Personal Data Protection Ordinance, 2025

(Ordinance No. 61 of 2025)

[November 06, 2025]

To take measures to protect the personal data of an individual, considering it as his property, and to make provisions for matters related to and incidental thereto.

Ordinance

Whereas it is appropriate and necessary to make provisions for the lawful processing of an individual's personal data with his consent, considering it to be his property; and

Whereas the processing of personal data requires the respect of fundamental rights of individuals, in particular the confidentiality, integrity, protection and security of data, as well as fairness, interoperability, the potential of the digital economy and the promotion of responsible innovation; and

Whereas it is necessary to ensure the fulfillment of the responsibilities and remedies assigned to the data controller and processor by taking measures to conduct and audit the above processing lawfully; and

Whereas Parliament is in a state of dissolution and it appears to the President to his satisfaction that the circumstances exist which require immediate action;

Therefore, by virtue of the powers conferred by Article 93 (1) of the Constitution of the People's Republic of Bangladesh, the President has made and promulgated the following Ordinance:-

CHAPTER ONE

Early

Short title, application and introduction

1. (1) This Ordinance may be called the Personal Data Protection Ordinance, 2025 .

(2) This shall apply to any person, data controller, processor, person involved in processing or any other person performing any duty or function under this Ordinance, who-

(a) a citizen of Bangladesh, resident in Bangladesh, ordinarily resident in Bangladesh, working in Bangladesh or temporarily staying in Bangladesh for business purposes;

(b) processes personal data within Bangladesh, except for the transfer of personal data through Bangladesh; or

(c) Processes personal data outside Bangladesh in connection with any activity related to the provision of products or services or monitoring or record management of data subjects located within Bangladesh.

(3) Except for section 23 and sections 31 to 46, this Ordinance shall come into force immediately, and after the expiry of 18 (eighteen) months from the date of promulgation of the Ordinance, the said sections shall come into force on such date as the Government may, by notification in the Official Gazette, appoint.

Definition.

2. Unless the subject or context otherwise requires, in this Ordinance-

(1) “Financial Data” means any type of transaction, by whatever name called, ongoing or completed by the data subject with a financial or any other institution, whether digital or otherwise (mode and methodology), or any information or data identifying any person, or any information or data collected or stored, which is helpful in determining the transaction;

(2) “Data-fiduciary” means a person who, alone or jointly, processes personal data for a specific purpose or supervises it for that purpose or authorizes another person to process personal data;

(3) “data subject” means any natural person to whom personal data relates, whether identified or identifiable, whether living or dead;

“Authority” means the National Data Management Authority established under Section 8 of the National Data Management Ordinance, 2025 ;

(5) “Significant data-fiduciary” means a data-fiduciary determined by regulation on the basis of the following matters;

(a) the potential impact on the sovereignty of the State;

(b) the amount of data or the financial implications of the data processed;

(c) Risk to the rights of the data subject;

(d) Potential threats to national security, public order, public safety, economic order and public health;

(6) “Pseudonymized Data” means any personal data processed by the data subject which does not allow the data subject to be identified without the use of additional information stored separately;

“Genetic Data” means data relating to the genetic characteristics of an individual, inherited from his or her ancestors, which provide other information about the behavioral characteristics, physiological condition or health of that individual and which is data obtained from the analysis of a biological sample or bodily fluid of that individual;

(8) “Tribunal” means the Cyber Tribunal constituted under section 68 of the Information and Communication Technology Act, 2006 (Act No. 39 of 2006);

(9) “Retention” means the storage of data in such a way that the data subject can be identified and the main purpose for which the data was collected exists, or the data is required for the lawful conduct or processing of the data;

(10) “Auditor” means any independent data auditor referred to in sub-section (1) of section 21;

(11) “Processing” means any operation which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, retention, transfer, adaptation or alteration, retrieval, use, disclosure by transmission, dissemination or otherwise making available, dissemination or otherwise making available, dissemination or otherwise making available, restriction, destruction or erasure;

(12) “processor” means any person who processes personal data on behalf of the data controller;

(13) “Regulations” means regulations made under this Ordinance;

(14) “profiling” means the automated processing of personal data of an individual to evaluate, analyse or predict aspects relating to that individual’s performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, habits, location or movements;

(15) “Biometric Data” means personal data generated through the measurement or technical processing of physical, physiological or behavioural characteristics of an individual, which is capable of otherwise identifying or confirming the identity of a specific individual, including deoxyribonucleic acid (DNA), blood group, fingerprints, facial images, iris scans, voiceprints and gait patterns, etc.;

(16) “Rules” means rules made under this Ordinance;

(17) “Person” means-

In the case of a data subject, any natural person; or

In the case of a data controller or processor, the legal entity;

(18) “Personal Data” means any information relating to an individual, such as name, parents’ names, identification number, mobile number, financial data, location data or any other similar online identifier or any

other factor containing physical, physiological, genetic, biometric, psychological, economic characteristics of an individual and any other factor containing characteristics prescribed by regulations, by which that individual can be identified;

(19) “Personal Data Breach” means a breach of security of personal data resulting in unauthorized access to or unlawful transfer, disclosure, alteration of any personal data processed under this Ordinance, or in the absence of equipment necessary for proper processing and storage, resulting in the possibility of accident, destruction, loss, intrusion;

(20) “Personally Identifiable Information” means information that can be used to uniquely identify or identify an individual;

(21) “Child” means a person below the age of 18 (eighteen) years or such age as may be prescribed by the Government;

(22) “Consent” means a clear, explicit, specific and freely given positive indication by the data subject for data processing;

(23) “Sensitive Personal Data” means any of the following personal data of the data subject, namely:-

(a) Genetic data;

(b) biometric data;

(c) Data related to small ethnic groups and communities;

(d) Data relating to political or philosophical opinions, religious beliefs or any other ideology or belief of a similar nature;

(e) Data relating to membership of any trade union;

(f) Health-related data;

(g) data related to sexual orientation;

(h) Personal data relating to the commission of a crime, criminal proceedings and convictions;

(i) Data relating to crimes alleged to have been committed by the data subject;

(j) Data relating to the momentary location or instantaneous geo-location of a data subject; and

(k) any other personal data prescribed by rules or regulations;

(24) “Health data” means the data subject’s—

(a) any data relating to physical or mental condition;

(b) Records relating to the past, present or future health status of the data subject;

(c) other data related to the provision of healthcare; and

(d) This shall also include personal data collected during the registration, payment or provision of healthcare services of the data subject;

(25) “Encryption” means the conversion of any data or communication using a standard cryptographic algorithm and one or more cryptographic keys in such a way that the data is not intelligible or reconstructible except with the appropriate key, and only authorized parties can decrypt it to verify its integrity or authenticity or gain access to the original data.

Precedence of ordinances

3. Notwithstanding anything to the contrary contained in any other law for the time being in force, the provisions of this Ordinance shall remain in force.

Extra-state application of the ordinance

4. (1) If any citizen of Bangladesh commits any offence under this Ordinance outside Bangladesh which, if committed in Bangladesh, would have been punishable under this Ordinance, the provisions of this Ordinance shall apply as if he had committed the said offence in Bangladesh.

(2) If any person commits an offence under this Ordinance from outside Bangladesh within Bangladesh, the provisions of this Ordinance shall apply against that person as if the entire process of that offence had been committed in Bangladesh.

(3) If any person commits an offence under this Ordinance from within Bangladesh outside Bangladesh, the provisions of this Ordinance shall apply as if the entire process of the said offence had been committed in Bangladesh.

CHAPTER TWO

Collection and processing of personal data

Lawful basis for processing personal data

5. (1) A data controller or processor may process personal data of a data subject with the consent of the data subject in accordance with the provisions of this Ordinance or the regulations made thereunder and subject to the provisions of sub-section (2).

(2) Every consent given under sub-section (1) shall be freely given, specific, unambiguous and revocable, and the consent shall be obtained by informing the data subject of the purpose of the data processing, the retention period, the transfer and the withdrawal procedure.

(3) Notwithstanding anything contained in sub-section (1), the data controller may process data without consent, subject to the conditions of usefulness, necessity, proportionality and purpose limitation of the processing, in accordance with the provisions laid down by the regulations, if the following legitimate grounds exist, namely:-

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

(b) taking necessary measures at the request of the data subject for the purpose of performing the contract;

(c) necessary for the establishment of any legal right or the exercise or defence of any suit or legal proceedings;

(d) Protection of vital interests related to the protection of life or health;

(e) the implementation of legal rights relating to employment, labor rights or social security;

Voluntary public disclosure by the data subject; and

(g) The likelihood of harm to another person as a result of unreasonably withholding consent from the data subject or another person on his or her behalf.

(4) The burden of proof regarding the proper consent of the data subject shall lie with the data controller in accordance with the provisions of this Ordinance.

Conditions for further processing of personal data

6. A data controller may, if necessary, further process the personal data of the data subject in accordance with this Ordinance or rules or regulations, if it is compatible with the main purpose.

Conditions for processing sensitive personal data

7. A data controller may, subject to the provisions of sections 5 and 6, process any sensitive personal data of a data subject subject to the following conditions, namely:-

(a) obtaining the specific consent of the data subject;

(b) execution of a contract by the data subject as a party;

(c) the performance of duties under any right or obligation conferred or imposed by any law relating to employment and social security in the course of the duties to be performed by the data controller;

(d) the performance of medical duties by health workers and the performance of emergency medical duties related to the risk to the life or health of the data subject;

(e) the performance of any duty imposed on any person by or under any law; and

Voluntary disclosure of any of the data subject's personal data to the public.

Data processing methods by the processor

8. (1) The data controller may, under a valid contract, appoint or otherwise engage a processor to process personal data on its behalf for the purpose of carrying out any activity related to the supply of goods or services to the data subject.

(2) Where any personal data processing operations are carried out by a processor on behalf of the data controller for the purposes of this Ordinance or the rules or regulations made thereunder, the processing of such personal data shall be deemed to have been carried out by the data controller, and the data controller shall be liable in respect thereof under this Ordinance.

(3) Every data controller shall take reasonable steps to ensure that the processor engaged in the processing of personal data on his behalf carries out the processing tasks assigned to him in due compliance with this Ordinance or the regulations made thereunder, and he shall also be liable for the actions of the processor.

Processing of personal data relating to children or individuals who are not capable of giving consent

9. (1) The data controller may collect or process personal data of a child or a person who is not capable of giving consent, in accordance with the procedure prescribed by the regulations, with the consent of the child or a person who is not capable of giving consent, either by his/her parents or legal guardian or by any person empowered to make decisions on his/her behalf.

(2) Personal data of a child or a person who is not capable of giving consent shall be processed with due regard to the protection and protection of the rights and interests of the child or a person who is not capable of giving consent.

(3) The data controller shall not conduct activities such as tracking, monitoring, profiling or targeted advertising of a specific child using his/her behavior or other data.

(4) Consent given by a parent or legal guardian or a person empowered to make decisions on behalf of a child or a person who is not capable of giving consent shall remain valid until the child reaches the age of 18 (eighteen) years or until the person who is not capable of giving consent attains the capacity to give consent, and in that case, the data controller or processor may take action under that consent.

CHAPTER THREE

Data subject rights

General conditions for the exercise of rights over personal data by the data subject

10. (1) The data subject may exercise his rights under this Chapter by making a written application to the data controller.

(2) The procedure for the acknowledgement of receipt of a request received by the data controller under sub-section (1), the action to be taken in response to the request, and the compliance with the request if accepted, and other matters related thereto, shall be prescribed by regulations.

(3) Upon receipt of the data subject's request, the data controller shall take appropriate steps to assess the sensitivity and risk of fraud of the data concerned at the beginning of the processing, and shall, where applicable, keep the actions taken for audit purposes and inform the data subject.

(4) The rights set forth in this Chapter shall be universal, inherent, inalienable and inviolable, and shall not be abrogated or derogated from by contract or notice.

Right to access and

portability

11. (1) The data subject shall have access to the data processed by the data controller.

(2) Upon receipt of a request from the data subject, the data controller shall provide the data subject with the personal data collected and processed by it in the manner prescribed by the regulations; and, where applicable, may arrange for the direct transfer of data to another data controller using Federated Interoperable Ecosystems.

(3) Upon request of the data subject, a copy of the personal data processed by the data controller shall be provided in a concise and intelligible format and shall include, in the manner prescribed by the regulations, a summary of the data, the activities undertaken, the purpose, type, recipients, retention, source, safeguards for cross-border transfers, a description of the rationale and significance of automated decisions, and other matters covered by this right.

(4) A copy of the personal data provided in response to a request under sub-section (3) shall be accompanied by a statement of the identity of all other persons, data controllers or processors with whom it has been shared.

(5) In cases where the provision of the requested data is likely to jeopardize national security, law and order or infringe upon the rights of third parties, the data controller shall inform the authority in writing and take further action as decided by the authority.

(6) The frequency limit of requests, the time limit for receipt, response and settlement of requests, and other matters relating to the provision of data by the data controller to the data subject shall be determined by regulations.

Explanation.- For the purposes of this section, “Federated Interoperable Ecosystem” means a process where multiple operators, while maintaining control, responsibility and accountability over their respective affiliated data, exchange the minimum required information in a secure and standardized manner upon mutual request.

Right to rectification, updating and completion of data

12. (1) The data subject shall have the right, taking into account the purposes of the processing of personal data, to have inaccurate or misleading personal data rectified, incomplete personal data completed, and, where necessary, to have personal data held by the controller for processing rectified, completed or updated if they are not up-to-date, and the data subject may request the controller to carry out such activities.

(2) If, in response to a request under sub-section (1), the data controller refuses to rectify, complete or update the requested personal data, taking into account the purposes of the processing, he shall inform the data subject in writing of the reasonable grounds for refusal.

(3) Where the data subject is not satisfied with the justification provided by the data controller under sub-section (2), he may request the data controller to mark the relevant personal data as objectionable and to inform the authority of the matter.

(4) If the data controller corrects, completes or updates any personal data in response to a request received under sub-section (1), he shall, within a maximum of 30 (thirty) days, inform the data subject and all concerned thereof.

(5) The procedure for submitting and processing requests for correction, completion or updating of personal data under this section, correction, completion, updating of personal data by the data controller and other matters shall be prescribed by regulations.

Withdrawal of consent, objection to processing and consequences

13. (1) The data subject may withdraw his consent, in whole or in part, to the following matters at any time in the simplified manner specified in the regulations, namely:-

(a) Personal data protection;

(b) processing of personal data; or

(c) Automated decision-making regarding personal data.

(2) The data controller shall, upon the request of the data subject, delete all personal data of the data subject concerned stored with him in the manner prescribed by the regulations, if-

(a) the purposes for which the personal data were processed no longer exist;

(b) the data subject withdraws the consent on the basis of which the data was processed;

(c) the data subject objects to the processing of the data in accordance with the provisions of this Ordinance;

(d) the personal data is processed unlawfully; and

(e) The erasure of personal data is necessary to comply with a legal obligation or to comply with other conditions prescribed by regulation.

(3) The data controller may refuse to delete data requested by the data subject if it is:

(a) relates to an ID that can be used to identify an individual while the data subject's consent continues;

(b) is intended for preservation purposes or for use in archives;

(c) is reserved for compliance with legal obligations;

(d) is confidential personal data; and

(e) Personal data is restricted.

(4) The lawfulness of processing carried out while the data subject's consent is in force shall not be impaired by the withdrawal of consent.

(5) If it appears to a data subject that there is a possibility that he or she will be harmed if any of his or her personal data is processed, he or she shall communicate with the data controller expressing his or her desire to withdraw the processing, and in light of that desire, the data controller shall inform the data subject and cease the processing.

(6) The data controller shall not undertake, conduct or perform any activity involving the processing, withdrawal, transfer or otherwise processing of personal data by automated means without informing the data subject under this Ordinance or any other law as applicable.

System-wide propagation of corrections, completions, and removals

14. (1) In processing a request approved under section 12 or 13, the original data controller shall, where applicable, follow the system-wide propagation procedure prescribed by the regulations.

(2) The Authority shall, taking into account practical importance and perspective, determine the priority order of the sources of the data field by considering the source which is logically at the top of the priority list as the primary source and, as applicable, ensure that the relevant records of any other data controller or processor (data field and alike) are consistent with the primary source.

(3) Primary data-custodian-

(a) verify and implement the update or deletion through its own system; and

(b) Inform the Authority of the applicable areas and precautions to be followed regarding retention, as applicable, in the manner prescribed by the regulations.

(4) After being so informed, the authority-

(a) shall issue an order to all secondary data controllers and processors concerned by the approved change to immediately implement the change in an automated manner; and

(b) Every change and acknowledgement of receipt shall be recorded in an immutable ledger, blockchain or equivalent technology, for correction, audit and verification.

(5) Once the primary source of personal data of any individual has been determined in order of accuracy in the process of system-wide propagation, it shall not be used for all actions and needs of that individual other than a "current address" other than that, in any other government or private registry, license, financial transaction, acquisition or relinquishment of ownership of any subject or property, or in any other case.

(6) The system-wide propagation referred to in sub-section (4) shall also apply to copies of the mirror, cache, backup, DR, test environment, migration dataset held by any data custodian or processor or data user.

(7) The steps taken to implement the system-wide propagation process shall be completed within the time limit specified by the regulations, and, as applicable, such steps shall be recorded in an immutable ledger and such information shall be submitted to the Authority.

(8) In cases where there is a possibility of the records being distorted as a result of deleting personal data, only requests to delete data of public interest or archival/scientific/historical records specified by the authority may be rejected, but in this case the reasons for the rejection must be mentioned and an appeal against the rejection may be filed.

Explanation.- If specific data of an individual (e.g., “current address”) is stored in separate registries of more than one ministry, commission, agency or institution and discrepancies are observed between the said

data, the concerned authority shall determine the primary source by considering the following factors:

(a) Primary methods of data collection and standards of accuracy;

(b) Data quality and regular updates;

(c) the reliability and verifiability of the data source; and

(d) Capability of automated or semi-automated processes.

After determining the "Order of Precedence" through this evaluation, the registry that appears to be the most accurate and authoritative will be considered the Primary Source of Truth, and based on that information, the relevant fields of all other registries will be corrected automatically or following a system-wide propagation process.

Example: If the “Current Address” field of the passport registry is designated as the primary source, the “Current Address” field of the individual in the registries of all other ministries, commissions or authorities will be automatically updated and in the case of a person who does not have a passport, the next source determined in order of accuracy, such as national identity card, local government registration, utility bill, employment information, health information or information from the police, will have to be updated everywhere through a system-wide propagation process.

CHAPTER FOUR

Responsibilities and duties of the data controller and processor

Accountability and transparency

15. (1) The data controller or processor shall be responsible for fulfilling the responsibilities assigned to him in accordance with the provisions of this Chapter and Chapter Five, as well as all other sections, in the processing of personal data.

(2) The data controller or processor shall take reasonable steps to apply all the principles and practices of processing personal data in a transparent manner, and shall ensure the availability of information to all concerned, and in the event of performing any significant task related to the processing of personal data of any data subject, inform the data subject concerned as follows, namely:-

(a) the categories of personal data generally collected and the methods of collection thereof;

(b) the general purposes of processing personal data;

(c) details of the categories of personal data that may be at risk of being affected by the processing of personal data in particular circumstances or for particular purposes;

(d) Procedures for exercising rights by the data subject and contact details in this regard;

(e) Details of complaints filed with the authority regarding the exercise of rights by the data subject;

(f) Where applicable, information regarding the transfer of personal data by the data controller to another location;

(g) the identity of the data custodian and the method of easy communication with him; and

(h) Any other conditions prescribed by regulations.

(3) The forms and procedures for ensuring the availability of information under sub-section (2), informing the data holder on the relevant matters and other matters shall be prescribed by regulations.

(4) If compliance with the provisions of this section would involve disproportionate effort or expense, the data controller or processor shall take such action as may be prescribed by the competent authority.

Privacy of personal data

16. Subject to the other provisions of this Ordinance, personal data shall not be disclosed for any purpose other than the purpose for which the personal data was collected, without the consent of the data subject.

Personal data protection and security standards

17. (1) Every data controller and processor shall take appropriate technical and organizational measures in relation to the processing of personal data in such a way as to ensure the security, integrity and confidentiality of personal data and to prevent their accidental or unlawful destruction, loss, misuse or alteration, unauthorized disclosure or access.

(2) While taking action under sub-section (1), every data controller and processor shall consider the following matters, namely:-

(a) the amount of personal data and its sensitivity;

(b) the extent and nature of the potential harm to the data subject resulting from the loss, disclosure or other misuse of the personal data;

(c) the scope of the processing;

(d) the period of data retention; and

(e) Availability and potential cost of the technology, materials or other measures to be implemented.

(3) While taking measures under sub-section (1), the following measures shall also be included, namely:-

(a) pseudonymization of personal data;

(b) encryption of personal data;

(c) ensuring the security, integrity, confidentiality, availability and resilience of processing systems and services;

(d) timely restoration of availability and access to personal data in the event of a physical or technical incident;

(e) Periodic assessment of risks in the field of data processing systems, services and transmission through electronic communication networks;

(f) Regularly testing, evaluating and monitoring the effectiveness of the measures introduced against current and emerging risks; and

(g) Regular updating of measures taken and introduction of new measures to address operational deficiencies and address emerging risks.

(4) The Authority may, by regulation, prescribe the criteria for the technical and institutional arrangements referred to in sub-section (1).

(5) The processor shall be responsible for complying with the security standards prescribed under this section.

Personal data retention terms

18. (1) The data controller shall not retain any personal data for a period exceeding the period prescribed by the regulations for the purpose for which the personal data were processed.

(2) Notwithstanding anything contained in sub-section (1), the data controller may retain personal data for a period exceeding the period referred to in sub-section (1) for reasons of public interest, scientific or historical research or statistical purposes, until technical and administrative measures are implemented to protect the rights of the data subject.

Preservation of records.

19. (1) Subject to the provisions of section 18, the data controller shall, unless otherwise specifically provided for in any other provision, properly preserve in a register all records relating to personal data processed by him for a period of at least 5 (five) years.

(2) The data controller shall keep records of the processing, retention, structuring, allocation, storage, adaptation, modification, portability and other matters related to the processing of the data of the data subject

under this Ordinance, in accordance with the prescribed procedure.

Personal data security breach (Breach)

20. (1) If a personal data breach is likely to cause significant damage to the data subject concerned, the data controller shall notify the Authority of such personal data breach in the form, manner and within the time limit prescribed by the regulations.

(2) In determining the extent of data deviation by regulation, the Authority shall, among other things, consider the following factors:

(a) the nature of the personal data breach and, where applicable, the categories and approximate number of data subjects concerned and the personal data records concerned;

(b) the place and address of contact with the data controller; and

(c) Measures taken or to be taken by the data controller or relevant processor to address the personal data breach, including measures to be taken to mitigate its potential adverse effects.

Data audit

21. (1) Certain categories of data controllers, as prescribed by regulations, shall arrange for the audit of personal data processing activities at such times as may be determined by the Authority through an independent data auditor authorised by the Authority under sub-section (4).

(2) The auditor shall evaluate all matters to be complied with under the provisions of this Ordinance and the regulations made thereunder.

(3) The qualifications of the auditor and the methods, forms, procedures and other matters relating to the audit of personal data under this section shall be prescribed by regulations.

(4) For the purpose of carrying out the audit, the Authority may form an audit panel comprising of persons having knowledge related to information and communication technology, computer systems, personal

data, personal data protection or data privacy.

(5) Notwithstanding anything contained in sub-section (1), if it appears to the Authority that the manner in which the data controller is processing personal data may be harmful to the data subject, it may direct the data controller to have an audit carried out by an auditor appointed by it, and if any such direction is given, the data controller concerned shall be bound to comply with it.

Data protection plan

22. Every data custodian-

(a) Identifying the harm to the data subject, plan to establish appropriate standards of technical systems, including adherence to institutional norms and policies, in order to avoid such harm;

(b) follow the standards set by regulations in the use of technology in the processing of personal data;

(c) process data lawfully, maintaining confidentiality and the interests of the data subject at all stages of data processing; and

(d) Process personal data with transparency, in accordance with the procedures prescribed by regulations.

Chief Data Officer

23. (1) For the purpose of protecting personal data under this Ordinance, all significant data controllers shall appoint a sufficient number of qualified Chief Data Officers under their control.

(2) The Chief Data Officer shall perform his duties and perform his duties at the place determined by the Authority.

(3) For the purpose of this Ordinance, the duties and responsibilities of the Chief Data Officer shall be as follows, namely:-

(a) Representation of the data controller before the authorities;

(b) Reporting on important matters to the authorities and data custodians;

(c) Acting as a means of communication for the exercise of data subject rights; and

(d) Acknowledge receipt of complaints regarding misuse or inefficient management of sensitive personal data within the stipulated time frame and ensure effective remedies to resolve them.

(4) The Chief Data Officer shall be involved in the overall activities related to the processing of personal data and shall perform the duties assigned to him/her, taking into account the purpose, nature, scope and context thereof.

CHAPTER FIVE

Exemption matters

Exemption

24. (1) Notwithstanding anything contained in any other provision of this Ordinance, the consent of the data subject shall be deemed to be waived if the processing of personal data is necessary in the following cases, namely:-

(a) in the interests of national security, defence, public order or public interest;

(b) to comply with the lawful orders of a court of competent jurisdiction;

(c) the prevention, detection, investigation, prosecution or prosecution of crime;

(d) prevention or detection of tax evasion;

(e) public health, medical or medical public interest; such as responding to an emergency medical situation involving a threat to the life or health of the data subject or another person;

Investigation or investigation into the misuse of public funds;

(g) Use of the data subject for personal, recreational or household purposes;

(h) preparing statistics or conducting scientific or historical research;

(i) publishing in the public interest, journalism, archival education, artistic work or literary writing; and

(j) Any other matter prescribed by regulations relating to the above matters.

(2) The exemption from obtaining consent for data processing of the data subject under sub-section (1) shall in no way be deemed to exempt from the application of the provisions applicable to data processing, preservation, storage, retention, disclosure, etc.

(3) The provisions of sub-sections (1) and (2) shall apply to any person or institution involved in the processing of data, including the data controller.

(4) The exemption provision mentioned in this section shall not apply to the following matters, namely:-

(a) for the purpose of avoiding legal obligations under this Ordinance; or

(b) if it creates a disproportionate impact on the rights and freedoms of the data subject; or

(c) In the absence of legal authority, necessity or documented justification.

(5) In order to prevent repeated use of the exemption for malicious purposes, the Authority may, at its own discretion, or upon application by any data subject, examine and review the validity of such exemption, and if the Authority is satisfied that such malicious purpose exists, it shall inform the data subject and the data controller that the exemption is not applicable in that case.

(6) Notwithstanding anything contained in the other provisions of this section, the Authority may, by regulation, prescribe the responsibilities and duties of the data controller or any other person or institution involved in the processing and use of data, the nature of exemption, the period of validity, the action to be taken upon expiry of the period, and the rules for maintaining the list of exempted data.

CHAPTER SIX

Functions of the authorities etc.

Functions of the Authority

25. The Authority shall, in addition to the functions assigned to it under the provisions of the National Data Management Ordinance, 2025, perform any of the following functions, namely:-

(a) Ensuring matters related to the proper implementation of this Ordinance;

(b) Upholding the rights of data subjects as provided for in this Ordinance, taking measures to prevent and remedy violations and deviations thereof;

(c) Ensuring that the interests of the data subject are not harmed due to managerial weaknesses of the data controller or processor in data processing;

(d) ensuring the confidentiality, security, fairness and interoperability of the processed data;

(e) Take necessary steps to create and increase public awareness about the objectives and provisions of this Ordinance;

Formulation of guidelines for the efficient management of data processing operations;

(g) Supporting the safe use of personal data in research and development and innovation for the economic development of the public;

(h) To coordinate with the Chief Data Officers of various ministries and departments, government or semi-government, autonomous, statutory or special power institutions or organizations and domestic and foreign government and private companies for the implementation of this Ordinance and the rules, regulations or orders made thereunder; and

(i) To perform such other duties as may be necessary for the purpose of this Ordinance.

Authority power

26. The Authority may exercise any of the following powers for the purpose of performing the functions under this Ordinance, including the functions conferred upon it under the provisions of the National Data Management Ordinance, 2025 , namely:-

(a) To issue necessary instructions to the data controller and processor regarding the conduct of processing activities in accordance with the provisions of this Ordinance or the regulations made thereunder;

(b) Order the data controller or processor or, as the case may be, the representative authorized for this purpose to provide the personal data necessary for the work performed by it;

(c) giving notice to the data controller or processor of any alleged violation of the provisions of this Ordinance, rules or regulations;

(d) access to personal data held or stored by the data controller or processor, or to the equipment or personal data used in the said process, or to any premises, including the place of ongoing processing, for the purpose of examination;

(5) To warn and provide necessary instructions to the data controller or processor in case of processing of personal data in violation of the provisions of this Ordinance, rules or regulations;

(f) If any violation or omission of the rights of any data subject is observed in his personal data, to provide necessary instructions to the data controller to prevent such violation;

(g) Imposition of administrative fines in the manner prescribed by regulations in the areas specified in this Ordinance;

(h) Ordering the cessation or suspension of the provision of personal data to a customer in a foreign country or international organization;

(i) prescribing fees or levies by regulation, where applicable, for important data controllers and processors;

(j) to advise the Data Controller in the performance of his duties under this Ordinance, rules and regulations; and

(k) Providing instructions to all concerned to follow the policies related to personal data protection standards.

Formulation of Standard Operating Procedures

27. (1) The Authority shall, with the prior approval of the Government, formulate general operating procedures for the processing of personal data and other matters related thereto, subject to the provisions of this Ordinance, rules and regulations.

(2) Without prejudice to the scope of exercise of the powers mentioned in sub-section (1), the Authority may, inter alia, formulate general operating procedures on the following matters, namely:-

(a) the conditions for the data subject to give consent to the processing of personal data;

(b) the exercise of rights under this Ordinance by the data subject;

(c) matters related to the processing of personal data;

(d) measures to be taken to ensure the quality of personal data processing and retention;

(e) to formulate forms, etc., including the necessary conditions, relating to notification under this Ordinance;

(f) Exercise of the right to portability of personal data;

(g) measures to be taken by the data controller and processor to maintain standards of personal data processing, including transparency and accountability;

(h) pseudonymous data processing methods;

(i) Procedures for destruction, erasure and deletion of personal data;

(j) Personal Data Protection Impact Assessment Procedures;

(k) Procedures for transferring personal data outside Bangladesh; and

(l) Other matters necessary for carrying out the purposes of this Ordinance.

Authority's power to issue instructions.

28. (1) Subject to the provisions of this Ordinance, rules or regulations, the Authority may, for the purpose of discharging its duties and performing its functions, issue necessary instructions to the data controller or any person responsible for processing, storing and transferring data, to provide personal data or in any other matter related thereto, and if any such instructions are issued, it shall be binding on them to comply with them.

(2) The Authority may, in the direction given under sub-section (1), specify the time limit for compliance therewith.

CHAPTER SEVEN

Provisions regarding the classification, storage and transfer of personal data

Classification of personal data

29. (1) The Government may, taking into account the characteristics mentioned in the Schedule, classify personal data as follows, namely:-

(a) Public or open personal data;

(b) internal personal data;

(c) confidential personal data;

(d) Limited personal data.

(2) The Government may, if necessary, in consultation with the authorities, amend the Schedule in the light of the categories mentioned in sub-section (1).

(3) Any personal data classified under sub-section (1) may be transferred abroad subject to the conditions of this section, if it contains-

(a) the consent of the relevant data subject is obtained; or

(b) involves the exchange of goods or services through a contract to which the data subject is a party; or

(c) With the consent of the data subject, matters related to his/her interests such as business, education, emigration, immigration, etc.

(4) Personal data that is legally transferable may only be transferred to places or countries where appropriate technology and equipment for storing personal data as prescribed by regulations exist.

(5) The Government may, by notification in the Official Gazette, determine fees or charges on the annual business or commercial profits of any institution arising from the use of personal data of Bangladeshi citizens.

(6) In the case of cross-border transfers of large amounts of sensitive personally identifiable data, it is mandatory to notify the authorities.

Explanation.- In this sub-section, “sensitive personally identifiable data” means the following data, the large-scale cross-border transfer of which may pose a risk to national sovereignty, national security or financial stability; namely:-

(a) Government Unique Identification Number: e.g. (National Identity Card Number, Passport Number, Taxpayer/TIN/PAN);

(b) Biometric identifiers: e.g. (fingerprints, facial recognition data, iris scans);

(c) Genetic/DNA related information; and

(d) Criminal record or conviction information.

(7) In the case of transfer, storage, processing, etc. of any personal data to any cloud computer, domestic or foreign:

(a) A complete data dictionary of classified data as per clauses (c) and (d) of rule (1) shall be provided to the Authority;

(b) At least one synchronized real-time copy of all data stored in the cloud must be kept within Bangladesh;

(c) If the Authority finds or identifies evidence of a breach of data of a citizen of Bangladesh, due to the geographical location or commercial nature of the cloud used by a data custodian or processor, or any other reason that poses a threat to the national interest or public security of Bangladesh, then it may order such organization to reorganize, relocate, or terminate the use of such cloud within 60 (sixty) days.

(8) The Authority may make regulations for carrying out the purposes of this section.

Bilateral, multilateral and cross-border cooperation

30. The Government may, for the purpose of carrying out the purposes of this Ordinance, enter into agreements with any other country or multilateral organization or consortium or forum for the purpose of bilateral, multilateral and cross-border personal data exchange and other cooperation.

CHAPTER EIGHT

Filing complaints with authorities and administrative fines, etc.

File a complaint

31. If a data subject or any person has reason to believe that a data controller or processor has violated the rights of the data subject granted under this Ordinance or has acted in violation of the provisions of this Ordinance, then the said data subject or person may file a complaint with the Authority within the time and in the manner prescribed by the regulations.

Administrative fines if data subject's rights are violated

32. (1) If a data controller or processor fails to comply with any of the rights of the data subject as set out in this Ordinance, such failure shall constitute a breach of the provisions of this Ordinance and shall be liable to an administrative fine not exceeding 2% but not less than 1% of the annual turnover of its business in Bangladesh.

(2) If any important data controller commits a violation as referred to in sub-section (1), an administrative fine of not more than 5% but not less than 2% of the annual turnover of his business in Bangladesh may be imposed on him.

(3) In case of a second or repeated violation of the provisions of sub-sections (1) and (2), the Authority may impose a fine in addition to the administrative fine imposed under the said two sub-sections at the rate prescribed by the regulations.

Remedies for failure to provide proper protection and security of data

33. If any data controller or processor fails to provide protection and security of personal data as prescribed in this Ordinance, the rules or regulations made thereunder or the general operating procedures, then such failure shall constitute negligence in discharging the duties of the data controller or processor as prescribed in this Ordinance and an administrative fine not exceeding 25 (twenty-five) lakh taka may be imposed on him for that.

Some considerations in determining administrative fines

34. The authority may consider the following factors in determining the administrative fine, namely:-

(a) The nature, extent, seriousness, timing and recurrence of the failure to perform the duties;

(b) the extent of the potential loss to the data subject resulting from the failure to perform the obligation, and the potential gain to the data controller or processor;

(c) promptly inform the authorities of the steps taken by the data controller or processor in relation to the breach;

(d) the steps taken by the data controller or processor after becoming aware of the breach; and

(e) Any other matter prescribed by the Authority through regulations.

Compensation.

35. (1) While disposing of the complaint filed by the data subject under sections 32 and 33, the Authority may, at its own discretion or as requested by the data subject, determine the compensation, and such compensation shall be deemed to be in addition to the administrative fine.

CHAPTER 9

Crime and Punishment

Processing or disclosure of data without consent or legal basis

36. Any person, including a data controller or processor, without the necessary consent or legal basis under this Ordinance, for malicious purposes or with the intention of gaining profit-

(a) processes personal data; or

(b) provides, transfers or discloses personal data to a third party; or

(c) a third party receives the data;

In that case, such act of the said person shall constitute an offence and he shall be punished with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 10 (ten) lakh taka or with both.

Unauthorized processing of sensitive personal data

37. If any person, in contravention of section 7 or any other provision of this Ordinance, processes sensitive personal data without explicit consent or any other lawful basis, such act of that person shall be an offence and he shall be punished with imprisonment for a term not exceeding 7 (seven) years or with fine not exceeding 20 (twenty) lakh taka or with both.

Illegal collection or use of children's personal data

38. If a person collects, processes or uses the personal data of a child -

(a) without the prior verifiable consent of the child's parents or legal guardian under section 9; or

(b) fails to take reasonable steps to ascertain the identity and authority of the consenting guardian,

In that case, such act of the said person shall constitute an offence and he shall be punished with imprisonment for a term not exceeding (three) years or with a fine not exceeding 5 (five) lakh taka or with both.

Unauthorized access, interception, or extraction of personal data.

39. If any person-

(a) Gain access to any system, device, or database and interfere with or obtain personal data without authorization; or

(b) Interferes with any communication or data flow during the transmission of personal data,

In that case, such act by the said person shall be an offence and he shall be punished with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 10 (ten) lakh taka or with both.

Obtaining consent through deception

40. If any person-

(a) obtains the consent of any data subject by fraud, force, impersonation, misrepresentation or any other unfair means; or

(b) collects or processes personal data on the basis of such fraudulently obtained consent; or

(c) knowingly obtains such personal data for any profit-making or unfair purpose,

In that case, such act by the said person shall constitute an offence and he shall be punished with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 10 (ten) lakh taka or with both.

Misuse or disclosure of personal data collected in the course of official or professional duties

41. Any person, including a data controller, processor, employee, contractor, or agent, if—

(a) discloses, transfers or uses any sensitive personal data or personally identifiable information (PII) obtained in the course of performing official or contractual duties; or

(b) uses or processes data for any purpose other than the purpose permitted under this Ordinance,

In that case, such act by the said person shall constitute an offence and he shall be punished with imprisonment for a term not exceeding 5 (five) years or with a fine not exceeding 15 (fifteen) lakh taka or with both.

Unlawful tampering, destruction, etc. of personal data

42. If any person-

(a) intentionally damages, destroys, alters, forges, or misrepresents the personal data of another person; or

(b) manipulates personal data to produce misleading or harmful results in any automated or manual processing,

In that case, such act of the said person shall constitute an offence and he shall be punished with imprisonment for a term not exceeding 3 (three) years or with a fine not exceeding 5 (five) lakh taka or with both.

Continued use or processing of personal data after withdrawal of consent or expiry of the legal retention period

43. If a data controller or processor-

(a) continues to store, use or disclose personal data after the withdrawal of consent under section 13, or after the expiry of the statutory retention period under section 18; or

(b) fails to implement the deletion, rectification or blocking measures without undue delay within 30 (thirty) days of receipt of the request under this Ordinance,

In that case, such act of the said person shall be an offence and he shall be punished with imprisonment for a term not exceeding 3 (three) years or with a fine not exceeding 5 (five) lakh taka or with both.

Punishment for aiding and abetting a crime

44. If any person or organization supports or approves the commission of the crimes described in this chapter, or provides assistance in the commission thereof, that person or organization shall be punished with the same punishment as the perpetrator of the crime.

Trial

45. (1) Offences committed under this Ordinance shall be tried by a tribunal.

(2) In trying offences committed under this Ordinance, the Tribunal shall follow the procedure set out in Chapter IX of the National Data Management Ordinance, 2025 .

Compromiseability and bailability of crimes

46. Offences committed under this Ordinance shall be cognizable and bailable.

Remedy for violation of provisions by government or statutory bodies or institutions

47. (1) Notwithstanding anything contained in any other law applicable to Government servants or in any rule or regulation made thereunder or in any other document having the force of law, any Government servant engaged in any act which violates the rights of the data subject in the course of processing, storing or retaining or transferring or disclosing or transferring personal data shall be liable to administrative penalty under the provisions of this Ordinance and shall be deemed to have committed an offence punishable by a Tribunal if the breach occurs in the performance of the duties entrusted to him.

(2) Notwithstanding anything contained in any law applicable to any statutory or autonomous institution or any rule, regulation made thereunder or any other document or agreement having the force of law, any employee of a statutory or autonomous institution involved in the performance of any act which violates the rights of the data subject while processing, storing or retaining or transferring or disclosing or transferring personal data shall be liable to administrative fine under the provisions of this Ordinance and shall be deemed to have committed an offence punishable by a tribunal if the breach occurs while performing the duties entrusted to him.

(3) If the matter of violation or omission mentioned under sub-sections (1) and (2) arises, the employee, irrespective of the rank, who is involved in it or whose negligence in the performance of his duties has caused the said violation or omission to be committed with malicious intent, shall be held liable.

(4) The Government may make rules or regulations, as applicable, for the implementation of the provisions of sub-sections (1) and (2).

Crime committed

by the company

48. If any data subject raises an allegation of violation or default of his rights against a company under this Ordinance, then any member of the board of directors of the said company, managing director, or any office bearer related to the management of the company or any employee engaged in the day-to-day functioning of the company who is involved in the said violation shall be punishable with an administrative fine imposed by the authority in accordance with the provisions, and with imprisonment or fine imposed by the tribunal for default, or with both.

CHAPTER TEN

Miscellaneous

Power of the government to issue instructions in certain cases

49. (1) For the purpose of carrying out the purposes of this Ordinance, the Government may, from time to time, issue any directions to the authorities as it deems necessary in the interest of the sovereignty and integrity of Bangladesh, national security, friendly relations with foreign countries or public order.

(2) Without prejudice to the other provisions of this Ordinance, the Authority shall be bound to comply with such directions of the Government in the performance of its duties under this Ordinance.

Reports etc.

50. The Government may, from time to time, if necessary, call for reports or statements from the Authority on any matter dealt with under this Ordinance, and if any report is so called for, the Authority shall furnish the same to the Government.

Provisions to be followed regarding personal data processed

51. If a data controller has processed any personal data from a data subject or any other third party before the coming into force of this Ordinance, such processing of personal data shall continue -

(a) until there is no change to the purposes for which the processing was originally carried out; and

before the coming into force of this Ordinance

(b) If there is any change in the original purpose, then the prior consent of the data subject to the changed purpose shall be obtained in accordance with the provisions of the regulations.

Power to make rules.

52. (1) The Government may, by notification in the Official Gazette, make rules for carrying out the purposes of this Ordinance.

(2) The Government shall, with a view to finalizing the draft of the rules, seek the views of the stakeholders or the public on it within a period of 14 (fourteen) days and publish the draft on the website, and shall publish it in at least one widely circulated Bengali and one English daily newspaper on the subject.

(3) After the expiry of the period specified under sub-section (2), the draft rules shall be revised after reviewing the opinions received from the stakeholders and the public and shall be published in the official gazette.

Power to make regulations.

53. (1) The Authority may, by notification in the Official Gazette, make regulations for carrying out the purposes of this Ordinance, on any matter not covered by the rules.

(2) The Authority shall, with a view to finalizing the draft of the regulations, seek the views of the stakeholders or the public on it within a period of 14 (fourteen) days and publish the draft on the website, and shall publish it in at least one widely circulated Bengali and one English daily newspaper on the subject.

(3) After the expiry of the period specified under sub-section (2), the draft regulations shall be revised after reviewing the opinions received from the stakeholders and the public and shall be published in the Official Gazette with the approval of the Government.

The power of the

authority or government to issue orders in case of emergency

54. If the processing, storage, retention or transfer of the data subject's data by the data controller or processor is deemed necessary for the purpose of enforcement, the government or authority may, as the case may be, issue an order in this regard.

Publishing translated text in English

55. (1) After the commencement of this Ordinance, the Government shall, by notification in the Official Gazette, publish an Authentic English Text thereof.

(2) In case of conflict between the Bengali and English texts, the Bengali text shall prevail.