THE PRIVACY (PROTECTION) BILL, 2013

[Long Title]

[Preamble]

CHAPTER I
PRELIMINARY

1. Short title, extent and commencement. – (1) This Act may be called the Privacy (Protection) Act, 2013.

(2) It extends to the whole of India.

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

2. Definitions. – In this Act and in any rules made thereunder, unless the context otherwise requires, –

(a) "anonymise" means, in relation to personal data, the removal of all data that may, whether directly or indirectly in conjunction with any other data, be used to identify the data subject;

(b) "appropriate government" means, in relation the Central Government or a Union Territory Administration, the Central Government; in relation a State Government, that State Government; and, in relation to a public authority which is established, constituted, owned, controlled or substantially financed by funds provided directly or indirectly –

(i) by the Central Government or a Union Territory Administration, the Central Government;

(ii) by a State Government, that State Government;

(c) "authorised officer" means an officer, not below the rank of a Gazetted Officer, of an All India Service or a Central Civil Service, as the case may be, who is empowered by the Central Government, by notification in the Official Gazette, to intercept a communication of another person or carry out surveillance of another person under this Act;

(d) "biometric data" means any data relating to the physical, physiological or behavioural characteristics of a person which allow their unique identification including, but not restricted to, facial images, finger prints, hand prints, foot prints, iris recognition, hand writing, typing dynamics, gait analysis and speech recognition;

(e) "Chairperson" and "Member" mean the Chairperson and Member appointed under sub-section (1) of section 17;

(f) "collect", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a data controller obtaining, or coming into the possession or control of, any personal data of a data subject;

(g) "communication" means a word or words, spoken, written or indicated, in any form, manner or language, encrypted or unencrypted, meaningful or otherwise, and includes visual representations of words, ideas, symbols and images, whether transmitted or not transmitted and, if transmitted, irrespective of the medium of transmission;

(h) "competent organisation" means an organisation or public authority listed in the Schedule;

(i) "data controller" means a person who, either alone or jointly or in concert with other persons, determines the purposes for which and the manner in which any personal data is processed;

(j) "data processor" means any person who processes any personal data on behalf of a data controller;

(k) "Data Protection Authority" means the Data Protection Authority constituted under sub-section (1) of section 17;

(l) "data subject" means a person who is the subject of personal data;

(m) "deoxyribonucleic acid data" means all data, of whatever type, concerning the characteristics of a person that are inherited or acquired during early prenatal development;

(n) "destroy", with its grammatical variations and cognate expressions, means, in relation to personal data, to cease the existence of, by deletion, erasure or otherwise, any personal data;

(o) "disclose", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or activity that results in a person who is not the data subject coming into the possession or control of that personal data;

(p) "intelligence organisation" means an intelligence organisation under the Intelligence Organisations (Restriction of Rights) Act, 1985 (58 of 1985);

(q) "interception" or "intercept" means any activity intended to capture, read, listen to or understand the communication of a person;

(r) "personal data" means any data which relates to a natural person if that person can, whether directly or indirectly in conjunction with any other data, be identified from it and includes sensitive personal data;

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

(t) "process", with its grammatical variations and cognate expressions, means, in relation to personal data, any action or operation which is performed upon personal data, whether or not by automated means including, but not restricted to, organisation, structuring, adaptation, modification, retrieval, consultation, use, alignment or destruction;

(u) "receive", with its grammatical variations and cognate expressions, means, in relation to personal data, to come into the possession or control of any personal data;

(v) "sensitive personal data" means personal data as to the data subject's –

(i) biometric data;
(ii) deoxyribonucleic acid data;
(iii) sexual preferences and practices;
(iv) medical history and health;

(v) political affiliation;
(vi) commission, or alleged commission, of any offence;
(vii) ethnicity, religion, race or caste; and
(viii) financial and credit information.

(w) "store", with its grammatical variations and cognate expressions, means, in relation to personal data, to retain, in any form or manner and for any purpose or reason, any personal data;

(x) "surveillance" means any activity intended to watch, monitor, record or collect, or to enhance the ability to watch, record or collect, any images, signals, data, movement, behaviour or actions, of a person, a group of persons, a place or an object, for the purpose of obtaining information of a person;

and all other expressions used herein shall have the meanings ascribed to them under the General Clauses Act, 1897 (10 of 1897) or the Code of Criminal Procedure, 1973 (2 of 1974), as the case may be.

CHAPTER II
REGULATION OF PERSONAL DATA

3. Regulation of personal data. – Notwithstanding anything contained in any other law for time being in force, no person shall collect, store, process, disclose or otherwise handle any personal data of another person except in accordance with the provisions of this Act and any rules made thereunder.

4. Exemption. – Nothing in this Act shall apply to the collection, storage, processing or disclosure of personal data for personal or domestic use.

CHAPTER III
PROTECTION OF PERSONAL DATA

5. Regulation of collection of personal data. – (1) No personal data of a data subject shall be collected except in conformity with section 6 and section 7.

(2) No personal data of a data subject may be collected under this Act unless it is necessary for the achievement of a purpose of the person seeking its collection.

(3) Subject to section 6 and section 7, no personal data may be collected under this Act prior to the data subject being given notice, in such and form and manner as may be prescribed, of the collection.

6. Collection of personal data with prior informed consent. – (1) Subject to sub-section (2), a person seeking to collect personal data under this section shall, prior to its collection, obtain the consent of the data subject.

(2) Prior to a collection of personal data under this section, the person seeking its collection shall inform the data subject of the following details in respect of his personal data, namely: –

(a) when it will be collected;
(b) its content and nature;
(c) the purpose of its collection;

(d) the manner in which it may be accessed, checked and modified;

(e) the security practices, privacy policies and other policies, if any, to which it will be subject;

(f) the conditions and manner of its disclosure; and

(g) the procedure for recourse in case of any grievance in relation to it.

(3) Consent to the collection of personal data under this section may be obtained from the data subject in any manner or medium but shall not be obtained as a result of a threat, duress or coercion:

Provided that the data subject may, at any time after his consent to the collection of personal data has been obtained, withdraw the consent for any reason whatsoever and all personal data collected following the original grant of consent shall be destroyed forthwith:

Provided that the person who collected the personal data in respect of which consent is subsequently withdrawn may, if the personal data is necessary for the delivery of any good or the provision of any service, not deliver that good or deny that service to the data subject who withdrew his grant of consent.

7. Collection of personal data without prior consent. – Personal data may be collected without the prior consent of the data subject if it is –

(a) necessary for the provision of an emergency medical service to the data subject;

(b) required for the establishment of the identity of the data subject and the collection is authorised by a law in this regard;

(c) necessary to prevent a reasonable threat to national security, defence or public order; or

(d) necessary to prevent, investigate or prosecute a cognisable offence.

8. Regulation of storage of personal data. – (1) No person shall store any personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose is achieved or ceases to exist for any reason, for any period following such achievement or cessation.

(2) Save as provided in sub-section (3), any personal data collected or received in relation to the achievement of a purpose shall, if that purpose is achieved or ceases to exist for any reason, be destroyed forthwith.

(3) Notwithstanding anything contained in this section, any personal data may be stored for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation, if –

(a) the data subject grants his consent to such storage prior to the purpose for which it was collected or received being achieved or ceasing to exist;

(b) it is adduced for an evidentiary purpose in a legal proceeding; or

(c) it is required to be stored under the provisions of an Act of Parliament:

Provided that only that amount of personal data that is necessary to achieve the purpose of storage under this sub-section shall be stored and any personal data that is not required to be stored for such purpose shall be destroyed forthwith:

Provided further that any personal data stored under this sub-section shall, to the extent possible, be anonymised.

9. Regulation of processing of personal data. – (1) No person shall process any personal data that is not necessary for the achievement of the purpose for which it was collected or received.

(2) Save as provided in sub-section (3), no personal data shall be processed for any purpose other than the purpose for which it was collected or received.

(3) Notwithstanding anything contained in this section, any personal data may be processed for a purpose other than the purpose for which it was collected or received if –

(a) the data subject grants his consent to the processing and only that amount of personal data that is necessary to achieve the other purpose is processed;

(b) it is necessary to perform a contractual duty to the data subject;

(c) it is necessary to prevent a reasonable threat to national security, defence or public order; or

(d) it necessary to prevent, investigate or prosecute a cognisable offence.

10. Transfer of personal data for processing. – (1) Subject to the provisions of this section, personal data that has been collected in conformity with this Act may be transferred by a data controller to a data processor, whether located in India or otherwise, if the transfer is pursuant to an agreement that explicitly binds the data processor to same or stronger measures in respect of the storage, processing, destruction, disclosure and other handling of the personal data as are contained in this Act.

(2) No data processor shall process any personal data transferred under this section except to achieve the purpose for which it was collected.

(3) A data controller that transfers personal data under this section shall remain liable to the data subject for the actions of the data processor.

11. Security of personal data and duty of confidentiality. – (1) No person shall collect, receive, store, process or otherwise handle any personal data without implementing measures, including, but not restricted to, technological, physical and administrative measures, adequate to secure its confidentiality, secrecy, integrity and safety, including from theft, loss, damage or destruction.

(2) Data controllers and data processors shall be subject to a duty of confidentiality and secrecy in respect of personal data in their possession or control.

(3) Without prejudice to the provisions of this section, a data controller or data processor shall, if the confidentiality, secrecy, integrity or safety of personal data in its possession or control is violated by theft, loss, damage or destruction, or as a result of any disclosure contrary to the provisions of this Act, or

for any other reason whatsoever, notify the data subject, in such form and manner as may be prescribed, forthwith.

12. Regulation of disclosure of personal data. – Subject to section 10, section 13 and section 14, no person shall disclose, or otherwise cause any other person to receive, the content or nature of any personal data that has been collected in conformity with this Act.

13. Disclosure of personal data with prior informed consent. – (1) Subject to sub-section (2), a data controller or data processor seeking to disclose personal data under this section shall, prior to its disclosure, obtain the consent of the data subject.

(2) Prior to a disclosure of personal data under this section, the data controller or data processor, as the case may be, seeking to disclose the personal data, shall inform the data subject of the following details in respect of his personal data, namely: –

(a) when it will be disclosed;
(b) the purpose of its disclosure;
(c) the security practices, privacy policies and other policies, if any, that will protect it; and
(d) the procedure for recourse in case of any grievance in relation to it.

14. Disclosure of personal data without prior consent. – (1) Subject to sub-section (2), personal data may be disclosed without the prior consent of the data subject if it is necessary –

(a) to prevent a reasonable threat to national security, defence or public order; or
(b) to prevent, investigate or prosecute a cognisable offence.

(2) No data controller or data processor shall disclose any personal data unless it has received an order in writing from a police officer not below the rank of [___] in such form and manner as may be prescribed:

Provided that an order for the disclosure of personal data made under this sub-section shall not require the disclosure of any personal data that is not necessary to achieve the purpose for which the disclosure is sought:

Provided further that the data subject shall be notified, in such form and manner as may be prescribed, of the disclosure of his personal data, including details of its content and nature, and the identity of the police officer who ordered its disclosure, forthwith.

15. Quality and accuracy of personal data. – (1) Each data controller and data processor shall, to the extent possible, ensure that the personal data in its possession or control, is accurate and, where necessary, is kept up to date.

(2) No data controller or data processor shall deny a data subject whose personal data is in its possession or control the opportunity to review his personal data and, where necessary, rectify anything that is inaccurate or not up to date.

(3) A data subject may, if he finds personal data in the possession or control of a data controller or data processor that is not necessary to achieve the purpose for which it was collected, received or stored, demand its destruction, and the data controller shall destroy, or cause the destruction of, the personal data forthwith.

16. Special provisions for sensitive personal data. – Notwithstanding anything contained in this Act and the provisions of any other law for the time being in force –

(a) no person shall store sensitive personal data for a period longer than is necessary to achieve the purpose for which it was collected or received, or, if that purpose has been achieved or ceases to exist for any reason, for any period following such achievement or cessation;

(b) no person shall process sensitive personal data for a purpose other than the purpose for which it was collected or received;

(c) no person shall disclose sensitive personal data to another person, or otherwise cause any other person to come into the possession or control of, the content or nature of any sensitive personal data, including any other details in respect thereof.

CHAPTER IV
THE DATA PROTECTION AUTHORITY

17. Constitution of the Data Protection Authority. – (1) The Central Government shall, by notification, constitute, with effect from such date as may be specified therein, a body to be called the Data Protection Authority consisting of a Chairperson and not more than four other Members, to exercise the jurisdiction and powers and discharge the functions and duties conferred or imposed upon it by or under this Act.

(2) The Chairperson shall be a person who has been a Judge of the Supreme Court:

Provided that the appointment of the Chairperson shall be made only after consultation with the Chief Justice of India.

(3) Each Member shall be a person of ability, integrity and standing who has a special knowledge of, and professional experience of not less than ten years in privacy law and policy.

18. Term of office, conditions of service, etc. of Chairperson and Members. – (1) Before appointing any person as the Chairperson or Member, the Central Government shall satisfy itself that the person does not, and will not, have any such financial or other interest as is likely to affect prejudicially his functions as such Chairperson or Member.

(2) The Chairperson and every Member shall hold office for such period, not exceeding five years, as may be specified in the order of his appointment, but shall be eligible for reappointment:

Provided that no person shall hold office as the Chairperson or Member after he has attained the age of sixty-seven years.

(3) Notwithstanding anything contained in sub-section (2), the Chairperson or any Member may –

(a) by writing under his hand resign his office at any time;
(b) be removed from office in accordance with the provisions of section 19 of this Act.

(4) A vacancy caused by the resignation or removal of the Chairperson or Member under sub-section (3) shall be filled by fresh appointment.

(5) In the event of the occurrence of a vacancy in the office of the Chairperson, such one of the Members as the Central Government may, by notification, authorise in this behalf, shall act as the Chairperson till the date on which a new Chairperson, appointed in accordance with the provisions of this Act, to fill such vacancy, enters upon his office.

(6) When the Chairperson is unable to discharge his functions owing to absence, illness or any other cause, such one of the Members as the Chairperson may authorise in writing in this behalf shall discharge the functions of the Chairperson, till the date on which the Chairperson resumes his duties.

(7) The salaries and allowances payable to and the other terms and conditions of service of the Chairperson and Members shall be such as may be prescribed:

Provided that neither the salary and allowances nor the other terms and conditions of service of the Chairperson and any member shall be varied to his disadvantage after his appointment.

19. Removal of Chairperson and Members from office in certain circumstances. – The Central Government may remove from office the Chairperson or any Member, who –

(a) is adjudged an insolvent; or
(b) engages during his term of office in any paid employment outside the duties of his office; or
(c) is unfit to continue in office by reason of infirmity of mind or body; or
(d) is of unsound mind and stands so declared by a competent court; or
(e) is convicted for an offence which in the opinion of the President involves moral turpitude; or
(f) has acquired such financial or other interest as is likely to affect prejudicially his functions as a Chairperson or Member, or
(g) has so abused his position as to render his continuance in offence prejudicial to the public interest.

20. Functions of the Data Protection Authority. – (1) The Chairperson may inquire, *suo moto* or on a petition presented to it by any person or by someone acting on his behalf, in respect of any matter connected with the collection, storage, processing, disclosure or other handling of any personal data and give such directions or pass such orders as are necessary for reasons to be recorded in writing.

(2) Without prejudice to the generality of the foregoing provision, the Data Protection Authority shall perform all or any of the following functions, namely –

(a) review the safeguards provided by or under this Act and other law for the time being in force for the protection of personal data and recommend measures for their effective implementation;

(b) review any measures taken by any entity for the protection of personal data and take such further action is it deems fit;

(c) review any action, policy or procedure of any entity to ensure compliance with this Act and any rules made hereunder;

(d) formulate, in consultation with experts, norms for the effective protection of personal data;

(e) promote awareness and knowledge of personal data protection through any means necessary;

(f) undertake and promote research in the field of protection of personal data;

(g) encourage the efforts of non-governmental organisations and institutions working in the field of personal data protection;

(h) publish periodic reports concerning the incidence of collection, processing, storage, disclosure and other handling of personal data;

(i) such other functions as it may consider necessary for the protection of personal data.

(3) Subject to the provisions of any rules prescribed in this behalf by the Central Government, the Data Protection Authority shall have the power to review any decision, judgement, decree or order made by it.

(4) In the exercise of its functions under this Act, the Data Protection Authority shall give such directions or pass such orders as are necessary for reasons to be recorded in writing.

(5) The Data Protection Authority may, in its own name, sue or be sued.

21. Secretary, officers and other employees of the Data Protection Authority. – (1) The Central Government shall appoint a Secretary to the Data Protection Authority to exercise and perform, under the control of the Chairperson such powers and duties as may be prescribed or as may be specified by the Chairperson.

(2) The Central Government may provide the Data Protection Authority with such other officers and employees as may be necessary for the efficient performance of the functions of the Data Protection Authority.

(3) The salaries and allowances payable to and the conditions of service of the Secretary and other officers and employees of the Data Protection Authority shall be such as may be prescribed.

22. Salaries, etc. be defrayed out of the Consolidated Fund of India. – The salaries and allowances payable to the Chairperson and Members and the administrative expenses, including salaries, allowances and pension, payable to or in respect of the officers and other employees of the of the Data Protection Authority shall be defrayed out of the Consolidated Fund of India.

23. Vacancies, etc. not to invalidate proceedings of the Data Protection Authority. – No act or proceeding of the Data Protection Authority shall be questioned on the ground merely of the existence of any vacancy or defect in the constitution of the Data Protection Authority or any defect in the appointment of a person acting as the Chairperson or Member.

24. Chairperson, Members and employees of the Data Protection Authority to be public servants. – The Chairperson and Members and other employees of the Data Protection Authority shall be deemed to be public servants within the meaning of section 21 of the Indian Penal Code, 1860 (45 of 1860).

25. Location of the office of the Data Protection Authority. – The offices of the Data Protection Authority shall be in [___] or any other location as directed by the Chairperson in consultation with the Central Government.

26. Procedure to be followed by the Data Protection Authority. – (1) Subject to the provisions of this Act, the Data Protection Authority shall have powers to regulate –

(a) the procedure and conduct of its business;

(b) the delegation to one or more Members of such powers or functions as the Chairperson may specify.

(2) In particular and without prejudice to the generality of the foregoing provisions, the powers of the Data Protection Authority shall include the power to determine the extent to which persons interested or claiming to be interested in the subject-matter of any proceeding before it may be allowed to be present or to be heard, either by themselves or by their representatives or to cross-examine witnesses or otherwise take part in the proceedings:

Provided that any such procedure as may be prescribed or followed shall be guided by the principles of natural justice.

27. Power relating to inquiries. – (1) The Data Protection Authority shall, for the purposes of any inquiry or for any other purpose under this Act, have the same powers as vested in a civil court under the Code of Civil Procedure, 1908 (5 of 1908), while trying suits in respect of the following matters, namely –

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

(b) the discovery and production of any document or other material object producible as evidence;

(c) the reception of evidence on affidavit;

(d) the requisitioning of any public record from any court or office;

(e) the issuing of any commission for the examination of witnesses; and,
(f) any other matter which may be prescribed.

(2) The Data Protection Authority shall have power to require any person, subject to any privilege which may be claimed by that person under any law for the time being in force, to furnish information on such points or matters as, in the opinion of the Data Protection Authority, may be useful for, or relevant to, the subject matter of an inquiry and any person so required shall be deemed to be legally bound to furnish such information within the meaning of section 176 and section 177 of the Indian Penal Code, 1860 (45 of 1860).

(3) The Data Protection Authority or any other officer, not below the rank of a Gazetted Officer, specially authorised in this behalf by the Data Protection Authority may enter any building or place where the Data Protection Authority has reason to believe that any document relating to the subject matter of the inquiry may be found, and may seize any such document or take extracts or copies therefrom subject to the provisions of section 100 of the Code of Criminal Procedure, 1973 (2 of 1974), in so far as it may be applicable.

(4) The Data Protection Authority shall be deemed to be a civil court and when any offence as is described in section 175, section 178, section 179, section 180 or section 228 of the Indian Penal Code, 1860 (45 of 1860) is committed in the view or presence of the Data Protection Authority, the Data Protection Authority may, after recording the facts constituting the offence and the statement of the accused as provided for in the Code of Criminal Procedure, 1973 (2 of 1974), forward the case to a Magistrate having jurisdiction to try the same and the Magistrate to whom any such case is forwarded shall proceed to hear the complaint against the accused as if the case had been forwarded to him under section 346 of the Code of Criminal Procedure, 1973 (2 of 1974).

28. Decisions of the Data Protection Authority. – (1) The decisions of the Data Protection Authority shall be binding.

(2) In its decisions, the Data Protection Authority has the power to –

(a) require an entity to take such steps as may be necessary to secure compliance with the provisions of this Act;
(b) require an entity to compensate any person for any loss or detriment suffered;
(c) impose any of the penalties provided under this Act.

29. Proceedings before the Data Protection Authority to be judicial proceedings. – The Data Protection Authority 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), and every proceeding before the Data Protection Authority shall be deemed to be a judicial proceeding within the meaning of section 193 and section 228 and for the purposes of section 196 of the Indian Penal Code, 1860 (45 of 1860).

CHAPTER V
REGULATION BY DATA CONTROLLERS AND DATA PROCESSORS

30. Co-regulation by Data Controllers and the Data Protection Authority. – (1) The Data Protection Authority may, in consultation with data controllers, formulate codes of conduct for the collection, storage, processing, disclosure or other handling of any personal data.

(2) No code of conduct formulated under sub-section (1) shall be binding on a data controller unless –

(a) it has received the written approval of the Data Protection Authority; and

(b) it has received the approval, by signature of a director or authorised signatory, of the data controller.

31. Co-regulation without prejudice to other remedies. – Any code of conduct formulated under this chapter shall be without prejudice to the jurisdiction, powers and functions of the Data Protection Authority.

32. Self-regulation by data controllers. – (1) The Data Protection Authority may encourage data controllers and data processors to formulate professional codes of conduct to establish rules for the collection, storage, processing, disclosure or other handling of any personal data.

(2) No code of conduct formulated under sub-section (1) shall be effective unless it is registered, in such form and manner as may be prescribed, by the Data Protection Authority.

(3) The Data Protection Authority shall, for reasons to be recorded in writing, not register any code of conduct formulated under sub-section (1) that is not adequate to protect personal data.

CHAPTER IV
SURVEILLANCE AND INTERCEPTION OF COMMUNICATIONS

33. Surveillance and interception of communication to be warranted. – Notwithstanding anything contained in any other law for the time being in force, no –

(i) surveillance shall be carried out, and no person shall order any surveillance of another person;

(ii) communication shall be intercepted, and no person shall order the interception of any communication of another person;

save in execution of a warrant issued under section 36, or an order made under section 38, of this Act.

34. Application for issuance of warrant. – (1) Any authorised officer seeking to carry out any surveillance or intercept any communication of another person shall prefer an application for issuance of a warrant to the Magistrate.

(2) The application for issuance of the warrant shall be in the form and manner prescribed in the Schedule and shall state the purpose for which the warrant is sought.

(3) The application for issuance of the warrant shall be accompanied by –

(i) a report by the authorised officer of the suspicious conduct of the person in respect of whom the warrant is sought, and all supporting material thereof;

(ii) an affidavit of the authorised officer, or a declaration under his hand and seal, that the contents of the report and application are true to the best of his knowledge, information and belief, and that the warrant shall be executed only for the purpose stated in the application and shall not be misused or abused in any manner including to interfere in the privacy of any person;

(iii) details of all warrants previously issued in respect of the person in respect of whom the warrant is sought, if any.

35. Considerations prior to the issuance of warrant. – (1) No warrant shall issue unless the requirements of section 34 and this section have been met.

(2) The Magistrate shall consider the application made under section 34 and shall satisfy himself that the information contained therein sets out –

(i) a reasonable threat to national security, defence or public order; or

(ii) a cognisable offence, the prevention, investigation or prosecution of which is necessary in the public interest.

(3) The Magistrate shall satisfy himself that all other lawful means to acquire the information that is sought by the execution of the warrant have been exhausted.

(4) The Magistrate shall verify the identity of the authorised officer and shall satisfy himself that the application for issuance of the warrant is authentic.

36. Issue of warrant. – (1) Subject to section 34 and section 35, the Magistrate may issue a warrant for surveillance or interception of communication, or both of them.

(2) The Magistrate may issue the warrant in Chambers.

37. Magistrate may reject application for issuance of warrant. – If the Magistrate is not satisfied that the requirements of section 34 and section 35 have been met, he may, for reasons to be recorded in writing, –

(i) refuse to issue the warrant and dispose of the application;

(ii) return the application to the authorised officer without disposing of it;

(iii) pass any order that he thinks fit.

38. Order by Home Secretary in emergent circumstances. – (1) Notwithstanding anything contained in section 35, if the Home Secretary of the appropriate government is satisfied that a grave threat to national security, defence or public order exists, he may, for reasons to be recorded in writing, order any surveillance or interception of communication.

(2) An authorised officer seeking an order for surveillance or interception of communication under this section shall prefer an application to the Home Secretary in the form and manner prescribed in the Schedule and accompanied by the documents required under sub-section (3) of section 34.

(3) No order for surveillance or interception of communication made by the Home Secretary under this section shall be valid upon the expiry of a period of seven days from the date of the order.

(4) Before the expiry of a period of seven days from the date of an order for surveillance or interception of communication made under this section, the authorised officer who applied for the order shall place the application before the Magistrate for confirmation.

39. Duration of warrant or order. – (1) The warrant or order for surveillance or interception of communication shall specify the period of its validity and, upon its expiry, all surveillance and interception of communication, as the case may be, carried out in relation to that warrant or order shall cease forthwith:

Provided that no warrant or order shall be valid upon the expiry of a period of sixty days from the date of its issue.

(2) A warrant issued under section 36, or an order issued under section 38, for surveillance or interception of communication, or both of them, may be renewed by a Magistrate if he is satisfied that the requirements of sub-section (2) of section 35 continue to exist.

40. Duty to inform the person concerned. – Subject to sub-section (2), before the expiry of a period of sixty days from the conclusion of any surveillance or interception of communication carried out under this Act, the authorised officer who carried out the surveillance or interception of communication shall, in writing in such form and manner as may be prescribed, notify, with reference to the warrant of the Magistrate, and, if applicable, the order of the Home Secretary, each person in respect of whom the warrant or order was issued, of the fact of such surveillance or interception and duration thereof.

(2) The Magistrate may, on an application made by an authorised officer in such form and manner as may be prescribed, if he is satisfied that the notification under sub-section (1) would –

(a) present a reasonable threat to national security, defence or public order, or
(b) adversely affect the prevention, investigation or prosecution of a cognisable offence,

for reasons to be recorded in writing addressed to the authorised officer, order that the person in respect of whom the warrant or order of surveillance or interception of communication was issued, not be notified of the fact of such interception or the duration thereof:

41. Security and duty of confidentiality and secrecy. – (1) No person shall carry out any surveillance or intercept any communication of another person without implementing measures, including, but not restricted to, technological, physical and administrative measures, to secure the confidentiality and secrecy of all information obtained as a result of the surveillance or interception of communication, as the case may be, including from theft, loss or unauthorised disclosure.

(2) Any person who carries out any surveillance or interception of any communication, or who obtains any information, including personal data, as a result of surveillance or interception of communication, shall be subject to a duty of confidentiality and secrecy in respect of it.

(3) Every competent organisation shall, before the expiry of a period of one hundred days from the enactment of this Act, designate as many officers as it deems fit as Privacy Officers who shall be administratively responsible for all interceptions of communications carried out by that competent organisation.

42. Disclosure of information. – (1) Save as provided in this section, no person shall disclose to any other person, or otherwise cause any other person to come into the knowledge or possession of, the content or nature of any information, including personal data, obtained as a result of any surveillance or interception carried out under this Act.

(2) Notwithstanding anything contained in this section, if the disclosure of any information, including personal data, obtained as a result of any surveillance or interception of any communication is necessary to –

(a) prevent a reasonable threat to national security, defence or public order, or
(b) prevent, investigate or prosecute a cognisable offence,

an authorised officer may disclose the information, including personal data, to any authorised officer of any other competent organisation.

CHAPTER VI
OFFENCES AND PENALTIES

43. Punishment for offences related to personal data. – (1) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes or otherwise handles any personal data shall be punishable with imprisonment for a term which may extend to [____] years and may also be liable to fine which may extend to [____] rupees.

(2) Whoever attempts to commit any offence under sub section (1) shall be punishable with the punishment provided for such offence under that sub-section.

(3) Whoever, except in conformity with the provisions of this Act, collects, receives, stores, processes or otherwise handles any sensitive personal data shall be punishable with imprisonment for a term which may extend to [*increased for sensitive personal data*] years and and may also be liable to fine which may extend to [____] rupees.

(4) Whoever attempts to commit any offence under sub section (3) shall be punishable with the punishment provided for such offence under that sub-section.

44. Abetment and repeat offenders. – (1) Whoever abets any offence punishable under this Act shall, if the act abetted is committed in consequence of the abetment, be punishable with the punishment provided for that offence.

(2) Whoever, having been convicted of an offence under any provision of this Act is again convicted of an offence under the same provision, shall be punishable, for the second and for each subsequent offence, with double the penalty provided for that offence.

45. Offences by companies. – (1) Where an offence under this Act has been committed by a company, every person who, at the time of 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:

Provided that nothing contained in this sub-section shall render any such person liable to any punishment, 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.

(2) Notwithstanding anything contained in sub-section (1), where any 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 be deemed to be guilty of that offence, and shall be liable to be proceeded against and punished accordingly.

46. Cognisance. – Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), the offences under section 43, section 44 and section 45 shall be cognisable and non-bailable.

47. General penalty. – Whoever, in any case in which a penalty is not expressly provided by this Act, fails to comply with any notice or order issued under any provisions thereof, or otherwise contravenes any of the provisions of this Act, shall be punishable with fine which may extend to [____] rupees, and, in the case of a continuing failure or contravention, with an additional fine which may extend to [____] rupees for every day after the first during which he has persisted in such failure or contravention.

48. Punishment to be without prejudice to any other action. – The award of punishment for an offence under this Act shall be without prejudice to any other action which has been or which may be taken under this Act with respect to such contravention.

CHAPTER VII
MISCELLANEOUS

49. Power to make rules. – (1) The Central Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for –

[__]

(3) Every rule made under this section shall be laid, as soon as may be after it is made, before each House of Parliament while it is in session for a period of thirty days which may be comprised in one session or in two successive sessions and if before the expiry of the session in which it is so laid or the session immediately following, both Houses agree in making any modification in the rule, or both Houses agree that the rule should not be made, the rule 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.

50. Bar of jurisdiction. – (1) On and from the appointed day, no court or authority shall have, or be entitled to exercise, any jurisdiction, powers or authority (except the Supreme Court and a High Court exercising powers under Article 32, Article 226 and Article 227 of the Constitution) in relation to matters specified in this Act.

(2) No order passed under this Act shall be appealable except as provided therein and no civil court shall have jurisdiction in respect of any matter which the Data Protection Authority 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.

51. Protection of action taken in good faith. – No suit or other legal proceeding shall lie against the Central Government, State Government, Data Protection Authority, Chairperson, Member or any person acting under the direction either of the Central Government, State Government, Data Protection Authority, Chairperson or Member in respect of anything which is in good faith done or intended to be done in pursuance of this Act or of any rules or any order made thereunder.

52. 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 appears to it to be necessary or expedient for removing the difficulty:

Provided that no such order shall be made under this section after the expiry of a period of three 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.

53. Act to have overriding effect. – The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.