition and qualifications for appointment of Chairperson and Members.—

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

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

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

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

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

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

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

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

21. Terms and conditions of appointment.—

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

(2) The salaries and allowances payable to, and other terms and conditions of service of the Chairperson and the Members of the Authority shall be such as may be prescribed.

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

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

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

(4) Notwithstanding anything contained in sub-section (1), the Chairperson or a Member of the Authority may—

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

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

22. Disqualification.—

(1) No person shall be a Chairperson or Member of the Authority constituted under this Act who—

(a) is or at any time has been adjudged insolvent, or

(b) is of unsound mind and has been so declared by a Competent Court, or

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

(d) has so abused, in the opinion of Central Government, their position as a Chairperson or member, as to render his continuation in office detrimental to the public interest; or

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

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

23. Functions of Authority.—

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

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

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

(b) taking prompt and appropriate action in response to the personal data breach or misuse of systems in accordance with the provisions of this act;

(c) examination of any data audit reports and taking any action pursuant thereto;

(d) issuance of a certificate of registration to data auditors and renewal, withdrawal, suspension or cancellation thereof and maintaining a database of registered data.

(3) Where pursuant to the provisions of this Act, the Authority processes any personal data, it shall be construed as the provider 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 provider or data processor, it shall not disclose such information unless required under any law to do so, or where it is required to carry out its function under this section.

24. Power of Authority to conduct inquiry.—

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

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

(b) any provider has contravened any of the provisions of this Act or the rules or regulations made thereunder, or any direction of the Authority.

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

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

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

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

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

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

(e) any other matter which may be prescribed.

25. Action to be taken pursuant to inquiry. —

(1) On receipt of a report under sub-section (2) of section 24, the Authority may, after giving such opportunity to the provider 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 provider or data processor where the business or activity is likely to violate the provisions of this Act;

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

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

(d) require the provider 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 provider 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 provider;

(g) suspend or discontinue any cross-border flow of personal data; or

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

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

26. Search and seizure.—Where in the course of an inquiry under section 24, the Inquiry Officer has reasonable ground to believe that any books, registers, documents, records or data belonging to any person as mentioned therein, are likely to be tampered with, altered, mutilated, manufactured, falsified or destroyed, the Inquiry Officer may make an application to such

designated court, as may be notified by the Central Government, for an order for the seizure of such books, registers, documents and records.

CHAPTER V

EXEMPTIONS

27. Power of Central Government to exempt any agency of Government of India from the application of the Act.—Where the Central Government is satisfied that it is necessary or expedient,—

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

(b) 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 of India in respect of the processing of such biometric identification, as may be specified in the order subject to such procedure, safeguards and oversight mechanism to be followed by the agency, namely—.

(i) the targeted search for specific potential victims of crime, including missing children;

(ii) the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or of a terrorist attack;

(iii) the detection, localisation, identification or prosecution of a perpetrator of the suspect of a criminal offence.

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

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

(i) the compliance with the provisions of this Act shall disproportionately divert resources from such purpose;

(ii) the purposes of processing cannot be achieved if the personal data is anonymised.

(e) the clause (d) of this section shall not be processed in the manner that gives rise to a risk of significant harm to the data principal under Chapter II section 4, it may, by notification,

exempt such class of research, archiving, or statistical purposes from the application of any of the provisions of this Act as may be specified by regulations.

Explanation.—For the purposes of this section,—

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

(b) the expression "processing of such biometric identification" includes sharing by or with such agency of the Government.

28. Exemption for manual processing by small entities. —

(1) The provisions of sections 7, 8, and sections 10 to 18 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 providers as may be classified, by regulations, by Authority, having regard to—

(a) the turnover of provider in the preceding financial year;

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

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

CHAPTER VI

APPELLATE TRIBUNAL

29. Establishment of Appellate Tribunal.—

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

(a) hear and dispose of any appeal from an order of the Authority under sub-section (2) of section 25;

(b) hear and dispose of any appeal from an order of the Adjudicating Officer under sub-section (3) of section 46; and

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

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

(4) Notwithstanding anything contained in sub-section (1) to (3), where, in the opinion of the Central Government, any existing body is competent to discharge the functions of the Appellate Tribunal under this Act, then, the Central Government may notify such body to act as the Appellate Tribunal under this Act.

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

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

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

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

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

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

32. Appeals to Appellate Tribunal. —

(1) Any person aggrieved by the decision of the Authority, may prefer an appeal to the Appellate Tribunal within a period of thirty days from the receipt of the order appealed against, in such form, verified in such manner and be accompanied by such fee, as may be prescribed:

Provided that the Appellate Tribunal may entertain any appeal after the expiry of the said period of thirty days if it is satisfied that there was sufficient cause for not filing it within that period.

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

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

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

33. Procedure and powers of Appellate Tribunal.—

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

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

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

(b) requiring the discovery and production of documents;

(c) receiving evidence on affidavits;

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

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

(f) reviewing its decisions;

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

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

(i) any other matter which may be prescribed.

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

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

(1) An order passed by the Appellate Tribunal under this Act shall be executable by the Appellate Tribunal as a decree of the 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.

35. Appeal to Supreme Court.—

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

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

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

Provided that the Supreme Court may entertain the appeal after the expiry of the said period of ninety days if it is satisfied that the appellant was prevented by sufficient cause from preferring the appeal in time

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

CHAPTER VII

OFFENCES

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

(1) Any person who, knowingly or intentionally—

(a) re-identifies personal data which has been de-identified by a provider 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 provider or data processor, then, such person shall be punishable with imprisonment for a term not exceeding three years or with a fine which may extend to two lakh rupees or both.

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

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

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

38. Offences to be cognizable and non-bailable.

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

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

39. Offences by companies.

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

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

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

officer shall also be deemed to be guilty of the offence and shall be liable to be proceeded against and punished accordingly.

40. Offences by State.

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

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

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

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

CHAPTER VIII

PENALTIES

41. Compensation for failure to protect data.-

(1) Any data principal who has suffered harm as a result of any violation of any provision under this Act or the rules or regulations made thereunder, by a provider or a data processor, shall have the right to seek compensation from the provider 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 ultra vires or contrary to the instructions of the provider pursuant to section 17, 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 13, or where it has violated any provisions of this Act expressly applicable to it.

(2) The data principal may seek compensation under this section by making a complaint to the Adjudicating Officer in such form and manner as may be prescribed.

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

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

42. Penalty for failure to furnish reports, returns, information, etc. If any provider, who is required under this Act, or the rules or regulations made thereunder, to furnish any report, return or information to the Authority, fails to furnish the same, then such provider shall be liable to a 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 providers and five lakh rupees in other cases.

43. Penalty for failure to comply with direction or order issued by Authority. If any provider or data processor fails to comply with any direction issued by the Authority or order issued by the Authority under section 28, such provider shall be liable to a penalty which may extend to twenty thousand rupees for each day during which such default continues, subject to a maximum of two crores rupees.

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

45. Appointment of Adjudicating Officer.

(1) For the purpose of adjudging the penalties under this chapter or awarding compensation under section 41, 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 the 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.

46. Procedure for adjudication by Adjudicating Officer.—

(1) No penalty shall be imposed under this Chapter, except after an inquiry made in such manner as may be prescribed, and the provider or data processor or any person, as the case may be, has been given a reasonable opportunity of being heard: Provided that no inquiry under this section shall be initiated except by a complaint made by the Authority.

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

(3) If on the conclusion of such inquiry, the Adjudicating Officer is satisfied that the person has failed to comply with the provisions of this Act or has caused harm to any data principal or user as a result of any contravention of the provisions of this Act, the Adjudicating Officer may impose such penalty specified under the relevant section.

47. Recovery of penalty.—

(1) The amount of any penalty imposed or compensation awarded under this Act, if not paid, may be recovered as if it were an arrear of land revenue. and the licence or the Certificate, as the case may be, shall be suspended till the penalty is paid.

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

———