(Unofficial 1st draft English Text of the proposed Data Protection Act, 2022)

THE DATA PROTECTION ACT, 2022

CONTENTS

CHAPTER VI

DATA SUBJECT RIGHTS

CHAPTER VII

ACCOUNTABILITY AND TRANSPARENCY

CHAPTER VIII

EXEMPTION

CHAPTER XIII

COMPLAINTS TURNED TO OFFENCES AND RELATED MATTERS

CHAPTER XIV

MISCELLANEOUS

Bill No. ……., 2022

An Act to make provisions to provide protection and control the matters relating to the processing of data of a person and matters ancillary and connected thereto.

Whereas it is necessary to make provisions as to collection, processing, storage, use or reuse, transfer, disclosure, destruction of and matters related thereto; and

Whereas it is necessary to establish a controlling authority under existing administrative process, and to supervise and monitoring the data being processed; and

Whereas it is expedient to provide protection of data belonging to any person for the purpose of overall development of the Information and Communication Technology sector; and

Whereas it is expedient and necessary to make provisions for the protection of data belonging to any person and its processing thereof and matters ancillary and connected thereto;

Now, therefore, it is enacted as follows:-

CHAPTER I

PRELIMINARY

1. Short title and commencement.- (1) This Act may be called the Data Protection Act, 2022.

(2) Subject to provisions of sub-section (3), it shall come into force on such date as the Government may, by notification in the official Gazette, appoint.

(3) Different dates of commencement of the provisions of different sections of this Act may be appointed in the notification issued under sub-section (2).

2. Definitions.- In this Act, unless there is anything repugnant in the subject or context,-

(a) “anonymized data" means data which has undergone the process of anonymization under this Act;

(b) “financial data” means any number or other data used to identify an account opened by, debit or credit card or payment instrument issued by a financial institution to a data subject or any data regarding the relationship between a financial institution and a data subject including financial status and credit history;

(c) "data" means a representation of any information, knowledge, fact, concepts or instructions which are being prepared or have been prepared in a formalized manner and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printout, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer, and includes the personal data for that purpose:

Provided that, the anonymized, encrypted or pseudonymized data which is incapable of identifying any individual shall not be included within the purview of personal data;

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

(e) "data protection office" means the Data Protection Office established under this Act;

(f) "data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, data transmitted, stored or otherwise processed;

(g) "genetic data" means data relating to the inherited or acquired genetic characteristics of an individual which give unique information about the behavioral 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;

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

(i) "data controller" means a person including the Government entity, a company or any juridical entity who either alone or jointly or in conjunction with other person determines the purpose and means of processes any data or has control over or authorizes the processing of any data, but does not include a data processor;

(j) "auditor" means a person engaged for auditing of data having qualification as determine under sub-section (3) of section 29;

(k) "profiling" means any act of collecting useful information or data of a person where description of necessary information or data of such person is inserted/compacted;

(l) "data processor" means any person who processes the data on behalf of the data controller, but does not include an employee of data controller;

(m) "processing" means any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval or recovery, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

(n) "Code of Criminal Procedure" meaning the Code of Criminal Procedure, 1898 (Act V of 1898);

(o) "biometric data" means facial images, fingerprints, iris scans, or any other similar data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data subject, which allow or confirm the unique identification of that natural person;

(p) "rules" means rules made under this Act;

(q) "person" includes an individual, any juridical person, company, firm, association, corporation, a body of individual or group of persons, whether incorporated or not;

(r) "user created or generated data" means private data of a data subject (for example text, message, images, videos, audios, reviews, email or any other private documents or similar other subject matter) which are created or generated by an individual or a group of individuals for limited use or share and not intended for public use;

(s) "Director General" means the Director General of the Digital Security Agency established under section 6(i) of Digital Security Act, 2018;

(t) "consent" of the data subject means any freely given and specific indication of the data subject's wishes by which data subject, by a statement or by a clear affirmative action, signifies agreement to the processing of data;

(u) "health data" means data related to the state of physical or mental health of the data subject, and includes records regarding the past, present or future state of the health of such data subject, data collected in the course of registration for, or provision of health services, data associating the data subject to the provision of specific health services;

(v) "sensitive data" means data or information of a data subject which consists of information relating to-

(1) financial or commercial data;
(2) health data, both physical or mental including medical records or information as to health of an individual;
(3) genetic data;
(4) biometric data;
(5) the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings;
(6) any other data as may be prescribed.

3. Overriding effect of the Act.- Notwithstanding anything contained to the contrary in any other law for the time being in force, the provisions of this Act shall have effect.

4. Application.- (1) This Act shall apply to a person-

(a) collecting, processing, using, shared or otherwise processed data within Bangladesh;
(b) outside Bangladesh who collects, processes, uses, shares or otherwise processes data relating to citizens of Bangladesh; or
(c) processing of data by a data controller or a data processor not present within Bangladesh, if such processing is in connection with any business carried on in Bangladesh, or any activity of offering goods or services to data subjects or which involves profiling of data subjects.

(2) Notwithstanding anything contained in sub-section (1), this Act shall not apply to processing of anonymized, encrypted or pseudonymized data.

CHAPTER II

DATA PROTECTION PRINCIPLES

5. Data protection principles.- For the purposes of this Act, any person who collects, process, holds or uses data shall comply with the following principles of data protection and the provisions of this Act and the rules made thereunder,-

(a) **Consent and accountability:** be accountable to the data subject for the data collected or processed, other than sensitive data, of a data subject with his consent to the processing of the data and in case of sensitive data, processing of such data shall be made in accordance with the provisions of this Act and rules made there under;

(b) **Fair and reasonable:** collect and process such data in a fair and reasonable manner that respects the provisions of this Act and the rules made thereunder;

(c) **Integrity:** collect, process, hold or use adequate, relevant and not excessive or unnecessary data and take reasonable steps to ensure that the data is accurate, complete, not misleading and kept upto date by having regard to the purpose;

(d) **Retention:** retain data for the period authorized by this Act and rules made thereunder and for which data is required to ensure that all data is destroyed permanently if it is no longer required for the purpose for which it was to be processed;

(e) **Access to data and data quality:** ensure quality of information collected, processed, held or used and a data subject shall be given access to his data held and be able to correct that data where the data is inaccurate, incomplete, misleading or not up to date;

(f) **Disclosure:** ensure transparency and participation of the data subject in collection, processing, holding or use of data, and subject to the provisions of this Act, no data shall, without the consent of the data subject, be disclosed for any purpose other than the purpose of processing, use and discloser as mentioned at the time of collection of the data;

(g) **Security:** observe security safeguards in respect of data and when processing data, take proper steps to protect the data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

CHAPTER III

PROCESSING OF DATA

6. Protection of data.- The processing of data shall be done in compliance with the provisions of this Act and the rules made thereunder.

7. Consent for data processing.- (1) Data of a data subject shall not be processed unless the data subject has given his consent, no later than at the commencement of the processing, to the processing of the data.

(2) The consent of the data subject under sub-section (1) must be free, specific, clear, and capable of being withdrawn.

(3) The data controller shall bear the burden of proof to establish that consent has been given by the data subject for processing of data in accordance with this section.

(4) Where the data subject withdraws consent for the processing of any data necessary for the performance of a contract to which the data subject is a party, all legal consequences for the effects of such withdrawal shall be borne by him.

(5) Notwithstanding sub-section (1), a data controller may process data of a data subject if the processing is necessary-

(a) for the performance of a contract to which the data subject is a party;

(b) for the taking of steps at the request of the data subject with a view to entering into a contract;

(c) for compliance with any legal obligation to which the data controller is the subject, other than an obligation imposed by a contract;

(d) for protecting the vital interests of the data subject;

Explanation.- For the purpose of this clause "vital interest" means matters relating to life, death or security of a data subject.

(e) for treatment, public health, medical or research purposes or to respond any medical emergency involving a threat to the life or to the health of a data subject or any other individual;

(f) for compliance with any order of the court of competent jurisdiction;

(g) for exercise of any functions conferred under any law;

(h) for the exercise of any function of the Government authorized by law for the provision of any service or benefit, or the issuance of any certification, license or permit.

(6) A data controller may process data of a data subject if the processing is necessary for any public interest which may be prescribed by rules.

8. Notice to a data subject.- A data controller shall issue a written notice to a data subject following the procedures in such manner as may be prescribed by rules, and such notice shall provide the information relating to the purpose of collection of data of data subject and its collection procedure.

9. Protection of privacy.- A data collector**,** data processor or data controller shall not collect, hold or process data in a manner which infringes the right of privacy of a data subject.

10. Manner of collection of data from data subject.- (1) Any person authorized by the data controller in this behalf may collect the data directly from data subject in such manner as may be prescribed.

(2) Notwithstanding anything contained in sub-section (1), data may be collected in a prescribed manner from another person or statutory body or government entity where-

(a) the data is contained in a public record;

(b) the data subject has deliberately made the data public or the data subject has consented to the collection of the data from another authorized source;

(c) the collection of the data from another source otherwise the source as mentioned in clause (b) is not likely to prejudice the privacy of the data subject;

(d) the collection of any data is necessary for the prevention, detection, investigation of an offence or for the national security.

CHAPTER IV

PROCESSING OF SENSITIVE DATA

11. Processing of sensitive data.- (1) Subject to sub-section (5) and (6) of section 7, a data controller shall not process any sensitive data of a data subject except in accordance with the following conditions-

(a) the data subject has given his explicit consent to the processing of the data;

(b) for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment; or

(c) in order to protect the interests of the data subject or another person, in a case where consent cannot be given by or on behalf of the data subject, or the data controller cannot reasonably be expected to obtain the consent of the data subject;

(d) in order to protect the interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld;

(e) for medical purposes and is undertaken by a healthcare professional, and to respond to any medical emergency involving a threat to life or to the health of a data subject;

(f) for the purpose of, or in connection with, any legal proceedings;

(g) for the purposes of establishing, exercising or defending legal rights;

(h) for orders of a court of competent jurisdiction;

(i) for the exercise of any functions conferred on any person by or under any law; or

(j) the information contained in the data has been made public as a result of steps deliberately taken by the data subject.

CHAPTER V

DATA OF CHILDREN

12. Data relating to children.- (1) A person shall not collector process data relating to a child unless the collection or processing thereof is necessary or carried out with the prior consent of the parent or guardian or relevant person having authority to make decisions on behalf of the child; or for research; or authorized for statistical purpose.

(2) Every data controller shall process data of children in a manner that protects the rights and interests of the child.

(3) The procedure for age verification, parental consent and related other matters shall be prescribed by rules in order to process the data of children.

Explanation.- For the purpose of this section-

(a) "children" means any person who is below the age of 18 years;

(b) "authorized person" means, in relation to a child, a person or guardian authorized by the court to make a data access or data correction request.

CHAPTER VI

DATA SUBJECT RIGHTS

13. Right of access to data.- (1) A person is entitled to be informed by a data controller whether data of which that person is the data subject is being processed by or on behalf of the data controller.

(2) A requestor may, upon payment of a prescribed fee, make a data access request to the data, in writing, to the data controller for the information as may be prescribed.

(3) A data access request for any information under sub-section (2) shall be treated as a single request.

(4) The data controller shall provide the information as required under this section to the data subject in a clear and concise manner that is easily comprehensible to a reasonable person.

(5) Where a data controller does not hold the data, but controls the processing of the data in such a way as to prohibit the data controller who holds the data from complying, whether in whole or part, with the data access request under sub-section (2) which relates to the data, the first mentioned data controller shall be deemed to hold the data and the provisions of this Act shall be construed accordingly.

14. Right to correction, etc.- (1) Where necessary, having regard to the purposes for which data is being processed, the data subject shall have the right to obtain the correction of inaccurate or misleading data, the completion of incomplete data, and the updating of data that is out of date from the data controller processing data of the data subject.

(2) Where the data controller receives a request under sub-section (1), and the data controller does not agree with the need for such correction, completion or updating having regard to the purposes of processing, the data controller shall provide the data subject with adequate justification in writing for rejecting the application.

(3) Where the data subject is not satisfied with the justification provided by the data controller under sub-section (2), the data subject may require that the data controller take reasonable steps to indicate, alongside the relevant data, that the same is disputed by the data subject.

(4) Where the data controller corrects, completes, or updates data in accordance with sub-section (1), the data controller shall also take reasonable steps within time as may be prescribed to notify all relevant entities or individuals to whom such data may have been disclosed regarding the relevant correction, completion or updating.

(5) Where a data controller does not hold the data, but controls the processing of the data in such a way as to prohibit the data controller who holds the data from complying, whether in whole or in part, with the data correction request under sub-section (1) which relates to the data, the first-mentioned data controller shall be deemed to be the data controller to whom such a request may be made and the provisions of this Act shall be construed accordingly.

15. Withdrawal of consent.- (1) A data subject may, by notice in writing withdraw his consent to the processing of data in respect of which he is the data subject.

(2) The data controller shall, upon receiving the notice under subsection (1), cease the processing of the data.

(3) The failure of the data subject to exercise the right conferred by subsection (1) does not affect any other rights conferred on him by this Act.

(4) The withdrawal of consent by data subject under this section and related other matters shall be conducted in such manner as may be prescribed.

16. Right to data portability.- (1)The data subject shall have the right to, receive the data related to the data subject in a structured, commonly used and machine-readable format which such data subject has provided to the data controller or which forms part of any profile on the data subject, or which the data controller has otherwise obtained, and have the data transferred to any other data controller.

(2) Sub-section (1) shall only apply where the processing has been carried out through automated means, and shall not apply where processing is necessary for functions of the Government or processing is in compliance of law.

17. Rights of foreign data subjects.- Foreign data subject resides in Bangladesh shall have all his rights under this act where his data has been collected.

18. Right to erasure.- (1) The data subject shall have the right to obtain from the data controller the erasure of data concerning him without undue delay and the data controller shall have the obligation to erase data within a prescribed period and maintaining the procedure where one or more of the following reason applies-

(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based;

(c) the data subject objects to the processing pursuant to the provisions of this Act;

(d) the data have been unlawfully processed;

(e) the data have to be erased for compliance with a legal obligation; or

(f) such other conditions as may be prescribed.

(2) Where the data controller has made the data public and is obliged pursuant to sub-section (1) to erase the data, the data controller shall take reasonable steps to erasure such data.

(3) Sub-sections (1) and (2) shall not apply to the extent that processing is necessary for-

(a) exercising the right of freedom of expression and information;

(b) compliance with a legal obligation or for the performance of a task carried out in the public interest;

(c) reasons of public interest in the area of public health; or

(d) archiving purposes in the public interest, scientific or historical research or statistical purposes in so far as the right referred to in sub-section (1) is likely to render impossible or seriously impair the achievement of the objectives of that processing.

19. Right to prevent processing of data.- (1) A data subject may at any time, by notice in writing to a data controller or data processor, require the data controller or data processor to stop processing data which causes or likely to cause unwarranted substantial damage to the data subject.

(2) A data controller shall, within the days as may be prescribed by rules after receipt of such notice under sub-section (1), inform the Director General and data subject that the data controller has complied or intends to comply with the notice or of reasons for non-compliance.

(3) Where the data controller gives reasons for non-compliance, a copy of the notice required by sub-section (2) shall be given to the Director General immediately.

(4) Where the Director General is satisfied that the data subject is justified, he shall direct the data controller to comply with the notice given by the data subject.

20. General conditions for the exercise of rights.- (1) The exercise of any right under this Chapter shall be on the basis of a request made in writing to the data controller with reasonable information to satisfy the data controller of the identity of the data subject making the request and the data controller shall acknowledge receipt of such request within such period of time as may be prescribed.

(2) The conditions for the exercise of rights, conditions of refusal to comply with the request and the procedure for compliance by a data controller under this section shall be prescribed by rules made under this Act.

CHAPTER VII

ACCOUNTABILITY AND TRANSPARENCY

21. Accountability.- (1) The data controller shall be responsible for complying with all obligations set out in this Act in respect of any processing of data undertaken by it or on its behalf, and be able to demonstrate that any processing undertaken by it or on its behalf is in accordance with the provisions of this Act.

22. Transparency.- (1) The data controller shall take reasonable steps to maintain transparency regarding its general practices related to processing of data and shall make available the following information in a prescribed form-

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

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

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

(d) the existence of and procedure for the exercise of data subject rights, and any related contact details for the same;

(e) the existence of a right to file complaints to the Director General;

(f) where applicable, information regarding transfers of data to the place that the data controller generally carries out; and

(g) such other information as may be prescribed.

(2) The data controller shall notify the data subject of important operations in the processing of data related to the data subject by notifications in such manner as may be prescribed.

23. Non-disclosure of data.- Subject to the provisions of this Act, no data shall, without the consent of the data subject, be disclosed for any purpose other than the purpose for which the data was to be disclosed at the time of collection of the data.

24. Security standards to protect data.- (1) The Government may prescribe standards to protect data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

(2) A data controller may, when processing data, take steps to protect the data may be considered necessary by having regard to-

(a) the nature of the data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;

(b) the place or location where the data is stored;

(c) any security measures incorporated into any equipment in which the data is stored;

(d) the measures taken for ensuring the reliability, integrity and competence of personnel having access to the data; and

(e) the measures taken for ensuring the secure transfer of the data.

(3) Where processing of data is carried out by a data processor on behalf of the data controller, the data controller shall, for the purpose of protecting the data, ensure that the data processor undertakes to adopt applicable technical and organizational security standards governing processing of data, as prescribed by rules.

(4) The data processor is independently liable to take steps to ensure compliance with security standards prescribed under sub-section (1).

25. Data Retention requirements.- (1) The data processed for any purpose shall not be kept longer than is necessary for the fulfillment of that purpose.

(2) It shall be the duty of a data controller to take all reasonable steps to ensure that all data is permanently destroyed if it is no longer required for the purpose for which it was to be processed.

26. Data integrity and access to data.- (1) A data controller shall take reasonable steps to ensure that the data is accurate, complete, not misleading and kept up to date by having regard to the purpose, including any directly related purpose, for which the data was collected and further processed.

(2) A data subject shall be given access to his data held by a data controller and be able to correct that data where the data is inaccurate, incomplete, misleading or not upto date, except where compliance with a request to such access or correction is refused under this Act.

27. Record to be kept by data controller.- (1) A data controller shall keep and maintain accurate and up-to-date the prescribed records of any application, notice, request or any other information relating to data that has been or is being processed by him.

(2) The records in sub-section (1) shall be maintained in such manner and form as prescribed.

28. Data breach notification.- (1) In the event of a data breach, data controller shall without undue delay and where reasonably possible, not beyond the period as may be prescribed, of becoming aware of the data breach, notify the Director General in respect of the data breach.

(2) The data breach notification shall provide such information as may be prescribed.

(3) The data controller shall maintain record of any data breaches, comprising the facts relating to the data breach, its effects and the remedial action taken, and the data processor shall give necessary instruction to the data processor to take action on such event.

29. Data audit.- (1) The data controller shall conduct of its processing of data audited by an independent data auditor as authorized by Director General within time as may be prescribed by him.

(2) The data auditor shall evaluate the compliance of the data controller under the provisions of this Act and rules made thereunder.

(3) The qualification of auditor and the manner, forms, procedure and the other related matters for conducting audit under this section shall be prescribed by rules.

(4) The Director General shall enroll persons with expertise in the area of information technology, computer systems, data science, data protection or privacy, with such qualifications, experience and eligibility of data auditors as may be prescribed.

(5) Notwithstanding anything contained in sub-section (1), where the Director General is of the view that the data controller is processing data in a manner that is likely to cause harm to a data subject, he may order the data controller to conduct an audit and shall appoint a data auditor for that purpose.

30. Responsibility of the data controller.- The data controller shall-

(a) implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act;

(b) perform the processing of data under this Act taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons;

(c) to implement appropriate data protection standard operations procedure as described in section 38;

(d) for the purpose of clauses (a), (b) and (c), undertake such other responsibility as may be prescribed.

31. Data Protection Officer.- (1) For the purpose of carrying out the functions of data protection, the data controller shall appoint a qualified data protection officer as may be prescribed.

(2) The data protection officer shall perform such functions and duties as may be prescribed.

(3) The data protection officer shall in the performance of his tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

32. Data protection by design.- Every data controller shall implement policies and measures to ensure that-

(a) the organizational and business practices and standard technical systems are designed in a manner to anticipate, identify and avoid harm to the data subject;

(b) the technology used in the processing of data is in accordance with prescribed standards;

(c) the legitimate interests of its functions may be achieved without compromising privacy interests and the interest of the data subject is accounted for at every stage of processing of data;

(d) the processing of data is carried out in a transparent manner as may be prescribed.

CHAPTER VIII

EXEMPTION

33. Exemption.- Subject to the provisions of section 34, the data processed-

(a) for the prevention or detection of crime or for the purpose of investigations; or the apprehension or prosecution of offenders; or the assessment or collection of any tax or duty or any other imposition of a similar nature,

(b) in relation to information of the physical or mental health of a data subject, if the application of the provisions to the data subject would be likely to cause serious harm to the physical or mental health of the data subject or any other person,

(c) for preparing statistics or carrying out research shall be exempted from the related provisions of this Act,

(d) necessary for the purpose of or in connection with any order or judgment of a court,

(e) for the purpose of discharging regulatory functions if the application of those provisions to the data would be likely to prejudice the proper discharge of those functions, or

(f) only for journalistic, literary, artistic or academic purposes,

shall be exempted from the provisions of this Act.

34. Power to make further exemptions.- (1) The Government may, by notification published in the official Gazette, exempt the application of any provision of this Act to any data controller or class of data controller.

(2) The Government may impose any terms or conditions as it thinks fit in respect of any exemption made under subsection (1).

CHAPTER IX

DATA PROTECTION OFFICE

35. Establishment of the data protection office, etc.-(1) Soon after the commencement of this Act, the Government shall establish, for carrying out the purposes of this Act, an office to be called data protection office.

(2) Data protection office shall be under direct control and administration of Digital Security Agency established under Digital Security Act, 2018.

(3) The Director General of the Digital Security Agency shall be the head of the data protection office.

(4) Data protection office shall consist of such officers and other employees as it considers necessary for the efficient performance of its functions of the office on such terms and conditions as may be prescribed.

36. Powers of the data protection office.- (1) Subject to the other provisions of this Act, the data protection office may take such measures and exercise such powers as may be necessary for carrying out the purposes of the Act.

(2) Without prejudice to the generality of the powers conferred by sub-section (1), the data protection office, as a supervisory authority, shall, in particular, have power all or any of the, following-

(a) **Investigative powers:**

(i) to order the controller and the processor, and, where applicable, the controller's or the processor's representative to provide any data it requires for the performance of its tasks;

(ii) to carry out investigations in the form of data protection audit;

(iii) to notify the controller or the processor of an alleged infringement of this Act and rules made thereunder;

(iv) to obtain, from the controller and the processor, access to all data necessary for the performance of its tasks;

(v) to obtain access to any premises of the controller and the processor, including to any data processing equipment and means;

(b) **Corrective powers:**

(i) to issue warnings to a controller or processor that intended processing operations are likely to infringe provisions of this Act and Rules;

(ii) to direct the controller or the processor to comply with the data subject's requests to exercise his rights pursuant to this Act;

(iii) to direct the controller or processor to bring processing operations into compliance with the provisions of this Act, where appropriate, in a manner and within a period as may be prescribed by rules;

(iv) to direct the controller to communicate a data breach to the data subject;

(v) to impose a ban on processing;

(vi) to order the rectification or erasure of data;

(vii) to present necessary data to impose an administrative fine under this Act;

(viii) to order the suspension of data flows to a recipient in a foreign country or to an international organization;

(c) **Authorization and advisory powers:**

(i) to advise the controller relating to the functions to be performed in accordance with this Act and rules made thereunder;

(ii) to issue to the concerned public on any issue related to the protection of data;

(iii) to adopt standard data protection guidelines;

(iv) to authorize administrative arrangements.

37. Functions of the data protection office.- For the purpose of this Act, the data protection office shall-

(a) oversee the implementation of this Act;

(b) promote the protection and observance of the right to privacy and of data;

(c) monitor, investigate, and report on the observance of the right to privacy and of data;

(d) take necessary steps intended to raise public awareness about the Act;

(e) receive and investigate complaints relating to violation or infringement of the right of data subject under the Act;

(f) establish and maintain a data protection and privacy register;

(g) make guidelines for efficient functioning the collection, processing, holding, using and other related matters of data;

(h) to do all other acts and things ancillary or incidental to any of the aforesaid functions;

(i) perform such other functions as may be prescribed by rules.

38. **Standard operations procedure.-** (1) The Director General, with prior approval of the Government, shall issue standard operations procedure, by following the provisions of this Act and rules made thereunder on collection, processing, store or retain, use and such other related matters.

(2) Without prejudice to sub-sections (1), or any other provision of this Act, the Director General may, among others, issue standard operations procedure in respect of the following matters, namely:-

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

(b) measures for ensuring quality of data processed and pertaining to the retention of data under this Act;

(c) conditions for valid consent under this Act;

(d) matters relating to processing of data;

(e) avail the right to data portability;

(f) transparency and accountability measures including the standards thereof to be maintained by data controllers and data processors;

(g) evaluation the impact of the standards for security safeguards;

(h) cross-border transfer of data;

(i) any other matter which may require for the purpose of this Act.

(3) Non-compliance by the data controller or data processor with any standard operations procedure shall be deemed to be violated the provisions of this Act.

39. Power to issue directions.- (1) The Director General may, for the discharge of its functions under this Act, issue such directions, from time to time, as it may consider necessary, to data controller or data processors and if any direction is issued under this section the data controller or data processors shall be bound to comply with such directions.

(2) The Director General may prescribe the time frame in the direction for discharge of its function.

40. Power to call for information.- (1) Without prejudice to the other provisions of this Act, the Director General may, in writing, require a data controller or data processor to provide such information as may be reasonably required by it for discharging its functions under this Act.

(2) If any direction is issued under sub-section (1) to provide information, the controller or processor or the person shall be bound to comply with such direction.

41. Power to conduct inquiry and investigation.- (1) The Director General may conduct an inquiry/investigation where it has reasonable grounds to believe that the activities of the data controller or data processor being conducted in a manner which is detrimental to the interest of data subjects, or any data controller or data processor has violated any of the provisions of this Act or the rules made there under, or directions issued by the Director General there under.

(2) For the purpose of sub-section (1), the Director General may, by an order in writing, authorize one of its officers as an Inquiry/investigating officer to inquire/investigate into the affairs of such data controller or data processor and to report to the Director General on any inquiry made.

(3) The detail procedure for inquiry/investigation and the action to be taken pursuant to an inquiry/investigation shall be prescribed by rules.

CHAPTER X
PROVISIONS RELATING TO STORAGE AND TRANSFER OF DATA

42. Storage of sensitive data, user created or generated data and classified data.- The sensitive data, user created or generated data and classified data shall be stored in Bangladesh, and shall remain beyond the jurisdiction of any court and law enforcers other than Bangladesh.

43. Transfer of data as mentioned in section 42.- (1) Any classified data specified by the Government, from time to time, by general or special order, may not be transferred to a place or system outside Bangladesh if it is not authorized so by the Government.

(2) Notwithstanding anything contained in any other provisions of this Act-

(a) a data subject by his consent to meet his necessity, may transfer any data including sensitive and user created data,

(b) for the purpose of maintaining international relations, cross-border business, immigration or any other data as specified by the Government, from time to time, may transfer any data,

to any country or organization outside Bangladesh or international organizations.

CHAPTER XI

DATA PROTECTION REGISTER

44. Data protection register.- (1) The Director General shall keep and maintain a data protection register as may be prescribed.

(2) The Director General shall register in the data protection register as may be prescribed, every person or organization collecting or processing data and the purpose for which the data is collected or processed.

(3) Every controller shall record and maintain, under his supervision, the collection, processing, retention, structuring, subtraction, storage, adaptation, modification, return of data and other matters relating thereto of a data subject under this Act in an accurate and up-to-date manner, following the procedure as may be prescribed by rules.

45. Access to register by public.- The director General shall make the information contained in the data protection register available for inspection by any person.

CHAPTER XII

COMPLAINTS, ADMINISTRATIVE FINES, ETC.

46. Filing of Complaints.- A data subject or any person who believes that a data controller, data processor or data collector is infringing upon their rights or acted, in violation of the provisions of this Act, may make a complaint to the Director General in such manner as may be prescribed.

47. Inquiry and remedy of the complaints.- (1) The Director General shall make inquiry or investigation, as the case may be, of every complaint made under this chapter and may direct a data controller, data processor or data collector to remedy any breach or take such action as he may specify with a view to removing the element of the complaint and restore the rights of the data subject.

(2) If the Director General is satisfied that, after completion of inquiry or investigation, as the case may be, of the relevant complaint, any controller, processor, collector or any other person authorized to do so has failed to perform any activity in accordance with the provisions of this Act, or has done anything inappropriate, then he may take required action to file a case or legal proceedings against the controller, processor, collector or the authorized person.

(3) The Director General may give necessary instructions to the controller, processor, collector or authorized person to restore the rights of the data subject provided in this Act.

48. Unlawful processing of data.- (1) Any person who processes or cause to be processed, disseminates or discloses data in violation of any of the provisions of this Act shall be liable to an administrative fine not exceeding to taka three lac and in case of a subsequent violation of unlawful processing of data, the fine may extend up to taka five lac.

(2) In case the offence committed under sub-section (1) relates to sensitive data the offender may be liable to an administrative fine not exceeding to taka five lac.

49. Failure to adopt appropriate data security measures.- Any person who fails to adopt the security measures that are necessary to ensure data security, when he is required to do so, in violation of the provisions laid down in this Act and the rules made there under shall be liable to an administrative fine not exceeding to taka three lac.

50. Failure to comply with orders made under this Act.- Any person who fails to comply with the orders made under this Act, when he is required to do so, shall be liable to an administrative fine not exceeding to taka two lac.

51. Obtaining, transferring or selling of data.- (1) Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act, obtains data, or discloses data, or transfers data to another person, or sells or offers to sell data to another person, which results in harm to a data subject, then such person shall be liable to an administrative fine not exceeding to taka three lac.

(2) In case the offence committed under sub-section (1) relates to sensitive data the offender may be punished with a fine not exceeding to taka five lac.

52. Certain violations may be prescribed.- (1) Violation of any of the provisions of this Act which is not specifically mentioned in this chapter or elsewhere, may be dealt within the scope of administrative fines, and the process and extent of such fines may be prescribed.

(2) As a recourse to the violation mentioned in sub-section (1) shall subject to fines which may extent to Taka five lac.

53. Compensation for failure to comply with this Act.- Where a data subject suffers damage or distress through the contravention of any provision of this Act, caused by a data controller, data processor or data collector, the data subject may apply to the Director General seeking compensation from the data controller, data processor or data collector for such damage or distress.

54. Violations of certain provisions of this Act by a foreign company.- If any foreign company registered under Chapter 10 of the Companies Act, 1994 (Act No. XVIII of 1994) violates the provisions of section 48, 49, 50, 51 and 52 shall be liable to an administrative fine which may extend to 5% (five percent) of its total turnover of the preceding financial year.

55. Imposition of Administrative fines.- (1) The Director General may, subject to other provisions of this section, giving the person concerned a reasonable opportunity of hearing, impose an administrative fines on an amount as prescribed in sections 47, 48, 49, 50, 51, 52 and 54, and in other cases the amount as prescribed by the rules.

(2) If a person fails to pay the administrative fine imposed on him under this Act, within the time prescribed by the rules, it shall be recoverable under the Public Demand Recovery Act, 1913 (Act 1X of 1913) as a government due.

(3) The amount of administrative fine to be imposed in certain cases in accordance with the severity of the complaint under this Act shall be determined by the rules.

56. Appeals.- (1) Any person aggrieved by a decision under this chapter may appeal to the Government, in the prescribed manner, within thirty days from the date of the decision.

(2) For filing an appeal, its copy shall be given to the Director General and the authority as may be prescribed.

CHAPTER XIII

COMPLAINTS TURNED TO OFFENCES AND RELATED MATTERS

57. Director General's power to return the complaint with specific direction.- (1) Violation to any provision of this Act to be filed with the Director General and the complaints which are, to ensure justice, following due process, appears to the Director General that administrative fine is not adequate may return the complaint to the complainant with specific direction as to proper relief.

(2) The complaint as mentioned in sub-section (1) shall be returned as soon as possible but not later than thirty days.

(3) If the Director General fails to return the complaint to the person concerned within the time prescribed under sub-section (2), the person may submit an application to the Government for appropriate remedy in that regard.

58. The limit of fine and punishment.- In awarding fine and punishment in the cases arising out of complaint as mentioned in section 56, the court of competent jurisdiction may award a fine which may extend to Taka ten lac, or with imprisonment which may extend to three years, or with both.

59. Power to investigate offences.- Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (V of 1898), any qualified officer engaged under Director General shall investigate any offence under this Act.

60. Trial of offence and appeal.- (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (V of 1898) or any other law for the time being in force, the offences committed under this Act shall be tried by the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 only.

(2) Any person aggrieved with the order or judgment of the Tribunal mentioned in sub-section (1) may prefer an appeal before Appellate Tribunal constituted under section 82 of the Information and Communication Technology Act, 2006.

61. Application of the Code of Criminal Procedure.- (1) Save as anything contrary to the provisions of this Act, the provisions of the Code of Criminal Procedure, 1898 shall be applicable to the investigation, trial, appeal and all other incidental matters related to any offence under this Act.

(2) The Cyber Tribunal mentioned in sub-section (1) of section 59 shall be deemed to be a Court of Session, and may exercise all powers of a Court of Session while trying any offence under this Act or any other offence derived from it.

(3) The person presenting the case before the said Tribunal on behalf of the complaint shall be regarded as public prosecutor.

62. Offences committed by companies.- (1) Where a company violates any provisions of this Act or fails to comply with an order or direction issued under this Act or rules made there under, than the owner, director, manager, secretary or any other officer or agent of the company shall be deemed to have violated such provision or failed to comply with the order or direction, unless he can prove that the violation or failure was beyond his knowledge or that he exercised due diligence to prevent such violation or failure.

Explanation.- For the purpose of this section—

(a) "company" means any statutory public authority, registered company, partnership, firm and association or organization;

(b) "director" in relation to a commercial establishment includes any partner or member of the board of directors.

(2) Where a company mentioned in sub-section (1) is a body corporate, such company, apart from any person charged and convicted under that sub-section, may also be charged and convicted under that sub-section in the same proceedings, but the penalty of fine only may be imposed on such company in a criminal proceeding.

CHAPTER XIV

MISCELLANEOUS

63. Power of Government to issue directions in certain cases.- (1)The Government may, from time to time, issue to the Director General such directions as it may think necessary in the interest of the sovereignty and integrity of Bangladesh, the security of the State, friendly relations with foreign States or public order.

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

64. Reports, etc.- The Director General shall furnish to the Government such reports and statements as the Government may, from time to time, require.

65. Delegation of powers.- The Director General may, by general or special order, in writing, delegate to any officer of the data protection office or of any authorized officer, subject to such conditions, if any, as may be specified in the order, such of its powers and functions under this Act as it may deem necessary.

66. Data processed before the date of coming into operation of this Act.- Where a data controller has collected data from the data subject or any third party before the date of coming into operation of this Act, he shall comply with the provisions of this Act within the time as may be prescribed by rules from the date of coming into operation of this Act.

67. Power to remove difficulties.- If any difficulty arises in giving effect to the provisions of this Act, the Government may, by order, published in the Official Gazette, make such provisions not inconsistent with the provisions of this Act as may appear to be necessary or expedient for removing the difficulty.

68. Power to make rules.- The Government may, by notification in the official Gazette, make rules to carry out the purposes of this Act.

69. Publication of English text.- (1) After the commencement of this Act, the Government may, by notification in the official Gazette, publish an authentic English text of this Act.

(2) In the event of conflict between the Bangla and the English text, the Bangla text shall prevail.

Statement of object and reasons

Minister in charge.

Date: 16 July 2022