

THE PERSONAL DATA PROTECTION ACT

Bill no. , 2020

An Act to protect the citizens of Bangladesh against the violation of their privacy and of personal data by regulating the collection, processing, holding, using and disclosure of personal information/data respecting the rights of freedom of thought and dignity of persons with regard to their right to privacy, right to life and personal liberty; to provide for the rights of the persons whose data is collected and the obligation of data controllers, data collectors and data processor; and for matters connected therewith and ancillary thereto;

Whereas it is expedient to protect the citizens of Bangladesh against the violation of their privacy and of personal data by regulating the collection, processing, holding, using and disclosure of personal information/data respecting the rights of freedom of thought and dignity of persons with regard to their right to privacy, right to life and personal liberty; to provide for the rights of the persons whose data is collected and the obligation of data controllers, data collectors and data processor; and for matters connected therewith and ancillary thereto;

It is hereby enacted as follows:-

CHAPTER I

PRELIMINARY

1. Short title and commencement.—(1) This Act may be called the Personal Data Protection Act, 2020.

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

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

- (a) “anonymised data” means data which has undergone the process of anonymisation under this Act;
- (b) “commercial transaction” means any transaction of a commercial nature, whether contractual or not, which includes any matters relating to the supply or exchange of goods or services, agency, investments, financing, banking and insurance;
- (c) “data” means information which is intentionally processed by means of equipment operating automatically or otherwise in response to instructions as part of a relevant data filing system and includes any representation of data that can be processed electronically;
- (d) “data controller” means a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorizes the processing of any personal data, but does not include a data processor;
- (e) “data processor”, in relation to personal data, means any person, other than an employee of the data controller, who processes the personal data solely on behalf of the data controller, and does not process the personal data for any of his own purposes”;
- (f) “data subject” means an individual who is the subject of the personal data;
- (g) “Director General” means the Director General of the Digital Security Act, 2018;
- (h) “personal data” means any information that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data controller, including any sensitive personal data and expression of opinion about the data subject which—
 - (i) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
 - (ii) is recorded with the intention that it should wholly or partly be

processed by means of such equipment; or

(iii) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system:

Provided that anonymised, encrypted or pseudonymized data which is incapable of identifying an individual is not personal data;

(i) “personal data protection office” means the personal data protection office established under this act;

(j) “processing”, in relation to personal data, means collecting, recording, holding or storing the personal data or carrying out any operation or set of operations on the personal data, including—

(i) the organization, adaptation or alteration of personal data;

(ii) the retrieval, consultation or use of personal data; and

(iii) the disclosure of personal data by transmission, transfer, dissemination or otherwise making available; or

(iv) the alignment, combination, correction, erasure or destruction of personal data;

(k) “third party”, in relation to personal data, means any person other than a data subject, a relevant person in relation to a data subject, a data controller, a data processor, or a person authorized in writing by the data controller to process the personal data under the direct control of the data controller;

(l) “rules” means rules made under this Act; and

(m) “sensitive personal data” means personal data consisting of information revealing racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership in political parties, trade unions, organizations and associations with a religious, philosophical, political or trade-union, biometric or genetic data, or provide information as to the health or sexual life of an individual, 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 and financial, or any other personal data as the Commission may determine by order published in the official Gazette;

- (n) “vital interests” means matters relating to life, death or security of a data subject. *[May be added more if necessary]*

3. Overriding effect of this Act.- Save as otherwise expressly provided under this Act, the provisions of this Act shall have an overriding effect to the extent that such provisions are inconsistent with any other law for the time being in force or any instrument having effect by virtue of any such law.

4. Application.- (1) This Act applies to any person who processes, and any person who has control over or authorizes the processing of, any personal where such data has been collected, disclosed, shared or otherwise processed within the territory of Bangladesh

(2) Subject to sub-section (1), this Act applies to a person in respect of personal data if—

- (a) the person is established in Bangladesh and the personal data is processed, whether or not in the context of that establishment, by that person or any other person employed or engaged by that establishment; and
- (b) the person is not established in Bangladesh, but uses equipment in Bangladesh for processing the personal data otherwise than for the purposes of transit through Bangladesh.

Explanation.- For the purpose of this sub-section,-

- (a) a person falling under this clause shall nominate a representative established in Bangladesh for the purposes of this Act;
- (b) each of the following is deemed to be as established in Bangladesh-
 - (i) an individual whose physical presence in Bangladesh shall not be less than one hundred and eighty days in one calendar year;

(ii) a body incorporated under the Companies Act, 1995;
(iii) a partnership or other unincorporated association formed under any written laws in Bangladesh; and

(iv) any person who does not fall within paragraphs (a), (b) or (c) but maintains an office, branch or agency through which he carries on any activity, or a regular practice in Bangladesh.

(3) Notwithstanding anything contained in sub-sections (1) and (2), this Act shall not apply to-

(a) processing of personal data by a person in the course of a purely personal or household activity or family purposes;

(b) processing of personal data exclusively for journalistic, artistic or literary purposes subject to the conditions as may be prescribed by rules;

(c) processing of anonymised data;

(d) processing of personal data by a government entity for the purposes provided in any other laws for the time being in force subject to the condition of ensuring security and secrecy for the protection and confidentiality of personal data.

CHAPTER II

PERSONAL DATA PROTECTION

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

(a) **Consent and accountability:** be accountable to the data subject for the data collected, and the personal data, other than sensitive personal data, process personal data of a data subject with his consent to the processing of the personal data and in the case of sensitive personal data, process

- sensitive personal data of a data subject except in accordance with the provisions of this Act and rules made thereunder;
- (b) **Fair and reasonable:** collect and process such personal data in a fair and reasonable manner that respects t of this Act and rules made thereunder he privacy of the data subject and following the provisions of this Act and rules made thereunder;
 - (c) **Integrity:** collect, process, hold or use adequate, relevant and not excessive or unnecessary personal data and take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up-to-date by having regard to the purpose;
 - (d) **Retention:** retain personal data for the period authorised by this Act and rules made thereunder and for which data is required to ensure that all personal 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 personal data held and be able to correct that personal data where the personal 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 personal data, and subject to the provisions of this Act, no personal data shall, without the consent of the data subject, be disclosed for any purpose other than the purpose for which the personal data is to be disclosed at the time of collection of the personal data;
 - (g) **Security:** observe security safeguards in respect of data and when processing personal data, take proper steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction.

CHAPTER III

PROCESSING OF PERSONAL DATA

6. Protection of personal data.- The processing of personal data shall only be done in compliance with the provisions of this Act.

7. Requirements for personal data processing.- (1) Personal data including sensitive personal 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 personal 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 personal data in accordance with sub-section (2).

(4) Where the data subject withdraws consent for the processing of any personal 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 personal 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 interests of the data subject;

(e) for where the data controller can reasonably be expected to obtain the consent of the data subject

(f) for the administration of justice pursuant to compliance with any order of the court of competent jurisdiction;

(g) for explicitly mandated under any law for the time being in force;

(h) for legitimate interests pursued by the data controller;

(i) for the exercise of any function of the Government authorised by law for the provision of any service or benefit to the data subject from, or the issuance of any certification, license or permit for any action or activity of the data subject by, the Government; or

- (j) for the exercise of any functions conferred on any person by or under any law for the time being in force;
- (k) for any public interest in processing for reasonable purpose as may be prescribed by rules.

(6) Personal data shall not be processed unless-

- (a) the personal data is processed for a lawful purpose directly related to an activity of the data controller;
- (b) the processing of the personal data is necessary for that purpose; and
- (c) the personal data is adequate but not excessive in relation to that purpose.

8. Notice to the data subject.- (1) A data controller shall by written notice inform a data subject, no later than at the time of collection of the personal data or, if the data is not collected from the data subject, as soon as is reasonably practicable—

- (a) the purposes for which the personal data is to be processed;
- (b) the categories of personal data being collected;
- (c) the identity and contact details of the data controller and the contact details of the data protection officer, if applicable;
- (d) the right of the data subject to withdraw such consent, and the procedure for such withdrawal, if it is processed on the basis of consent;
- (e) the basis for such processing, and the consequences of the failure to provide such personal data;
- (f) the source of such collection, if the personal data is not collected from the data subject;
- (g) the individuals or entities including other data controller or data processors, with whom such personal data may be shared, if applicable, or the third parties to whom the data controller may disclose the personal data ;
- (h) information regarding any cross-border transfer of the personal data that the data fiduciary intends to carry out, if applicable;
- (i) the legal basis for the processing of personal data and time duration for which data is likely to be processed and retained thereafter;

- (j) the data subject's right to request access to and correction of the personal data and how to contact the data controller with any inquiries or complain in respect of personal data;
- (k) whether it is obligatory or voluntary for the data subject to supply the personal data; and
- (l) any other information as may be specified by the Director General.

(2) The data controller shall provide the information as required under this section to the data subject in a clear, concise and readily accessible comprehensible means to a reasonable person and in Bangla languages.

(3) The notice under sub-section (1) shall be given as soon as reasonably possible/practicable by the data controller when the data subject is first asked by the data controller to provide his personal data; or when the data controller first collects the personal data of the data subject; or before the data controller uses the personal data of the data subject for a purpose other than the purpose for which the personal data was collected and discloses the personal data to a third party.

9. Protection of privacy.- A data collector, data processor or data controller shall not collect, hold or process personal 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 authorised by the data controller in this behalf may collect the personal data directly from data subject.

(2) Notwithstanding anything contained in sub-section (1), personal data may be collected 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 authorised source;
- (c) the collection of the data from another source is not likely to prejudice the privacy of the data subject;
- (d) the collection of the data is necessary for the prevention, detection, investigation of an offence or for the national security.

CHAPTER IV

PROCESSING OF SENSITIVE PERSONAL DATA

11. Processing of sensitive personal data.- (1) Subject to subsection (2) of section 6, a data controller shall not process any sensitive personal 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 personal data;
- (b) the processing is necessary—
 - (i) 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
 - (ii) 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;
 - (iii) 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;
 - (iv) for medical purposes and is undertaken by a healthcare professional; or a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;
 - (v) for the purpose of, or in connection with, any legal proceedings;
 - (vi) for the purpose of obtaining legal advice while ensuring its integrity and secrecy;
 - (vii) for the purposes of establishing, exercising or defending legal rights;
 - (viii) for the administration of justice pursuant to orders of a court of competent jurisdiction; or
 - (ix) for the exercise of any functions conferred on any person by or under any law; or
- (c) the information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

(2) The Director General may by order exclude the application of clauses (i), (viii) or (ix) of clause (b) of subsection (1) in such cases as may be specified in the order, or provide that, in such cases as may be specified in the order, any condition in clauses (i), (viii) or (ix) of clause (b) of subsection (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

Explanation.- For the purposes of this section—

“medical purposes” includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services;

“healthcare professional” means a medical practitioner, dental practitioner, pharmacist, clinical psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist and other allied healthcare professionals and any other person involved in the giving of medical, health, dental, pharmaceutical or any other healthcare services authorised to provide such services.

CHAPTER V

PERSONAL DATA OF CHILDREN

12. Personal data relating to children.- (1) A person shall not collect or process personal data relating to a child unless the collection or processing thereof is-

- (a) carried out with the prior consent of the parent or guardian or relevant person having authority to make decisions on behalf of the child;
- (b) necessary to comply with the law; or
- (c) for research or authorised statistical purpose.

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

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

Explanation.- “relevant person”, in relation to a data subject, means-

- (a) in the case of a data subject who is below the age of 18 years, the parent or a guardian appointed by a court of competent jurisdiction;

- (b) in case of a data subject who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs; or
- (c) a person authorized by the data subject to make a data access or data correction request or both such requests.

CHAPTER VI

DATA SUBJECT RIGHTS

13. Right of access to personal data.- (1) An individual is entitled to be informed by a data controller whether personal data of which that individual 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 personal data, in writing, to the data controller for the following information —

- (a) for information of the data subject's personal data that is being processed by or on behalf of the data controller;
- (b) to have communicated to him a copy of the personal data in an intelligible form
- (c) confirmation whether the data controller is processing or has processed personal data of the data subject;
- (d) a brief summary of -
 - (i) the personal data of the data subject being processed or that has been processed by the data fiduciary;
 - (ii) processing activities undertaken by the data controller with respect to the personal data of the data subject;
- (e) the purposes of the processing;
- (f) the categories of personal data concerned;
- (g) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
- (h) the envisaged period for which the personal data will be stored;

(i) where the personal data are not collected from the data subject, any available information as to their source.

(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 personal data, but controls the processing of the personal data in such a way as to prohibit the data controller who holds the personal data from complying, whether in whole or part, with the data access request under sub-section (2) which relates to the personal data, the first mentioned data controller shall be deemed to hold the personal 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 personal data is being processed, the data subject shall have the right to obtain the correction of inaccurate or misleading personal data, the completion of incomplete personal data, and the updating of personal data that is out of date from the data controller processing personal 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 personal data, that the same is disputed by the data subject.

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

(5) Where a data controller does not hold the personal data, but controls the processing of the personal data in such a way as to prohibit the data controller who

holds the personal data from complying, whether in whole or in part, with the data correction request under sub-section (1) which relates to the personal 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.

Withdrawal of consent to process personal data

15. Withdrawal of consent.- (1) A data subject may by notice in writing withdraw his consent to the processing of personal 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 personal 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.

16. Right to Data Portability.- (1) The data subject shall have the right to—

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

(i) which such data subject has provided to the data controller;

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

(iii) which forms part of any profile on the data subject, or which the data controller has otherwise obtained.

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

(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 for the time being in force.

17. Rights of foreign data subjects.- Foreign data subject shall have all his rights, if any provided under the laws of the country where the foreign data has been collected or data subject resides in so far as consistent with this Act.

18. Right to erasure (Right to be Forgotten).- (1) The data subject shall have the right to obtain from the data controller the erasure of personal data concerning him without undue delay and the data controller shall have the obligation to erase personal data within a period as may be prescribed by rules where one or more of the following condition applies-

- (a) the personal 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 personal data have been unlawfully processed; or
- (e) the personal data have to be erased for compliance with a legal obligation.

(2) Where the data controller has made the personal data public and is obliged pursuant to sub-section (1) to erase the personal data, the data controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform data processors which are processing the personal data that the data subject has requested the erasure by such data controllers of any links to, or copy or replication of, those personal data.

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

- (a) for exercising the right of freedom of expression and information;
- (b) for compliance with a legal obligation or for the performance of a task carried out in the public interest;
- (c) for reasons of public interest in the area of public health; or

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

19. Right to prevent processing of personal 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 personal 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 inform the data subject in writing 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 specified.

(2) A data controller shall comply with a data access request under this chapter not later than days as may be prescribed by rules from the date of receipt of the data access request.

(3) A data controller who is unable to comply with a data access request within the period specified in subsection (2) shall before the expiration of that period by notice in writing inform the requestor that the data controller is unable to comply with the data access request within such period and the reasons why the data controller is unable to do so, and comply with the data access request to the extent that the data controller is able to do so.

(4) The data controller may charge a reasonable fee as may be prescribed by rules to be paid for complying with requests made under this Chapter.

(5) The Director General may specify a reasonable time period within which the data controller shall comply with the requests under this Chapter, and such time period shall be communicated to the data subject along with the acknowledgement referred to in sub-section (1).

(6) Where any request made under this Chapter is refused by the data controller, it shall provide the data subject making such request with adequate reasons for such refusal as per the provisions of this Chapter in writing.

(7) The data controller is not obliged to comply with any request made under this Chapter where such compliance would harm the rights of any other data controller under this Act.

(8) The manner and procedure of exercise of rights, including the circumstances where data controller may refuse to comply with data access request, under this Chapter shall be in such form as may be prescribed by rules.

CHAPTER VII

TRANSPARENCY AND ACCOUNTABILITY

21. Accountability.- (1) The data controller shall be responsible for complying with all obligations set out in this Act in respect of any processing undertaken by it or on its behalf, and 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 personal data and shall make the following information available in an easily accessible form as may be specified—

- (a) the categories of personal data generally collected and the manner of such collection;
- (b) the purposes for which personal data is generally processed;
- (c) any categories of personal data processed in exceptional situations or any exceptional purposes of processing that create a risk of significant harm;
- (d) the existence of and procedure for the exercise of data subject rights mentioned in Chapter V, and any related contact details for the same;

- (e) the existence of a right to file complaints to the Authority;
- (f) where applicable, any rating in the form of a data trust score that may be accorded to the data controller;
- (g) where applicable, information regarding cross-border transfers of personal data that the data controller generally carries out; and
- (h) any other information as may be specified prescribed by rules.

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

23. Non-disclosure of personal data.- Subject to the provisions section xxx, no personal data shall, without the consent of the data subject, be disclosed for any purpose other than the purpose for which the personal data was to be disclosed at the time of collection of the personal data; or a purpose directly related to such purpose, or to any party other than a third party as specified in section 7.

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

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

- (a) to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction;
- (b) to the place or location where the personal data is stored;
- (c) to any security measures incorporated into any equipment in which the personal data is stored;
- (d) to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and
- (e) to the measures taken for ensuring the secure transfer of the personal data.

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

26. Data Retention requirements.- (1) The personal 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 personal 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 personal 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 personal data was collected and further processed.

(2) A data subject shall be given access to his personal data held by a data controller and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-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 personal 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 by rules.

28. Data protection impact assessment.- (1) The controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

(2) A single assessment may address a set of similar processing operations that present similar high risks.

(3) The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

(4) A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data or of personal data relating to offences under this Act or any other laws for the time being in force; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

(5) The personal data protection office shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment.

(6) The assessment shall contain-

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects; and

(d) the measures envisaged to address the risks taking into account the rights and legitimate interests of data subjects and other persons concerned.

(7) Compliance with approved codes of conduct as may be prescribed by rules by the relevant controllers or processors shall be taken into due account in assessing the

impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

Alternative

28. Data Protection Impact Assessment. – (1) Where the data controller intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, or any other processing which carries a risk of significant harm to data subjects, such processing shall not be commenced unless the data controller has undertaken a data protection impact assessment in accordance with the provisions of this section.

(2) The Director General, with prior approval of the Government, may, in addition, specify those circumstances, or classes of data controllers, or processing operations where such data protection impact assessment shall be mandatory, and may also specify those instances where a data auditor under this Act shall be engaged by the data controller to undertake a data protection impact assessment.

(3) A data protection impact assessment shall, among others, contain-

- (a) detailed description of the proposed processing operation, the purpose of processing and the nature of personal data being processed;
- (b) assessment of the potential harm that may be caused to the data subjects whose personal data is proposed to be processed; and
- (c) measures for managing, mitigating or removing such risk of harm.

(4) Upon completion of the data protection impact assessment, the data protection officer shall review the assessment prepared and shall submit the same to the Director General in such manner as may be prescribed by rules.

(5) On receipt of the assessment, if the Director General has reason to believe that the processing is likely to cause harm to the data subject, he may direct the data controller to cease such processing or direct that such processing shall be subject to such conditions as may be prescribed by rules.

29. Personal data breach notification.- (1) In the event of a personal data breach, data controller shall without undue delay and where reasonably possible, not beyond the period as may prescribed, of becoming aware of the personal data breach, notify the Director General in respect of the personal data breach except where the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.

(2) In the event of delay in notifying personal data breach beyond the period as may prescribed mentioned in sub-section (1), the personal data breach notification to the Director General shall be accompanied by reasons for the delay.

(3) The personal data breach notification shall at least provide the information as prescribed by rules.

(4) The data controller shall maintain record of any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken.

(5) The data processor shall follow the personal data breach notification requirements under this section in event of becoming aware of a personal data breach.

30. Data audits.- (1) The data controller shall have its policies and the conduct of its processing of personal data audited annually by an independent data auditor as authorised by Director General under this Act.

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

(3) The manner, forms and procedure for conducting audits 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 (having regard to factors such as independence, integrity ability, etc.) as data auditors under this Act.

(5) Notwithstanding anything contained in sub-section (1), where the Director General is of the view that the data controller is processing personal 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.

31. Responsibility of the data controller.- (1) 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, the data controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Act.

(2) The measures referred to in sub-section (1) shall include the implementation of appropriate data protection codes of conduct and policies by the data controller.

(3) In addition to the responsibility mentioned in sub-sections (1) and (2), the data controller shall undertake such other responsibility as may be prescribed by rules.

32. Data protection officer. - (1) For the purpose of carrying out the following functions the data controller shall appoint a data protection officer—

- (a) providing information and advice to the data controller on matters relating to fulfilling its obligations under this Act;
- (b) monitoring personal data processing activities of the data controller to ensure that such processing does not violate the provisions of this Act;
- (c) providing advice to the data controller where required on the manner in which data protection impact assessments must be carried out, and carry out the review of such assessment;
- (d) providing advice to the data controller, where required on the manner in which internal mechanisms may be developed in order to satisfy the principles set out under this Act;
- (e) providing assistance to and cooperating with the personal data protection office on matters of compliance of the data controller with provisions under this Act;
- (f) act as the point of contact for the data subject for the purpose of raising grievances to the data controller; and
- (g) maintaining an inventory of all records maintained by the data controller;

- (h) any other functions as may be assigned to him as it may consider necessary by the data controller from time to time;
- (i) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Act;
- (j) to monitor compliance with this Act including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- (k) to provide advice where requested as regards the data protection impact assessment;
- (l) to cooperate with the personal data protection office;
- (m) to act as the contact point for the supervisory authority on issues relating to processing.

(2) 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.

(3) The data protection officer shall meet the eligibility and qualification requirements to carry out its functions as may be prescribed by rules.

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

- (a) managerial, organisational, business practices and technical systems are designed in a manner to anticipate, identify and avoid harm to the data subject;
- (b) technology used in the processing of personal data is in accordance with commercially accepted or certified standards;
- (c) legitimate interests of businesses may be achieved without compromising privacy interests and the interest of the data subject is accounted for at every stage of processing of personal data;

- (d) privacy must be protected throughout processing from the point of collection to deletion of personal data to the extent of their processing, storage and accessibility; and
- (e) processing of personal data is carried out in a transparent manner.

CHAPTER VIII

EXEMPTION

34. Exemption.- (1) There shall be exempted from the provisions of this Act personal data processed by an individual only for the purposes of that individual's personal, family or household affairs, including recreational purposes.

(2) Subject to section 35, personal data-

(a) processed for-

- (i) the prevention or detection of crime or for the purpose of investigations;
- (ii) the apprehension or prosecution of offenders; or
- (iii) the assessment or collection of any tax or duty or any other imposition of a similar nature, shall be exempted from the related provisions of this Act as may be prescribed by the Government;

(b) processed in relation to information of the physical or mental health of a data subject shall be exempted from the related provisions of this Act as may be prescribed by the Government of which 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 individual;

(b) processed for preparing statistics or carrying out research shall be exempted from the related provisions of this Act as may be prescribed by the Government, provided that such personal data is not processed for any other purpose and that the resulting statistics or the results of the research are not made available in a form which identifies the data subject;

(c) that is necessary for the purpose of or in connection with any order or

judgment of a court shall be exempted from the related provisions of this Act as may be prescribed by the Government;

- (d) processed for the purpose of discharging regulatory functions shall be exempted from the related provisions of this Act as may be prescribed by the Government, if the application of those provisions to the personal data would be likely to prejudice the proper discharge of those functions; or
- (f) processed only for journalistic, literary or artistic purposes shall be exempted from the related provisions of this Act as may be prescribed by the Government.

35. Power to make further exemptions.- (1) The Government may, by order 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).

(3) The Government may, at any time, by order published in the Gazette, revoke any order made under subsection (1).

(4) An appeal against an order passed by the Government under subsection (1) shall lie to the High Court Division.

CHAPTER IX

PERSONAL DATA PROTECTION OFFICE

36. Establishment of the personal data protection office.- (1) As soon after the commencement of this Act, the Government shall, by notification in the official Gazette, establish, for carrying out the purposes of this Act, an office to be called Personal Data Protection Office.

(2) Personal data protection office established under sub-section (1) shall be-

- (a) under direct control and administration of Digital Security Agency constituted under Digital Security Act, 2018; and
- (b) headed by the Director General of the Digital Security Agency.

(3) Personal data protection office shall consist of such officers and other employees as it consider necessary for the efficient performance of its functions of the office on such terms and conditions as may be prescribed by the Government.

37. Powers of the personal data protection office.- (1) Subject to the other provisions of this Act, the personal 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 personal 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 information it requires for the performance of its tasks;
- (ii) to carry out investigations in the form of data protection audits;
- (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 personal data and to all information 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;
- (ii) to order the controller or the processor to comply with the data subject's requests to exercise his rights pursuant to this Act;

- (iii) to order 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 order the controller to communicate a personal data breach to the data subject;
- (v) to impose a ban on processing;
- (vi) to order the rectification or erasure of personal data;
- (vii) to impose an administrative fine under this Act;
- (viii) to order the suspension of data flows to a recipient in a third country or to an international organisation;

(c) Authorisation and advisory powers:

- (i) to advise the controller in accordance with the prior consultation procedure;
- (ii) to issue to other institutions and bodies as well as to the public on any issue related to the protection of personal data;
- (iii) to adopt standard data protection guidelines;
- (iv) to authorise administrative arrangements.

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

- (a) oversee the implementation of and be responsible for the enforcement of this Act;
- (b) promote the protection and observance of the right to privacy and of personal data;
- (c) monitor, investigate, and report on the observance of the right to privacy and of personal data;
- (d) formulate, implement and oversee programs 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 personal data;
 - (h) perform such other functions as may be prescribed by rules as it consider necessary for the promotion, implementation and enforcement of the Act;
 - (i) to do all other acts and things ancillary or incidental to any of the aforesaid functions.

39. Codes of conduct/practice.- (1) The Director General, with prior approval of the Government, shall issue codes of conduct/practice in accordance with this section to promote good conduct/practices of data protection and facilitate compliance with the obligations under this Act.

(2) A code of conduct/practice shall not be issued unless the Director General has undertaken a requisite consultation process with relevant stakeholders and has followed the procedure for issuance of such code of practice, as may be prescribed.

(3) Without prejudice to sub-sections (1), or any other provision of this Act, the Director General may issue codes of conduct/practice in respect of the following matters—

- (a) requirements for notice under section 7 of this Act including any model forms or guidelines relating to notice;
- (b) measures for ensuring quality of personal data processed and pertaining to the retention of personal data under this Act;
- (c) conditions for valid consent under this Act;
- (d) processing of personal data, of sensitive personal data and of personal data of children ;

- (e) exercise of any right by data subjects under this Act;
- (f) the standards and means by which a data subject may avail the right to data portability under this Act;
- (g) transparency and accountability measures including the standards thereof to be maintained by data fiduciaries and data processors under this Act;
- (h) standards for security safeguards to be maintained by data fiduciaries and data processors under this Act;
- (i) methods of de-identification and anonymisation;
- (j) methods of destruction, deletion, or erasure of personal data where required under this Act;
- (k) manner in which data protection impact assessments may be carried out by the data controller;
- (l) cross-border transfer of personal data;
- (m) any other matter which may require issuance of a code of practice.

(4) Non-compliance by the data controller or data processor with any code of practice issued under this section shall be deemed to be violated the provisions of this Act.

(5) The Director General, with the prior permission of the government, may review, modify or revoke a code of practice issued under this section in the manner prescribed by rules.

40. 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 sub-section the data controller or data processors shall be bound to comply with such directions.

41. 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.

42. Power to conduct inquiry/investigation. - (1) The Director General may conduct an inquiry/investigation where it has reasonable grounds to believe that—

- (a) the activities of the data controller or data processor being conducted in a manner which is detrimental to the interest of data subjects; or
- (b) any data controller or data processor has violated any of the provisions of this Act or the rules prescribed, or directions issued by the Director General thereunder.

(2) For the purpose of sub-section (1), the Director General may, by an order in writing, appoint 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 detailed procedure for inquiry/investigation and the action to be taken pursuant to an inquiry/investigation shall be prescribed by rules.

CHAPTER X

TRANSFER OF PERSONAL DATA OUTSIDE BANGLADESH

43. Transfer of personal data to places outside Bangladesh.- (1) A data controller shall not transfer any personal data of a data subject to a place outside Bangladesh unless to such place as specified by the Government, by notification published in the official Gazette.

(2) For the purposes of subsection (1), the Minister may specify any place outside Bangladesh if there is in that place in force any law which is substantially similar to this Act, or that serves the same purposes as this Act, or that place ensures an adequate level of protection in relation to the processing of personal data which is at least equivalent to the level of protection afforded by this Act.

(3) Notwithstanding anything contained in sub-section (1), a data controller may transfer any personal data to a place outside Bangladesh if-

- (a) the data subject has given his consent to the transfer;

- (b) the transfer is necessary for the performance of a contract between the data subject and the data controller;
- (c) the transfer is necessary for the conclusion or performance of a contract between the data controller and a third party which is entered into at the request of the data subject, or is in the interests of the data subject;
- (d) the data controller has reasonable grounds for believing that in all circumstances of the case the transfer is for the avoidance or mitigation of adverse action against the data subject;
- (e) the data controller has taken all reasonable precautions and exercised all due diligence to ensure that the personal data will not in that place be processed in any manner which, if that place is Bangladesh, would be a contravention of this Act;
- (f) the transfer is necessary in order to protect the vital interests of the data subject; or
- (g) the transfer is necessary as being in the public interest in circumstances as determined by the Government.

Alternative

43. Restrictions on cross-border transfer of personal data, etc.- (1) Every data controller shall ensure the storage on a server or data centre located in Bangladesh of at least one serving copy of personal data to which this Act applies.

(2) The Government may notify categories of personal data as critical personal data that shall only be processed in a server or data center located in Bangladesh.

(3) Notwithstanding anything contained in sub-section (1), the Government may notify certain categories of personal data as exempt from the requirement under sub-section (1) on the grounds of necessity or strategic interests of the country.

(4) Nothing contained in sub-section (3) shall apply to sensitive personal data.

(5) Personal data other than those categories of sensitive personal data may be transferred outside the territory of Bangladesh where -

- (a) the transfer is made subject to standard contractual clauses or intra-group schemes as approved by the Government; or
- (b) the transfer is permitted by the Government to a particular country, or to a sector within a country or to a particular international organisation; or
- (c) the Government approves a particular transfer or set of transfers as permissible due to a situation of necessity; or
- (d) the data subject, being satisfied,-
 - (i) has consented to such transfer of personal data; or
 - (ii) has explicitly consented to such transfer of sensitive personal data, which does not include the categories of sensitive personal data.

(6) The Government may prescribe the permissibility of transfers under clause (b) of sub-section (1) where it finds that the relevant personal data shall be subject to an adequate level of protection, having regard to the applicable laws and international agreements, and the effectiveness of the enforcement by authorities with appropriate jurisdiction, and shall monitor the circumstances applicable to such data in order to review decisions made under this sub-section.

(7) Sensitive personal data notified by the Government may be transferred outside the territory of Bangladesh—

- (a) to a particular person or entity engaged in the provision of health services or emergency services where such transfer is strictly necessary for prompt action under Act; and
- (b) to a particular country or a prescribed sector within a country or to a particular international organisation that has been prescribed under clause (b) of sub-section (1), where the Government is satisfied that such transfer or class of transfers is necessary for any data controller or data subject and does not hamper the effective enforcement of this Act.

(8) Any transfer under sub-section (3) shall be notified to the Government/Director General within such time period as may be prescribed by rules.

CHAPTER XI

COMPLAINTS

44. Complaints against breach and non-compliance.- (1) A data subject or any person who believes that a data controller, data processor or data collector is infringing upon their rights or is acted in violation of the provisions of this Act may make a complaint in the manner as may be prescribed by rules to the Director General.

(2) A data controller, data processor or data collector may, in writing, make a complaint in the manner as may be prescribed by rules to the Director General about any violation or non-compliances with this Act.

Alternative

44. Complaint.- (1) Any aggrieved person may file a complaint before the Director General against any violation of personal data protection rights as granted under this Act, and conduct of any data controller, data processor or their processes which a complainant regards as involving-

- (a) a breach of data subject's consent to process data;
- (b) a breach of obligations of the data controller or the data processor in performance of their functions under this Act;
- (c) provision of incomplete, misleading or false information while taking consent of the data subject; or
- (d) any other matter relating to protection of personal data.

(2) The complainant may file a complaint on a plain paper or on a simplified sample format prescribed by rule.

(3) The Director General may charge reasonable fee for filing or processing of the complaint as prescribed under this Act and shall also facilitate on-line receipt of complaints.

(4) The Director General shall acknowledge the receipt of complaint within three working days and shall dispose of the complaint under intimation to the complainant within thirty days of its receipt, or, for reasons to be recorded in writing, within such extended time as reasonably determined by the Commission.

(5) After receipt of the complaint, the Commission may seek explanation from the data controller or data processor against whom the complaint has been made by affording him reasonable time and opportunity to be heard through an efficient mode of communication, and contact, if deemed necessary, the complainant to seek further information or his comments on the response of the data controller or the data processor or any other concerned agency.

(6) The Director General shall efficiently dispose of a complaint and it may issue directions to stop breach of data protection rights of a data subject without first seeking comments from the concerned data processor and data controller, as the case may be.

(7) The Director General may employ electronic means of communication to dispose of complaints and shall maintain appropriate record of such communications.

(8) The Commission may, as soon as possible, establish an online facility to receive, process, manage and dispose of complaints in an efficient and cost effective manner.

(9) In case of failure of the data collector or data processor, as the case may be, to respond to the Director General or to execute its orders, he may initiate enforcement proceedings as per rules prescribed under this Act.

45. Investigation of the complaints.- The Director General shall investigate 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 to restore the integrity of data collected, processed or held by the data controller, data processor or data collector or the rights of data subject.

46. Compensation for failure to comply with this Act.- (1) Where a data subject suffers damage or distress through the contravention by a data controller, data processor or data collector of the requirements of this Act, the data subject is entitled to apply to an authority as may be specified by the rules for compensation from the a data controller, data processor or data collector for such damage or distress.

(2) In proceeding against a person under this section, it is a defense to prove the person took reasonable care in all the circumstances to comply with the requirements of this Act.

47. Administrative fines.- (1) The Director General may impose administrative fines in respect of infringements or for violations of the provisions of this Act and the rules made thereunder.

(2) Administrative fines shall, depending on the circumstances of the case, be imposed in addition to, or instead of, measures taken under this Act and the rules made thereunder.

(3) When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each case due regard, as prescribed by rules, shall be given.

(4) The amount and detail procedure for imposition of administrative fines under this Act shall be determined by rules.

48. Appeals.- (1) Any person aggrieved by a decision under this this chapter may appeal, within thirty days from the date notice of the decision, to the government.

(2) A copy of the appeal shall be provided to the Director General.

CHAPTER XII

OFFENCES

49. Unlawful processing of personal data.- Anyone who processes or cause to be processed, disseminates or discloses personal data in violation of any of the provisions of this Act shall be punished with ----- (*only fines may be imposed*) ---- and in case of a subsequent unlawful processing of personal data, the fine may exceed to -----(*only fines may be imposed*) ----- .

(2) In case the offence committed under sub-section (1) relates to sensitive data the offender may be punished with -----(*only fines may be imposed*) -----
--

50. Failure to adopt appropriate data security measures.- Anyone 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 thereunder shall be punished with -----(*only fines may be imposed*) -- .

51. Failure to comply with orders.- Anyone who fails to comply with the orders made under this Act, when he is required to do so, shall be punished -----(*only fines may be imposed*)----- .

52. Obtaining, transferring or selling of sensitive personal data contrary to the Act.- Any person who alone or jointly with others, knowingly or intentionally or recklessly, in contravention of the provisions of this Act—

- (a) obtains sensitive personal data; or
- (b) discloses sensitive personal data; or
- (c) transfers sensitive personal data to another person; or
- (d) sells or offers to sell sensitive personal data to another person,

which results in harm to a data subject, then such person shall be punished with ---
----- (*both imprisonment and fine may be imposed*) ----- .

53. Re-identification and processing of de-identified personal data. - (1) Any person who, knowingly or intentionally or recklessly re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be, or re-identifies and processes such personal data without the consent of such data fiduciary or data processor, then such person shall be punished with -----
-----(*both imprisonment and fine may be imposed*) ----- .

54. Certain offences may be specified/prescribed in the rules.- Subject to the other provisions of this section, certain offences and penalties for such offences may be specified in the rules, but the penalty so specified shall not exceed imprisonment for 2 (two) years/----- years or a fine of Tk. ----- or both.

55. Offences to be cognizable and non-bailable.- Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (V of 1898), an offence punishable under this Act shall be cognizable and non-bailable.

56. Power to investigate offences.- Notwithstanding anything contained in the Code of Criminal Procedure, 1898 (V of 1898), a police officer not below the rank of Inspector shall investigate any offence under this Act.

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

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

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

Explanation.- For the purpose of this section—

(a) “company” means any body corporate, and includes a firm; and an association of persons or a body of individuals whether incorporated or not.

(b) “director” in relation to a firm, means a partner in the firm; and an association of persons or a body of individuals, means any member controlling affairs thereof.

CHAPTER XIII

MISCELLANEOUS

58. 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.

59. Reports, etc.- The Director General/personal data protection office shall furnish to the Government such reports and statements as the Government may, from time to time, require.

60. Protection of action taken in good faith. - No suit, prosecution or other legal proceedings shall lie against the Director General and employee or officer of the personal data protection office for anything which is done in good faith or intended to be done under this Act, or the rules made thereunder.

61. Delegation of powers.- The Director General may, by general or special order, in writing, delegate to any officer of the personal data protection office or of any authorised 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.

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

63. Power to exempt certain data processors.- The Government may, by notification in the official Gazette, exempt from the application of this Act or any provisions of this Act for processing of personal data of data subjects not within the territory of Bangladesh, pursuant to any contract entered into with any person outside the territory of Bangladesh.

64. Public servant.- The Director General, any officer or employee of the personal data protection office or any authorized officer while discharging his duty or performing his functions or exercising his powers under this Act in such capacity shall be deemed to be a public servant within the meaning of the section 21 of the Penal Code (Act V of 1860).

65. Protection against suit and legal proceedings.- No action, suit, prosecution or other proceedings shall lie or be brought, instituted or maintained in any court

against the Director General or any officer or employee of the personal data protection office or any authorized officer in respect of any act or omission done or omitted by him or it in good faith in such capacity.

66. Personal data processed before the date of coming into operation of this Act.- Where a data controller has collected personal 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 make rules.- (1) The Government may, by notification in the official Gazette, make rules to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely-

[Items of rules may be specified here for the purpose of this Act]

Statement of object and reasons

Minister in charge.