TRANSPARENCY
INTERNATIONAL
BANGLADESH
Social movement against corruption

The Revised Draft Data Protection Act (DPA) 2023
Review and recommendations in light of submissions on the earlier version

I. Introduction

In this era of ubiquitous use of the internet and digital platforms, nearly all human activities occur online, making extensive use of personal data. This makes personal data a key driving force in the digital realm. This digital landscape makes life easier, faster, prosperous, and more innovative but poses tremendous challenges to privacy, particularly protecting the right to personal data privacy. It is commendable that following the global trend, Bangladesh is working towards creating a legal framework for personal data protection by adopting a personal data protection law. Multiple rounds of drafting of a Personal Data Protection Act (DPA) have taken place with a reasonable degree of participation of stakeholders. Transparency International Bangladesh (TIB) has been participating in the process by reviewing the successive drafts so far made publicly available. TIB deeply appreciates that some of its recommendations on earlier versions were positively considered. In continuation of the process, TIB submits the following reviews and recommendations on the latest draft of DPA 2023. For convenience, references have been made to the extent to which this latest version represents consideration of TIB’s earlier reviews and recommendations.

II. Review of the latest draft DPA 2023 and Recommendations

SL	Topics, sections, sub-sections	Issues in the previous DPA draft & TIB’s previous observations/ recommendations	Acceptance Status	Recommendations and Logic behind
1.	Title	In the previous submission, we recommended that the ‘Data Protection Act 2023’ be renamed the ‘Personal Data Protection Act 2023’.	Not taken into consideration	The latest version of the DPA lacks a comprehensive definition of ‘personal data’ in section 2(p), and the term ‘personal data’ is sparingly used in the bill. This context

		Data protection laws aim to ensure the fair, transparent, and secure processing of individuals' personal data. They establish processing principles, mandate informed consent, and confer rights to access, rectify, and erase data. Organisations handling personal data must implement security measures to prevent unauthorised access or breaches. The primary focus of the DPA is on personal data, and expanding its scope beyond this realm would counter its purpose. Consequently, our previous research recommended renaming the proposed DPA as the 'Personal Data Protection Act, 2023' rather than the 'Data Protection Act, 2023'. We also suggested that using the title 'Data Protection Act' could be possible if the law expressly specifies its application to personal data within this Act.		suggests that the draft DPA is geared towards safeguarding 'data' in a broader sense rather than specifically focusing on the protection of 'personal data' of individuals. Therefore, we further emphasise that the draft DPA should be renamed the 'Personal Data Protection Act, 2023' instead of the 'Data Protection Act, 2023'.
2.	Preambular paragraph	The previous DPA draft lacked clarity in its wording, making it difficult to discern its focus and objectives. While data protection bills commonly refer to human and fundamental rights as outlined in the relevant Constitution and international human rights instruments, the draft DPA did not refer to the Constitution of Bangladesh or any international human rights instruments. Accordingly, in our previous submission, we recommended incorporating such provisions in the draft DPA that explicitly articulate its commitment to safeguarding and promoting human rights as enshrined in the national Constitution and international human rights instruments.	Partially accepted	Our recommendations are partially accepted by adding the following statement: 'as data use is crucial to join worldwide free trade following internationally accepted data protection rules'. However, the preambular paragraph of the proposed 'Data Protection Act, 2023' may be worded as follows – *Having regard to the right to privacy as enshrined in Article 12 of the Universal Declaration of Human Rights (UDHR), 1948, Article 17 of the International Covenant on Civil and Political Rights (ICCPR), 1966 and Article 43 of the Constitution of the People's Republic of Bangladesh-* *Whereas it is expedient to make provisions for the protection of privacy and personal data*

				required to lead a quality life in this data-driven world, and whereas it is essential to create a unique digital culture promoting a free and fair digital economy, ensuring the controls of the individuals over their personal data, fostering businesses, competition and innovation through digital governance, and inclusion of all affairs correlated or incidental thereto, it is hereby enacted as follows:
3.	Short title and commencement of DPA (section 1)	The DPA shall come into effect from the day as indicated by the government in the official gazette.	New inclusion	International best practices suggest that at least a 2-year grace period shall be given for individuals and organisations to prepare for the new law. Hence, we recommend allowing at least 2 years grace period for individuals and organisations to prepare for the new DPA.
4.	Definition of sensitive personal data by rule (section 2(t)(iv))	Declaring sensitive data by rule is problematic. Along with health data, genetic data, biometric data, and criminal conviction data, the government can declare any data as sensitive. The following data can be considered sensitive data per international best practices. a) racial or ethnic origin. b) political beliefs. c) religious or philosophical beliefs. d) trade union membership. e) genetic or biometric data. f) physical or mental health. g) sex life or sexual orientation.	New inclusion	Sensitive data cannot be made by rule as that could be deemed as the exercise of the excessive use of executive powers and against the prevailing norms. Hence, we recommend repealing this provision.

5.	Anonymised and pseudonymised data (sections 2(a), 4(2))	The previous draft treated anonymised and pseudonymised data in the same manner, which is undesirable as they are distinct concepts. Section 2(a) of the draft DPA treats anonymised and pseudonymised data on an equal footing. For instance, section 4(2) states that the DPA shall not apply to anonymised and pseudonymised data. However, international best practices differentiate between these two forms of data. Pseudonymised data refers to personal data processed in a way that replaces identifying information with a pseudonym or code. It can still be linked to an identified or identifiable natural person with additional separately held information. Therefore, pseudonymised data generally falls within the scope of data protection laws, requiring compliance from organisations that collect, process, or store it. In contrast, anonymised data is no longer considered personal data and falls outside the scope of data protection laws. In our previous submission, we recommended amending the draft DPA to distinguish between anonymised and pseudonymised data, aligning it with international best practices.	Partially accepted	As per section 2(a), both anonymised and pseudonymised data are identical, although they are not. However, the last paragraph of section 2(b) ensures that the DPA shall not apply to pseudonymised data. The DPA should clarify that anonymised and pseudonymised data are different.
6.	Definition of the data subject, section 2(d)	In the previous draft, the definition of ‘data subject’ in section 2(d) was notably brief and unconventional, simply stating ‘persons relating to data.’ In our previous submission, we recommended amending this definition to include additional elements such as ‘identified or identifiable natural person,’ among others.	Not taken into consideration	Our recommendation to amend the definition of 'data subject' in the previous draft DPA to include elements such as 'identified or identifiable natural person' is grounded in several logical arguments. Firstly, the inclusion of 'identified or identifiable natural person' aligns with established international

				data protection standards, providing a more comprehensive and precise definition that conforms to best practices. Secondly, specifying that personal data pertains to an 'identified or identifiable natural person’ ensures that the definition is in line with the core principle of data protection, which revolves around safeguarding the privacy and rights of individuals. Thirdly, the proposed definition adds clarity and legal robustness to the DPA, reducing the potential for misinterpretation and facilitating its effective implementation. We recommend adopting the following definition for ‘data subject’: ‘*Data subject’ means an identified or identifiable natural person whose personal data is used or processed, as understood under this data protection law, by the data controller or data processor*.
7.	Definition of ‘person’ in section 2(p) and application of law in section 4(1)(a)	In the previous submission, we shared that the definition of ‘person’ in section 2(r) and the application of the law in section 4(1)(a) might lead to the implications that the data protection law applies to both natural and legal persons. It is important to note that data protection laws primarily apply to the protection of the personal data of natural persons, not organisations. However, the previous DPA’s scope extended its application to data concerning both natural and legal persons, encompassing various entities such as individuals,	Not taken into consideration	Our recommendation to replace the term ‘person’ with ‘natural person’ in sections 2(r), 4(1)(a), and other relevant sections throughout the draft DPA is guided by several logical considerations. Firstly, it ensures alignment with the core principle of data protection, which primarily concerns the safeguarding of the personal data of natural individuals, not organisations or legal entities. Secondly, specifying ‘natural

		legal entities, organisations, businesses, companies, associations, corporations, cooperative societies, institutions, and statutory bodies. In our previous submission, we proposed to replace the term ‘person’ with ‘natural person’ in section 2(r), 4(1)(a) and other places throughout the draft DPA.		person’ clarifies the scope of the DPA, preventing any misinterpretation that it applies to both natural and legal entities, which can lead to unintended consequences and legal complexities. Thirdly, this modification brings the DPA in line with international data protection standards, enhancing its consistency and compliance with established norms.
8.	Structuring the ‘Definition Clause’ and definition of personal data	In the initial draft of the Data Protection Act (DPA), there were issues related to the arrangement of terms within the 'Definition Clause.' In the earlier version of the draft DPA, the term 'financial data' was defined ahead of 'data,' and notably, 'personal data' remained undefined throughout the document. This sequencing discrepancy deviated from the logical order of definitions, as 'data' logically should precede the definition of 'financial data.' We recommended a reordering of the DPA to ensure ‘data’ comes before the definition of ‘financial data’. Moreover, we proposed the consistent replacement of the term ‘data’ with ‘personal data’ throughout the bill, together with the inclusion of the subsequent definition of ‘personal data’ for clarity and coherence. “Personal Data’ means any information relating to an identified or identifiable natural person and it may include the following: Name, email address, phone number, home address, date of birth, credit card numbers, the photograph of a person, any identification card number (e.g., NID card number), cookie ID, an online identifier, e.g., internet protocol (IP) address, location data (for example, the location data from a mobile phone or other	Partially accepted	The definition of personal data should be specifically included. We specifically recommend the following be included in the definition section: “Personal Data’ means any information relating to an identified or identifiable natural person, and it may include Name, email address, phone number, home address, date of birth, credit card numbers, the photograph of a person, any identification card number (e.g., NID card number), cookie ID, an online identifier, e.g., internet protocol (IP) address, location data (for example, the location data from a mobile phone or other device data, the advertising identifier of one’s phone or device and social media profile IDs/links, and any physical, physiological, genetic, health data and medical records, mental and physical predicament/disability-related data, economic, religious, cultural, ethnic or social identity, political opinion, trade union memberships data, biometric data, spouse and

		device data, the advertising identifier of one’s phone or device and social media profile IDs/links, and any physical, physiological, genetic, health data and medical records, mental and physical predicament/disability-related data, economic, religious, cultural, ethnic or social identity, political opinion, trade union memberships data, biometric data, spouse and children name, educational and employment data and history including job and other titles. However, ‘personal data’ does not cover the following: • Information about a deceased person; • Properly anonymised data, and • Information about public authorities and companies.		children name, educational and employment data and history including job and other titles. The recommendation to reorder the definitions in the DPA, placing ‘data’ before other kinds of data, e.g., ‘financial data’, is based on the logical progression of definitions. In any legal document, the sequencing of terms should follow a logical order. This reordering ensures clarity and consistency in the understanding of definitions within the DPA. Furthermore, the proposal to consistently replace the term ‘data’ with ‘personal data’ throughout the bill, along with the inclusion of a comprehensive definition of 'personal data,' serves several logical purposes. Hence, we recommend reordering the definition clause and inserting ‘data’ to personal data all through the DPA.
9.	Definition of ‘profiling’ in section 2(j)	In the previous draft, the definition of ‘profiling’ lacked consistency with international best practices and required additional relevant text. The definition that was incorporated in the previous version looked like the following, which still exists in the latest draft: “Profiling” means any act of collecting user information or data about a person where the description of necessary information or data of such person is inserted.” However, this definition does not align with established international best practices. As the incomplete definition of	Not taken into consideration	Our recommendation to revise the definition of ‘profiling’ in the draft DPA is based on the need for alignment with international best practices and the need for a comprehensive and precise understanding of the term. The previous definition of ‘profiling’ in the draft DPA lacked clarity and consistency with established international data protection norms. It did not provide a detailed and comprehensive explanation of what profiling

		'profiling' still existed in the latest draft, we recommend incorporating the following definition in line with best practices: ' *Profiling' means the automated processing of personal data of a natural person to analyse, evaluate, or predict his/ her personal characteristics with regard to performance at work, behaviour, reliability, location, economic condition, health condition, personal interests, preferences, movements, etc.*		entails, which could lead to misinterpretation and ambiguity. The proposed definition aligns with international best practices by providing a clear and detailed explanation of profiling. It specifies that profiling involves the automated processing of personal data to analyse, evaluate, or predict various personal characteristics and aspects, such as performance at work, behaviour, location, economic condition, health condition, personal interests, preferences, and movements. This detailed definition ensures that the DPA is in line with established norms, provides clarity to practitioners, and offers a robust framework for addressing issues related to profiling.
10	Definition of 'agency', section 35	Based on the definition of 'agency' in section 35, the previous draft failed to establish an independent data protection authority in Bangladesh. In the previous draft, section 2(f) defined the term 'agency' as the 'Data Protection Agency' (renamed as Data Protection Board) established under section 35 of the draft DPA. However, section 36 allowed the government to appoint the 'Data Protection Agency,' which possessed investigative, corrective, and advisory capabilities but lacked complete independence in its operations. Independence is crucial based on global best practices. In our previous submission, we emphasised that the effectiveness of a data protection framework relies	Not taken into consideration	Due to paramount importance, we suggest that there should be a clear statement in the DPA regarding the independence of the data protection board.

		significantly on the autonomy of the data protection authority. Given the government's role as a significant user and processor of personal data, the presence of government influence or control could lead to conflicts of interest. To ensure autonomy, the ‘Data Protection Agency’ should possess investigative, corrective, and advisory powers while operating independently from government influence or control. Additionally, the Act should mandate the Data Protection Agency to offer expert guidance on data breaches, and data protection matters to all personal data users and processors, including the government.		
11	Data protection principles, section 5	Data protection law is generally principle-bound legislation and hugely based on the key data protection principles set by the OECD Privacy Guidelines, 1980 and followed by major data protection regulations of the world, but in the draft DPA, they are not appropriately articulated. The precise titles of the previous draft of the DPA were as follows: *(a) consent and accountability, (b) fair and reasonable, (c) integrity, (d) retention, (e) access to data and data quality, (f) disclosure, (g) security, (h) risk-based protection and consistent protection, and (j) enforceable standards.* The UN High-Level Committee on Management (HLCM), at its 36th Meeting on 11 October 2018, outlined the following data protection principles, which are followed by all United Nations System Organizations, including UNESCO, in carrying out their mandated activities: 1. Fair and Legitimate Processing 2. Purpose Specification 3. Proportionality and Necessity	Not taken into consideration	The contents and precise titles of the ‘data protection principles’ remain unaltered in the current version of the DPA in comparison to the prior version. Therefore, we suggest that the latest draft of the DPA should include data protection principles aligned with international best practices. Given the GDPR’s status as the leading global standard for data protection regulations, we propose the following GDPR-creep data protection principles for Bangladesh’s latest DPA: **Data Protection Principles:** The controller shall be responsible for the compliance of the following principles, and accordingly, personal data shall be – (a) processed in a lawful, fair and transparent manner only as regards the data subject

		4. Retention 5. Accuracy 6. Confidentiality 7. Security 8. Transparency 9. Transfers (UN Global pulse taken it as Technology Collaborators and Data Transfers) 10. Accountability.[1] Whereas the UN Global Pulse Principles on Data Protection and Privacy added, in line with the UN Principles on Personal Data Protection and Privacy, adopted by the HLCM in 2018 and the UNSDG Guidance Note on Big Data for Achievement of the 2030 Agenda: Data Privacy, Ethics and Protection, three more principles as shared below: 11. No Re-identification 12. Data Sensitivity Risks 13. Harms and Benefits Assessment.[2] In our previous submission, we commented that as per international best practices, including the General Data Protection Regulation (GDPR) 2018, OECD Privacy Guidelines 1980 (revised 2013), Convention 108 1981 and Convention 108+ (adopted in 2018) and APEC Privacy Framework 2015 (originally published in 2005), the precise titles of the key data protection principles may be as follows: (a) Lawfulness, fairness and transparency		(*lawfulness, fairness and transparency principle*); (b) collected for any specific, explicit and legitimate purposes, or processed further for any archive purpose for the public interest grounds, including scientific, historical, or statistical research purposes only, and not proceeded further incompatible with the initial purposes (*purpose limitation principle*); (c) processed adequate, relevant and limited to what is essential for the original purposes (*data minimisation principle*); (d) kept accurate and up-to-date, and every reasonable step shall have to be taken without any delay to erase or rectify any data if it is found that there remains any inaccuracy (*accuracy principle*); (e) stored for a period necessary to the original purposes, and personal data may be kept for a long term in as much as it is processed for any archive purpose for the public interest grounds, covering scientific, historical, or statistical research purposes subject to satisfying appropriate technical and organisational measures essential for the protection of the rights

[1] https://archives.un.org/sites/archives.un.org/files/_un-principles-on-personal-data-protection-privacy-hlcm-2018.pdf; https://www.unesco.org/en/privacy-policy.

[2] https://www.unglobalpulse.org/policy/ungp-principles-on-data-privacy-and-protection/.

		(b) Purpose limitation (c) Data minimisation (d) Accuracy (e) Storage limitation (f) Integrity and confidentiality (security) (g) Accountability.		and freedoms of the data subject (*storage limitation principle*); (f) processed, ensuring appropriate security, technical and organisational measures to save personal data from any unauthorised or unlawful processing, and against any damage, destruction, or accidental loss (*integrity and confidentiality principle*).
12	Data Collection and Processing Section 6 - 10	These sections establish regulations governing data collection and processing, specifically delineating provisions regarding the acquisition of the data subject's consent along with the obligation to furnish the data subject with information pertaining to said data collection and processing. However, subsection 7(6) states that the data fiduciary shall have the authority to process any data pertaining to a data subject, provided that such processing is necessitated by matters pertaining to the public interest and the modalities governing such data processing shall be delineated through subsequently promulgated rules. In Subsection 10(2-d), it is stated that notwithstanding anything contained in Subsection 10(1), data may be gathered from individuals, entities, statutory bodies, or government authorities, contingent upon adherence to established regulations, in cases pertaining to data relevant to the preservation of national security, the prevention of offences, and the identification and subsequent investigation thereof.		We recommend that the provision allowing data fiduciaries to process data for "public interest" and national security purposes be revised to align with international best practices in data protection and privacy. To address the outlined concerns, it is essential to provide clear and specific definitions of what constitutes "public interest" and "national security." This should include strict guidelines and safeguards to prevent misuse and overreach. Additionally, there should be a balance between security interests and privacy rights, ensuring that data collection is proportionate, necessary, and subject to stringent oversight to prevent discrimination and abuse of surveillance powers.

11	Processing of sensitive data, section 11	According to section 11 of the previous DPA draft, sensitive data processing was allowed based on lawful processing grounds, subject to written consent from data subjects and other specified conditions, but without the necessity of adhering to specific data protection principles. Aligning with global best practices, we recommended in our earlier submission that, beyond obtaining the data subject’s written consent, processing sensitive personal data should also be bound by legal obligations to follow principles such as purpose limitation, data minimisation, security, retention, transparency, and accountability.	Not taken into consideration	We suggest making strict rules for handling sensitive personal information because it's more likely to be misused or have privacy problems. These rules should follow global standards for how data is treated, which are important to protect people's rights and privacy. We further recommend that beyond obtaining the data subject’s written consent, processing sensitive personal data should also be bound by legal obligations to follow principles such as purpose limitation, data minimisation, security, retention, transparency, and accountability.
12	Data relating to children, section 12	Distinguishing the age of consent for online services from the age of majority is essential as setting the age of majority at 18 years could hinder online activities, notably impacting online learning, particularly from the context of the COVID-19 pandemic. However, in the previous draft of the DPA, the age for children was fixed at 18 years under section 12(3)(a)). Recent research indicates that EU Member States set the age of majority between 13-16 years for data processing activities. The USA’s Children’s Online Privacy Protection Act of 1998 (COPPA) also stipulates that parental consent is required for processing the personal data of children under 13. Accordingly, we suggested adopting 13-16 years for self-reliant data processing activities.	Not taken into consideration	Against the discussed backdrop, we recommend that the draft DPA should incorporate the age of majority for children’s consent as between 13-16 years, aligning with prevailing international best practices. Encouraging 13-16-year-old children to engage in self-reliant data processing activities offers numerous educational and mental development benefits. Firstly, it cultivates critical thinking and problem-solving skills as they analyse and manipulate data. Secondly, it enhances their digital literacy, a vital competency in today’s technology-driven world. Thirdly, it fosters a sense of autonomy and responsibility as they independently manage data-related tasks. Fourthly, it sparks creativity and innovation as they explore data visualisation and analysis

				methods. Lastly, these activities promote a positive attitude towards learning, as children see tangible results from their efforts, boosting their self-esteem and motivation.
13	Right to correction, section 14	Data controllers' decisions on correcting or refusing to correct misleading personal data of data subjects lacked a specific timeframe in the previous DPA draft, potentially leading to misuse. Therefore, we suggested in our earlier submission that the draft DPA should include clear timeframes for notifying data subjects about correction decisions and refusals.	Not taken into consideration	We recommend the inclusion of clear timeframes for notifying data subjects about correction decisions and refusals in the draft DPA for several important reasons. Firstly, specific timeframes ensure transparency and accountability in the data correction process, preventing indefinite delays that may harm data subjects. Secondly, it sets a standard for data controllers, promoting efficient and responsible data management. Thirdly, prompt notification allows data subjects to take appropriate actions or seek further recourse if their requests are denied, fostering trust in the data handling process. Lastly, it aligns with the principles of fairness and data accuracy, which are fundamental aspects of data protection regulations.
14	Right to data portability, section 16 (2)	The inclusion of the right to data portability provisions in section 16(2) of the previous DPA draft concerning anonymised data was problematic. Data protection laws typically pertain to pseudonymised data rather than anonymised data. Accordingly, we reiterated in our prior submission that the provision applying the right to data portability to anonymised data should be removed from the draft DPA, given that	Not taken into consideration	Our recommendation to remove the provision applying the right to data portability to anonymised data in the draft DPA is grounded in several key logical arguments. Firstly, anonymised data, by definition, cannot be linked back to individuals, making the application of data portability irrelevant in such cases. Secondly, including anonymised data within these provisions could lead to

		anonymised data is generally exempt from the scope of data protection laws. Nonetheless, the provisions remain unchanged in the current draft. Hence, we strongly recommend revising the draft DPA to align with the standard practice of excluding anonymised data from such provisions.		unnecessary complexities and potential misuse, as there is no identifiable data subject to exercise these rights. Thirdly, adhering to the standard practice of excluding anonymised data ensures consistency with established data protection principles, where the focus is primarily on pseudonymised data that still relates to individuals. Therefore, revising the draft DPA to align with this practice promotes clarity, effectiveness, and compliance with data protection laws, ultimately benefiting both data subjects and data controllers.
15	Rights of Foreign Data Subjects, section 17	The absence of comprehensive provisions concerning the rights of foreign data subjects according to section 17 of the previous DPA draft posed an issue. Specifically, section 17 of the draft DPA states that foreign data subjects residing in Bangladesh will have all their data protection rights under this law without providing the necessary details. In light of this, we reiterated in our previous submission that the draft DPA should clarify whether foreign residents will enjoy rights in the same manner as Bangladeshi citizens. The legislation should also outline any obligatory conditions for foreign nationals to access services under the DPA, along with specific regulations for data collection, retention, transfer, and processing principles applicable to refugees hosted in Bangladesh, among other aspects.	Not taken into consideration	Our recommendation for comprehensive provisions concerning the rights of foreign data subjects in the draft DPA is grounded in several logical arguments. Firstly, it addresses a potential ambiguity in Section 17 of the previous DPA draft, ensuring that the rights of foreign data subjects are clearly defined and aligned with international data protection standards. Secondly, specifying whether foreign residents will enjoy rights on par with Bangladeshi citizens promotes fairness and transparency in data protection practices, preventing any disparities or misconceptions. Thirdly, outlining obligatory conditions for foreign nationals to access services under the DPA ensures that data processing activities are carried out in compliance with legal and

				ethical standards. Lastly, the inclusion of specific regulations for data collection, retention, transfer, and processing concerning refugees hosted in Bangladesh reflects a commitment to safeguarding the rights and privacy of vulnerable populations. In summary, these provisions are essential for establishing a robust and equitable data protection framework that respects the rights of all individuals, regardless of their nationality or residency status.
16	Right to erasure of personal data, also known as ‘the right to be forgotten’, section 18(3)(a)	Freedom of expression is generally not considered an exemption within data protection laws, although it was granted in the previous draft of the DPA. The right to data protection is recognised as a fundamental human right across countries and international legal frameworks, safeguarding individuals from the unauthorised collection, processing, and sharing of their personal data. While freedom of expression is also a fundamental right, it can conflict with data protection when involving the collection and processing of personal data without consent. Adhering to international best practices, the protection of privacy and personal data should not be limited by freedom of expression. Even the freedom of expression is granted in the Constitution of Bangladesh, subject to any reasonable restrictions imposed by law (article 39).	Not taken into consideration	The recommendation to revise the draft DPA to remove freedom of expression as an exemption within data protection laws is grounded in succinct logic. While both freedom of expression and data protection are fundamental rights, they usually conflict, particularly in the case of the collection and processing of personal data without consent. This provision is imperative since data protection laws aim to protect individuals from unauthorised data collection, processing, and sharing, ensuring their privacy and security. Even the Constitution of Bangladesh itself grants the freedom of expression subject to reasonable restrictions imposed by law.

17	Excessive Reliance of Rule-Making Powers under sections 5-8, 10, 12-15, 18-20, 22, 24-32, 38-40, 44-50, 55-56, 58-59, and 72.	In the previous version of the DPA, the term ‘rules’ was used 96 times, and ‘by rules’ a total of 63 times throughout various sections, including 5-8, 10, 12-15, 18-20, 22, 24-32, 38-40, 44-50, 55-56, 58-59, and 72. This excessive reliance on rule-making is undesirable, and the power for creating rules should be limited, well-defined, and directed toward specific purposes. Concerns exist about the potential misuse of rule-making power, leading to excessive discretion and wide interpretation. Given the absence of obligatory publication requirements for rule-making powers, there exists a potential for executive misuse of this authority. Consequently, in our earlier submission, we suggested that the DPA should only be approved by the parliament after clearly outlining all the sections left at that time for rule-making.	Not taken into consideration	The recommendation to limit and define rule-making powers in the DPA is based on several concise yet compelling reasons. Firstly, the excessive use of the term 'rules' throughout the document raises concerns about the potential for wide interpretation and misuse of rule-making authority, which could result in excessive discretion. Furthermore, without obligatory publication requirements for rule-making, there is a risk of executive misuse of this authority. To address these issues, the recommendation suggests that the DPA should only be approved by parliament after clearly outlining all the sections reserved for rulemaking, ensuring transparency and accountability in the process. In essence, the recommendation seeks to prevent potential misuse of rule-making powers, enhance transparency, and provide clear definitions and purposes for such rules, ultimately promoting good governance within the data protection framework.
18	Accountability and Transparency, Chapter Seven	The earlier version of the draft DPA allocated significant data security responsibilities to data controllers in Chapter Seven. However, it is noteworthy that one size does not fit all due to varying implications depending on socio-economic categories, business sizes, and external factors like COVID-19, climate change, and economic crises.	Not taken into consideration	The recommendation to organise data controller responsibilities into different timeframes is rooted in the recognition that a one-size-fits-all approach may not be suitable given the diverse landscape of data controllers. Socio-economic categories, business sizes, and external factors like COVID-19 and economic crises can

		In light of this, our prior suggestion was to categorise data controller responsibilities based on their capacities and capabilities across various timeframes. For instance, prominent data processors such as those in the telecommunications, banking, insurance, education, and healthcare sectors could align themselves with these obligations during the initial phase, while other relevant entities of varying sizes (medium and small) could adopt them in subsequent stages after engaging in consultations with pertinent stakeholders.		significantly impact their capabilities and readiness for compliance. By implementing phased responsibilities, major data processors can lead the way during the initial phase, ensuring efficient compliance. Subsequent stages would then accommodate other institutions, especially medium and small-sized ones, allowing them to adapt gradually and consult relevant stakeholders. This approach acknowledges the unique challenges faced by different data controllers and aims to provide a flexible framework that promotes effective data security measures while considering the broader socio-economic context and external factors that may affect compliance readiness.
19	Accountability, section 21	The accountability provisions in section 21 could be substituted with the accountability principle outlined in section 5(a), following best practices for clarity. The incorporation of accountability provisions in section 21 duplicates the accountability principle already stated in section 5(a). Therefore, in our previous submission, we advised removing the provisions of section 21 as they are redundant and unnecessary but were not considered.	Not taken into consideration	The recommendation to eliminate the provisions in section 21 is based on the principle of avoiding redundancy and ensuring clarity within the data protection framework. Section 5(a) already outlines the accountability principle, and duplicating similar provisions in section 21 adds unnecessary complexity to the law. By removing the redundant provisions, the draft DPA can maintain clarity and coherence, aligning with best practices in legal drafting. This streamlining not only simplifies the legislation but also ensures that the

				accountability principle is consistently applied throughout the document, reducing the risk of misinterpretation and promoting effective compliance.
20	Transparency, section 22	The transparency provisions in section 22 of the previous draft of the DPA appear overly ambitious in the context of Bangladesh. The requirements of data categorisation, processing purposes, risk-prone data identification, data subject rights, complaints to the Data Protection Agency's Director General, data portability, and data subject notification may pose challenges for startups and small businesses. These provisions are challenging, as they impose complex formalities for data controllers to ensure transparency. For transparency, countries with long-standing data protection laws have focused on simple procedures to ensure compliance rather than incorporating rigid bureaucratic processes. Hence, our prior recommendation was to simplify the procedure, initially applying it only to large-scale data processing companies and extending it later to medium and small-sized ones after consulting relevant stakeholders.	Not taken into consideration	The recommendation to simplify the transparency provisions in section 22 is grounded in the practicality and adaptability needed for the context of Bangladesh, particularly for startups and small businesses. The overly ambitious requirements can impose significant challenges for these entities, potentially hindering their ability to comply with complex formalities. By initially enforcing these rules for large-scale data processors and gradually extending them to medium and small-sized entities after stakeholder consultation, a balanced approach can be achieved. This phased implementation allows for the adaptation of businesses to evolving data protection standards while promoting transparency without overwhelming smaller players. It aligns with international best practices that prioritise simplicity and practicality in data protection regulations, especially in regions where the ecosystem may be less mature.
21	Security standards for data protection,	In the previous draft of the DPA, the determination of minimum data security standards was left to rules as outlined in section 24(1), which could pose issues.	Not taken into consideration	Our recommendation to specify minimum data security standards within the legislation, rather than leaving them to be determined by the rule, is rooted in the need for clarity and legal robustness. These standards,

	section 24(1)	We recommended in our prior submission that these standards, covering aspects like encryption, secure networks, restricted data transfers, controlled employee access, authentication, risk management, physical security, vulnerability control, and training, should be specified in the law.		encompassing various critical aspects of data security, including encryption, network security, access control, and more, are fundamental in safeguarding personal data. By explicitly defining these standards in the law, it provides a clear and enforceable framework for data controllers to follow. It eliminates ambiguity and ensures that all relevant parties are aware of their obligations, enhancing compliance and ultimately strengthening data protection practices. Additionally, it aligns with international best practices that emphasise the importance of setting clear and comprehensive data security standards within data protection laws.
22	Redundancy of provisions, sections 25 & 26	The provisions outlined in sections 25 and 26 of the prior DPA draft were redundant as they pertained to the purpose limitation and accuracy principles, as laid down in section 5. In our previous submission, we opined that these redundant provisions could be eliminated, considering that these two principles are adequately articulated in section 5 under the category of ‘Data Protection Principles’.	Not taken into consideration	Our recommendation to eliminate the provisions in sections 25 and 26, which relate to the purpose limitation and accuracy principles, is based on the principles of clarity, conciseness, and elimination of redundancy within the law. These principles are already comprehensively addressed in section 5 under the category of 'Data Protection Principles.' Therefore, replicating them in sections 25 and 26 creates unnecessary redundancy and the potential for confusion. By removing these duplicate provisions, the law becomes more concise and easier to interpret, ensuring that the essential data protection principles are clearly outlined

				in a single section, thus enhancing the overall clarity and effectiveness of the legislation.
23	Preservation of records by the data controller, section 27	The rules for keeping records safe by the data controller, as outlined in section 27 of the earlier draft DPA, are commendable. However, in the previous submission, we observed that the above rules might seem burdensome for small businesses falling under the DPA. We also argued that the data controller would likely shift the financial burdens of maintaining data to individuals and accordingly suggested avoiding such rules by offering targeted incentives, such as subsidies, contingent on the size of the data controllers. However, there are no reflections on our suggestions in the latest draft of the DPA.	Not taken into consideration	Considering the probable concerns, the latest DPA draft should include provisions easing the burden on small businesses due to record-keeping rules in section 27. Additionally, the DPA should incorporate clauses that discourage data controllers from transferring financial obligations to individuals and introduce incentives like subsidies proportionate to the size of data controllers to ensure responsible data management practices.
24	Data breach notification, section 28	The earlier draft did not specify a timeframe for notifying data subjects and the regulatory body about data breaches. The previous draft of the DPA required the data controller to immediately notify the Director-General of the 'Data Protection Agency' about the data breach incidents. However, the term 'immediately' lacked clarity. Following international best practices, we suggested that the data controller inform the regulatory authority about data breaches without undue delay, preferably within 72 hours. We also proposed that if a data breach posed significant risks to data subjects' rights and freedoms, the controller should promptly inform affected individuals. The timeframe for such notifications could be even longer but must be clearly defined.	Partially accepted	It is admirable that the newest DPA draft now states that data controllers must notify the regulatory authority (Data Protection Board) within 72 hours. However, the latest draft does not take into notice suggestions for cases of high risks to data subjects' rights and freedoms. In such instances, the data controller should promptly inform affected data subjects about the breach without undue delay. The timeframe for this notification could be extended but should be clearly specified. We recommend specifying clear timeframes for data breach notifications to ensure transparency, accountability, and timely response to such incidents. This aligns with international best practices and helps protect

				data subjects' rights and freedoms while enabling a swift and efficient regulatory response.
25	Data audit, section 29	The earlier DPA draft postulated that the data controller, being authorised by the Director-General of the ‘Data Protection Agency’, might appoint an auditor with expertise in ICT, computer systems, data, data protection, and data privacy to conduct inspections on data processing activities. We proposed that along with the discussed expertise, a data auditor should have familiarity with data protection laws and regulations. We think that a data protection auditor should have a solid understanding of contemporary data protection laws and regulations apart from computational, technical, analytical, and communication skills.	Not taken into consideration	Without changing the term ‘Data Protection Agency’ to ‘Data Protection Board,’ the criteria for auditor qualifications remain unchanged from the previous DPA draft. Hence, we suggest that the upcoming DPA bill should specify that a data protection auditor must possess a comprehensive grasp of current data protection laws and regulations, along with computational, technical, analytical, and communication skills. This addition ensures that auditors not only possess technical and analytical skills but also comprehend the legal framework within which data processing activities operate, thereby enhancing their ability to conduct comprehensive and effective audits in compliance with data protection laws.
26	Data protection officer, section 31	The appointment of a data protection officer for all types of businesses or organisations in Bangladesh, stipulated by section 31 of the previous draft of the DPA, raised concerns. Based on established norms, our earlier submission advocated for the mandatory appointment of a Data Protection Officer (DPO) only in specific circumstances, including (1) the public authorities and bodies, regardless of their size, (2) organisations that engage in large-scale	Not taken into consideration	Our recommendation for the mandatory appointment of a Data Protection Officer (DPO) only in specific circumstances aligns with international best practices and ensures a balanced approach to compliance. Mandating a DPO for organisations that engage in large-scale data processing or systematic monitoring of individuals on a large scale is

		processing of personal data, and (3) institutions that deal with systematic monitoring of individuals on a large scale. We also expressed that organisations not falling within these categories could voluntarily, rather than mandatorily, appoint a DPO to ensure adherence to data protection laws and regulations. We further recommended that there should be clear indications of what the DPO should perform for data protection issues. Accordingly, we shared the following activities that a DPO usually performs- (i) Advising and assisting the controllers and all their staff regarding data protection and informing them about their obligations under data protection law; (ii) Monitoring compliance issues under data protection laws; (iii) Giving directions concerning data protection impact assessment and monitoring its performance; (iv) Act as a contact point between controllers and the relevant supervisory authority or independent data protection authority (DPA); (v) Raising awareness, conducting training, and answering queries or complaints on data protection issues and (vi) Keeping records regarding data protection issues.		pragmatic, as these are the scenarios where the risk to individuals' data privacy is highest. Additionally, providing clear indications of the DPO's responsibilities ensures that organisations understand their obligations and helps maintain consistency in DPO roles across different entities, fostering better compliance with data protection laws and regulations.

27	Data protection by design, section 32	The development of data protection strategies is a multifaceted and dynamic undertaking that requires continuous assessment and improvement of the responsibilities and duties of the data controller. Although section 32 of the draft DPA encompasses a range of controller obligations such as technical measures, adhering to rule-based standards in technology-driven data processing, ensuring data erasure to protect the privacy and personal data of subjects, and lawful data processing, there are further responsibilities suggested in our previous submission. These additional controller duties include: 1. Maintaining records of data processing activities; 2. Ensuring integrity and security of data; 3. Restricting unnecessary access to data; 4. Ensuring appropriate organisational measures along with technical measures; 5. Providing information to data subjects about the data breach notification, associated risk factors, protection mechanisms, and cross-border data transfer; 6. Conducting privacy impact assessment to learn about the need and proportionality of data processing 7. Keeping all records up-to-date, and In our prior recommendation, we stressed the importance of diligently implementing data protection by design and	Not taken into consideration	Our recommendation to expand the framework of data controller responsibilities in the DPA is rooted in the evolving and complex nature of data protection. As technology and data processing methods continue to advance, it is crucial to ensure that data controllers have a comprehensive set of responsibilities to adapt to these changes. These provisions include maintaining detailed records, ensuring data security, limiting access, informing data subjects about data breaches and transfers, conducting privacy impact assessments, and keeping records up-to-date. Implementing data protection by design and default throughout the entire project lifecycle is essential for proactive compliance and data privacy. By including these additional responsibilities in the DPA, we aim to provide a robust framework that helps organisations stay compliant with evolving data protection standards and safeguards the privacy and rights of data subjects.

		default, starting from project design through completion, including all systems and services involving personal data processing.		
28	Exemption, Section 33	The draft Data Protection Act includes exemptions for government agencies from complying with data processing provisions outlined in the data protection law when engaged in activities related to crime prevention, identification, the investigation leading to the apprehension of criminals, filing criminal cases, or the collection and assessment of taxes and duties etc.		We recommend that the draft Data Protection Act align with international best practices by including specific provisions defining the scope of government agency exemptions, establishing robust safeguards to prevent potential misuse of personal data, and requiring transparency, accountability, and adherence to principles like proportionality, data minimisation, and the right to privacy. These provisions should also emphasise the need for procedural safeguards such as judicial oversight and data protection impact assessments to ensure that government data processing activities respect individuals' privacy rights and maintain necessary checks and balances, all while fulfilling legitimate government purposes such as crime prevention and tax collection.
31.	Power to make further exemptions , section 34	Section 34 in the prior DPA draft granted unrestrained exemptions to government agencies regarding data protection, deviating from international standards and potentially enabling misuse. Generally, data protection laws aim to protect individual's rights and freedoms in personal data processing, achieved by governing data collection, use, storage, and disclosure while imposing lawful, impartial, and transparent obligations on data processors.	Not taken into consideration	Our recommendation to revise Section 34 of the DPA draft is based on the need for a balanced approach to data protection, particularly concerning government agencies. Data protection laws are designed to safeguard individuals' rights and freedoms in personal data processing, irrespective of whether the data controller is a government office or a private entity. While limited exemptions for government agencies may be necessary in cases related to national security,

		Government offices are also subject to these laws, obligated to meet the same criteria as private sector entities. In specific cases, government offices may enjoy exemptions in limited scenarios like national security, public order, or citizens’ rights preservation. Accordingly, in the previous proposal, we suggested a precise exemption list in line with international best practices. We also reiterated that even if government institutions got exemptions, they should responsibly handle personal data and ensure any exemptions granted are valid, essential, and do not compromise fundamental rights protection and promotion. We further emphasised the need for independent supervisory authorities to oversee and review exempt entities, ensuring proper and lawful use of exemptions.		public order, or citizens' rights, it's crucial to define these circumstances precisely. Aligning with international best practices ensures that exemptions are not misused and that the fundamental rights of individuals are protected. To maintain the integrity of data protection principles, it's essential to subject exempted entities, including government offices, to oversight by independent supervisory authorities. This oversight helps prevent any potential abuse of exemptions and ensures that data processing remains lawful, impartial, and transparent, in line with global data protection standards.
32.	Establishment of data protection board, office, etc., sections 35 & 36	The earlier draft of the DPA lacked any mention of the independence of the ‘Data Protection Agency’. Section 35 of the previous draft empowered the government to establish a ‘Data Protection Agency’ to fulfil the objectives of the DPA. Section 36 authorised the government to appoint and determine terms, including those of the Director General (DG) of ‘The Data Protection Agency’ and other directors. However, the absence of reference to the independence of the data protection authority contradicts international best practices essential for safeguarding citizens’ privacy in the digital age. For the independent and conflict-free execution of responsibilities, an autonomous data protection authority must possess sufficient powers, resources, and autonomy. Consequently, in our prior submission, we urged the	Not taken into consideration	Our recommendation to include explicit provisions regarding the independence of the Data Protection Board is grounded in the fundamental principles of data protection and international best practices. To effectively safeguard citizens' privacy in the digital age, the data protection authority must operate independently and free from conflicts of interest. Operational independence, coupled with clear powers and functions, ensures that the authority can execute its responsibilities without external interference. Staff with relevant expertise and experience are essential

		inclusion of explicit provisions outlining the appointment, tenure, and removal of the data protection authority's head and staff, coupled with a clear delineation of their powers and functions. Furthermore, we emphasised the need for operational independence, staff equipped with relevant professional expertise and experience, and built-in mechanisms of checks and balances to prevent authority abuse.		to make informed decisions and provide guidance on complex data protection matters. Furthermore, mechanisms of checks and balances are necessary to prevent any potential abuse of authority and to maintain transparency and accountability in the data protection process. Overall, these recommendations aim to establish a robust and trustworthy data protection framework that upholds individual rights and privacy.
33.	Powers of Data Protection Agency, sections 38(2)(b)(iv) and 38(2)(a)(v) (Section 40, Latest Draft)	Sections 38(2)(a)(iv) and 38(2)(b)(v) in the earlier DPA draft bestowed extensive powers upon the 'Data Protection Agency' to access data from data controllers or processors and to prohibit data processing by controllers. These provisions posed concerns as conflicted with international best practices and the core objectives of the DPA. The absence of judicial oversight in section 38(2)(a)(iv) regarding data access by the 'Data Protection Agency' could impede the rights of data controllers, processors, and subjects. Thus, we proposed that government access to data undergo judicial scrutiny, with access requests disclosed (without identifying individuals) in the Authority's monthly transparency report, mandated by law, not regulations. Moreover, the Data Protection Authority's powers to ban data processing activities under section 38(2)(b)(v)) could adversely affect stakeholders without allowing the controller's self-defence. Accordingly, in the previous submission, we strongly recommended the removal of such	Not taken into consideration	Our recommendation to revise sections 40(2)(d) and 40(2)(j) of the latest draft of the DPA to include judicial oversight is grounded in the principles of checks and balances and the protection of individual rights. Data protection laws should strike a balance between enabling authorities to access data when necessary and safeguarding the rights of data controllers, processors, and subjects. Introducing judicial oversight ensures that data access requests are subjected to legal scrutiny, preventing potential abuses of power and protecting individual privacy. It also promotes transparency by mandating the disclosure of access requests in the Authority's monthly transparency report, enhancing accountability. Furthermore, allowing data controllers the opportunity to defend themselves before their data processing activities are banned is

		provisions; however, these recommendations were not heeded.		essential to prevent undue disruptions and to ensure a fair and just process. These recommendations aim to align the DPA with international best practices and uphold the core objectives of data protection.
34.	Functions of data protection office, section 39 (Section 41, Latest Draft)	The provisions regarding the powers of the 'Data Protection Agency' to enhance citizens' quality of life based on government policies and programs, as outlined in section 39(b) of the earlier DPA draft, was inconsistent with standard data protection laws, leading to potential misinterpretation and abuse. Therefore, we recommended the removal of such provisions from the draft DPA bill to prevent such ambiguity and misuse. Furthermore, section 39(i) of the previous draft introduced a data protection registration requirement without specifying the necessary details. While incorporating a registration mandate for specific data controllers, processors, or entities could be appropriate, crucial questions need addressing beforehand: (a) identification of entities subject to registration, (b) specifics of the registration process, (c) mandatory nature of the requirement, and applicable data, (d) potential exemptions, among others. Hence, we advised that before implementing a registration obligation, these questions should be addressed within the draft DPA to ensure a clear, comprehensive, and effective registration framework aligned with its purpose of enhancing data protection for citizens.	Not taken into consideration	Our recommendation to remove the provisions granting the 'Data Protection Agency' powers to enhance citizens' quality of life through government policies, as stated in section 39(b) of the earlier draft, is based on the need for clarity and consistency within data protection laws. Data protection laws should primarily focus on safeguarding individuals' personal data and privacy rights, and introducing provisions related to government policies and programs could lead to ambiguity and potential misuse. Regarding section 39(i) and the data protection registration requirement, it is crucial to establish a clear and well-defined framework for registration to ensure compliance and effectiveness. This framework should address critical aspects such as who is subject to registration, the registration process, the mandatory nature of the requirement, the types of data covered, and any potential exemptions. Addressing these questions within the draft DPA ensures that the registration requirement serves its intended purpose of enhancing data protection for citizens while aligning with international

				best practices and established data protection principles.
35.	Standard Operating Procedures (SOPs), or Code of Conduct, section 40 (Section 42, Latest Draft)	Section 40 of the prior draft of the DPA authorised the DG of the ‘Data Protection Agency’ to develop standard operating procedures (SOPs) or a code of conduct. Nevertheless, this responsibility falls under the purview of controllers, processors, or data protection officers for specific organisations or groups of organisations rather than the DG of the ‘Data Protection Agency’. The previous draft of the DPA treats these codes of practice as regulations, implying that they hold the weight of the law, with non-compliance equated to legal non-compliance. This perspective on codes of practice as ‘law’ misconstrues the data protection framework and raises doubts about the DG’s technical expertise to issue such codes. To ensure effective compliance with data protection regulations by businesses, regulatory bodies should encourage relevant stakeholders, including controllers, processors, and data protection officers of specific organisations or groups, to craft customised codes of conduct aligned with their respective processing sectors and the requirements of different enterprise sizes. Best practices recommend that these stakeholders, such as businesses, controllers, or processors, draft the code of conduct and submit it to the supervisory authority for approval. Once approved, businesses must adhere to these codes to govern their data processing endeavours.	Not taken into consideration	Our recommendation to revise section 40 of the prior draft of the DPA is based on the principles of effective data protection regulation and governance. Codes of conduct and standard operating procedures (SOPs) should ideally be developed by the relevant stakeholders within specific organisations or groups who have a deep understanding of their data processing activities and sector-specific requirements. Delegating the responsibility of crafting these codes to the DG of the ‘Data Protection Board’ might not align with the practical realities of data processing and could potentially lead to codes that are disconnected from real-world business operations. Encouraging businesses, controllers, processors, and data protection officers to create customised codes of conduct, subject to approval by the supervisory authority, ensures that the codes are tailored to the specific needs and nuances of different organisations and sectors. This approach promotes a more practical and effective implementation of data protection regulations, fostering a culture of compliance within the industry.

		We previously proposed that the section be revised to delegate the adoption of SOPs or codes of conduct in line with DPA provisions to relevant organisations or groups. Regrettably, our recommendation has not been taken into account.		
36.	Data localisation policy – Storage of sensitive data, user-created or generated data and classified data, section 44 (Section 50, Latest Draft)	Section 44 of the previous DPA draft introduced data localisation rules requiring storage of sensitive, user-generated, and classified data to be stored within Bangladesh's geographical boundaries. However, we expressed concerns about the risks and challenges of establishing such infrastructure in Bangladesh. Enforcing strict data localisation might hinder digital business growth, jeopardise privacy, and limit freedom of expression. It could raise costs, limit access to services, hamper innovation, and hinder multinational data management. This approach may conflict with economic development goals and impede local tech companies. We recommended a thorough assessment of economic and environmental impacts, suggesting optional or removal of data localisation provisions in the DPA. However, our recommendations have been partially accepted as storage of sensitive and user-generated data has been repealed from the latest draft of the DPA. Moreover, storing classified data within the geographical boundaries of Bangladesh can also be considered a form of data localisation policy.	Partially accepted	While there may be a valid objective to secure sensitive data that holds the potential to jeopardise national security if exposed, the current provision is drafted in a manner that implies the Government's authority to periodically and arbitrarily designate data as classified, devoid of any specific criteria or limitations. This provision lacks the necessary clarity for individuals and organisations to discern which data the Government might deem classified at present or in the future. Such ambiguity could result in arbitrary decisions that could adversely affect the activities of civil society organisations and independent journalists who may transmit data to international partners, news outlets, or donors or who may store their data in foreign-based data centres, commonly referred to as "the cloud." The imposition of broad data localisation requirements, particularly in environments conducive to censorship and extensive surveillance, raises legitimate concerns regarding potential misuse. Instead, TIB suggests that Section 50 be revised to reference existing legislation or policy that precisely defines the circumstances under which the Government

				classifies information as "classified." In cases where no such legislation or policy currently exists, the new draft should establish clear parameters for authorities to determine when public information may be categorised as classified. This approach would enhance transparency and provide a more defined framework for the classification of data.
37.	Provisions relating to the transfer of data, section 45	In the previous draft of the DPA, section 45(1) allowed the transfer of personal data outside Bangladesh for purposes like inter-state trade, international relations, or government determinations subject to the data protection principles, as outlined in section 5 of the DPA. Additionally, the transfer of sensitive, user-generated, or any other data outside Bangladesh was subject to data subject consent and compliance with the prescribed procedure outlined in the rules (section (3)(b)). Furthermore, section 45(2) of the draft DPA stated that entities such as Bangladesh Bank, BTRC, and NBR would follow their established procedures for cross-border data transfer, which could potentially complicate matters. However, conditional approval for cross-border data transfer might impede the intended goals of the DPA. The procedural limitations set by the rules could pose significant challenges to such transfers, considering potential delays and complexities in the rule-making process, thereby hindering the core purpose of the Act. To enhance the effectiveness of the draft DPA, we recommended in our earlier submission that both section	Accepted	In our previous submission, we precisely recommended repealing sections 45(2) and 45(3), which incorporated the provisions about the transfer of sensitive, user-generated, or any other data outside Bangladesh subject to data subject consent, and Bangladesh Bank, BTRC, and NBR’s data transfer as per their procedures. It is commendable that our recommendation in this regard has been accepted. We hope this approach will facilitate cross-border data transfer in Bangladesh.

		44 and sections 45(2) and 45(3) should be completely omitted.		
38.	Data protection register, sections 46, 47 & 48 (Sections 52, 53 & 54, Latest Draft)	The data protection registration requirements outlined in sections 46, 47, and 48 of the prior draft of the DPA could potentially present a range of challenges for the ‘Data Protection Agency’, encompassing administrative burdens, complexities, data security risks, potential relaxation of data controller liability, inconsistency in requirements, and limited advantages. Paying heed to stringent internal accountability measures, the General Data Protection Regulation (GDPR) and several recent global data protection regulations do not incorporate such registration prerequisites. Considering the associated compliance costs, administrative burdens, complexities, data security apprehensions, inconsistent requirements, limited benefits, and potential lack of technical proficiency, our earlier recommendation urged the removal of the data protection registration mandates from the draft DPA.	Not taken into consideration	Our recommendation to remove the data protection registration requirements in sections 46, 47, and 48 of the DPA draft was based on several key logical considerations. Firstly, such registration prerequisites could impose administrative burdens and complexities on both data controllers and the Data Protection Agency. Secondly, these requirements might raise data security risks by necessitating the submission of potentially sensitive information to regulatory authorities, potentially increasing the risk of data breaches or unauthorised access. Thirdly, global data protection regulations like the GDPR do not typically include such registration mandates and imposing them could result in inconsistency with international standards.
39.	Inquiry and remedy of the complaints, section 50 (Section 55-59,	Section 50(1) of the prior draft of the DPA mandated the Director General to investigate and address complaints from section 49, following prescribed guidelines. Alternatively, an appointed subordinate may conduct the inquiry. However, concerns arise regarding legal actions without granting the accused controller a right to self-defence, which contradicts the principles of natural justice, such as *“audi alteram partem”* – nobody should be condemned without being heard.	Not taken into consideration	Our recommendation to include the right to self-defence for controllers facing legal actions from data breach complaints is grounded in principles of fairness and justice. It aligns with the age-long fundamental principle of natural justice, e.g., *“audi alteram partem”,* which ensures that nobody should be condemned unheard.

	Latest Draft)	In our previous submission, we emphasised that it would be neither just nor lawful for a data protection authority to initiate legal actions against a controller without allowing them to defend themselves. Therefore, we recommended the inclusion of the right to self-defence for controllers facing legal actions stemming from data breach complaints. However, our suggestions did not receive due attention.		This inclusion not only upholds the principles of natural justice but also ensures that the data protection authority operates in a just and lawful manner, fostering transparency and due process in legal proceedings related to data breaches.
40.	Imposition of punishments by rule, section 55 (Section 60, Latest Draft)	In the prior draft, section 55 granted the government the authority to establish penalties through rules for various unspecified activities, potentially leading to arbitrary misuse of power. This provision could result in arbitrary, biased, and unfair punishment, which is counterproductive and possibly detrimental. Moreover, that approach disregarded the principles of fairness and due process integral to the legal system, potentially undermining the effectiveness of the penalties. Therefore, in our earlier submission, we advised either removing or revising section 55 to include transparent and fair procedures, preventing unwarranted penalties without clear justification, and ensuring the legitimacy of penalties based on specific and well-defined reasons.	Not taken into consideration	Our recommendation is to revisit and amend section 60, which is rooted in the principles of fairness, due process, and the prevention of arbitrary misuse of power. We sought to ensure that the enforcement of penalties within the data protection framework would adhere to fundamental legal principles, preventing unfair and biased punishments while upholding the integrity and effectiveness of the penalties. This approach aimed to maintain a balanced and just system of penalties in line with the principles of fairness and due process essential to the rule of law. Punishments of any kind should be imposed by laws only made by the parliament, not by executive orders.
41.	Compensation for failure to comply with this	Section 56 of the prior draft granted the data protection agency or any authority designated by rules the ability to receive compensation for data breaches. While allowing the data protection agency to receive compensation is reasonable, extending this provision to other entities established by future rules could undermine transparency	Not taken into consideration	Considering the possible threats to transparency and accountability, we suggest reviewing section 61 in the most recent version of the DPA. We further recommend taking proper initiatives to guarantee public confidence and prevent potential misuse of powers as may be exercised by entities

	Act, section 56 (Section 61, Latest Draft)	and accountability, which are pivotal for fostering public trust. This approach may result in unchecked authority, potentially leading to abuses of power, reduced privacy rights, and undermining the rule of law. Hence, we previously advised that section 56 be omitted and urged the inclusion of measures ensuring full transparency and robust oversight for the data protection authority.		designated by rules and restrict compensation provisions to the data protection agency formed under this law, not by any rules, while following rigorous oversight and accountability measures.
43.	Appeal to the government, section 59, application to the government for an appropriate remedy, section 60(3). (Section 64, Latest Draft)	In the earlier version of the DPA, sections 59 and 60(3) suggested the government as the appeal authority, but the reasoning behind this choice was unclear. As per international best practices, the government cannot serve as the appeal authority for DPA-related remedies. Since the government acts as both a data subject and a data controller, it could lead to a conflict of interest if it holds appeal authority. Based on these considerations, we recommended in our previous submission to repeal this provision. We suggested that there should be a judicial entity to perform the remedial under the DPA. Hopefully, the latest draft has accepted our recommendations in this regard.	Accepted but added prolonged timeframe for appeal resolution	The unclear rationale for proposing the government as the appeal authority in sections 59 and 60(3) of the previous DPA version raises concerns, as international best practices advise against the government's involvement due to its dual role as a data subject and controller, potentially leading to conflicts of interest. Thus, we advocated in our previous submission to repeal this provision, proposing instead the involvement of a judicial body to oversee DPA-related remedies. Hopefully, the latest draft reflects these suggestions. However, the latest draft of the DPA allows 90 days for the appellate authority to the appeal resolution, leading to negative consequences. Granting a long time for appeal resolution in the case of a data breach incident could lead to prolonged vulnerability of affected individuals' data, erosion of trust,

				potential legal non-compliance, and increased costs for the organisation. Hence, we suggest reducing the appeal resolution to not more than 30 days. Although the GDPR does not specify an exact timeframe for appeal resolution, it allows a one-month period for answering data-related questions by all authorities.[3] The California Consumer Privacy Act (CCPA) provides a 30-day window for businesses to fix data breach issues;[4] the Personal Information Protection and Electronic Documents Act (PIPEDA) of Canada requires organisations to respond to access to personal information requests within 30 days,[5] and the UK's Data Protection Act 2018 allows 28 days to appeal after the Information Commissioner's Office (ICO) sends the appellant its decision.[6]
44.	Application of the Code of Criminal Procedure, 64	International best practices indicate that data protection laws come under civil jurisdiction, not criminal jurisdiction. Data protection laws primarily aim to ensure fair and lawful processing of personal data with a focus on imposing civil remedies and administrative fines to discourage non-compliance with data protection regulations. Due to the recent emergence of data protection laws, there is a lack of consensus regarding the application of criminal offences to breaches. The enforcement of	Accepted	It is encouraging that our recommendations regarding the non-application of the Code of Criminal Procedure have been considered and incorporated into the latest draft of the DPA while aligning with the principles of civil jurisdiction, civil remedies, and administrative fines for enhanced data protection compliance.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1692852686641.

[4] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[5] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/.

[6] https://www.gov.uk/guidance/information-rights-appeal-against-the-commissioners-decision.

		criminal sanctions is further complicated by the cross-border nature of data and the diversity of legal systems. Furthermore, the complexities of enforcing criminal cases and satisfying the burden of proof can impede the establishment of criminal liability for data breaches. Therefore, our previous recommendation was to remove provisions for criminal sanctions and instead integrate civil remedies and administrative fines to ensure effective compliance with data protection regulations. Thankfully, our suggestions have been taken into account.		
45.	Offences committed by companies, section 65	Section 65 of the earlier draft of the DPA proposed simultaneous liability on various positions like owner, chief executive, director, manager, secretary, partner, officer, staff, or representative, which was deemed unacceptable. The responsibility for a data breach within an organisational framework can vary based on factors like an organisation’s size, structure, and policies. Generally, the ultimate responsibility for a data breach rests with the organisation's leadership—owner, chief executive, director, or manager - rather than subordinate staff. Nonetheless, other staff members, such as officers, partners, secretaries, representatives, and employees, may also assume limited responsibility if they fail to adhere to established security policies, procedures, or other regulations of the DPA. Overall, the primary accountability for data protection lies with the highest authority, not their subordinates. Considering these factors, our previous submission recommended amending the relevant section. Hopefully,	Accepted	Our recommendations have been positively acknowledged in the most recent DPA draft by repealing section 65 and its associated provisions, ensuring a more accurate allocation of responsibility for data breaches within the organisational hierarchy. This amendment acknowledges the primary accountability of the highest authority, aligning with international best practices concerning data protection.

		our suggestions have been taken into account by the deletion of the above section and underlying provisions.		
46	Section 65 (new draft)	The draft Data Protection Act, as outlined in section 65, states that in pursuit of the objectives set forth in this legislation and to safeguard national sovereignty, integrity, national security, and diplomatic relationships with foreign nations, the government may issue instructions to the Data Protection Board as it deems necessary from time to time.		We recommend aligning the draft Data Protection Act with international data protection standards by safeguarding the independence of the Data Protection Board. This can be achieved by introducing clear legal provisions that prevent government interference while also addressing legitimate national security and diplomatic concerns through transparent and accountable mechanisms. Such measures are essential to ensure the effective protection of individual privacy rights and compliance with established global best practices, as seen in the GDPR and guidelines from data protection authorities and organisations.

III. Concluding Remarks (Priorities)

The present version of the draft DPA 2023 is a somewhat improved variant of the earlier one. However, concerns remain over a large number of issues, as detailed above under the column on Recommendations. We call upon the Government to take all these into consideration with a particular emphasis on:

- Our recommendation is to use the term ‘Personal Data Protection Act’ (instead of Data Protection Act, as currently used) as the title of the law so that it is consistent with the core mandate of such a law, which is to protect personal data, not all data. Alternately, it should include a clause/definition to specifically provide that the word data under this law should be understood as personal data only. It may be added that the Data Protection *Act seeks to empower individuals to take control of their personal data and to support organisations with their lawful processing of personal data*.[7] Moreover, a data protection *regulation lays*

[7] https://ico.org.uk/media/2614158/ico-introduction-to-the-data-protection-bill.pdf.

down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[8]

- Definition of personal data should be specifically provided. We specifically recommend the following be included in the definition section: "Personal Data' means any information relating to an identified or identifiable natural person and it may include the following: Name, email address, phone number, home address, date of birth, credit card numbers, the photograph of a person, any identification card number (e.g., NID card number), cookie ID, an online identifier, e.g., internet protocol (IP) address, location data (for example, the location data from a mobile phone or other device data, the advertising identifier of one's phone or device and social media profile IDs/links, and any physical, physiological, genetic, health data and medical records, mental and physical predicament/disability-related data, economic, religious, cultural, ethnic or social identity, political opinion, trade union memberships data, biometric data, spouse and children name, educational and employment data and history including job and other titles. However, 'personal data' does not cover the following: Information about a deceased person, Properly anonymised data, and Information about public authorities and companies.
- Another concern in the draft DPA is the treatment of anonymised and pseudonymised data as equivalent, a stance that has persisted through multiple drafts (sections 2(a) and 4(2)). We strongly recommend distinguishing between these two types of data and amending relevant provisions accordingly. Additionally, the right to data portability for anonymised data should be removed from the draft DPA, as such data typically falls outside the scope of data protection laws (section 16(2)).

- The previous draft of the DPA failed to establish an independent data protection authority in Bangladesh, and this issue persists in the current draft. We stressed the importance of creating an independent data protection authority with investigative, corrective, and advisory powers to ensure autonomy from government influence. However, the draft DPA lacks any reference to the authority's independence (sections 35-36). We recommend that the law should specifically provide that the data protection authority shall be an independent commission outside the influence of the Government.

- To align with international best practices, specific amendments are needed in the draft DPA. These include articulating data protection principles in line with the GDPR (section 5), adjusting the age of data processing consent for minors (section 12(3)(a)), setting a specific timeframe for decisions on correcting or rejecting misleading personal data by the controller (section 14), clarifying the rights of foreign residents (section 17), and ensuring that data protection rights are not constrained by freedom of speech (section 18(3)(a)).

[8] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&qid=1694408530272.

- The current draft of the DPA contains several provisions that could adversely affect the rights of data subjects and, in some cases, the rights of controllers and processors. These issues include granting excessive rule-making powers to the executive (the term ‘rules’ appeared 96 times, and ‘by rules’ appeared 63 times), imposing uniform data security responsibilities on controllers regardless of various factors (Chapter Seven), requiring uniform data record-keeping duties for all controllers (section 27), failing to specify timeframes for data breach responses in case of data breaches that pose high risks to the data subjects (section 28), mandating the recruitment of data protection officers for all businesses (section 31), providing broad exemptions for government agencies’ data access (section 34), allowing extensive data access and prevent processing by the data protection board without judicial oversight (section 40(2)(d) and 40(2)(j), and introducing mandatory data protection registration requirements for businesses without essential details (section 39(i)).

- Finally, to establish an adequate data protection regime in Bangladesh, the latest draft of the DPA requires several amendments, such as transferring the duty of preparing standard operating procedures (SOPs) or a code of conduct from the Data Protection Board to specific organisations or groups (section 42), repealing storage requirements for classified data (section 50), eliminating mandatory data protection registration requirements for all businesses (sections 52-54), granting the right to self-defence for controllers facing legal actions arising from data breach complaints (sections 55-59, repealing government authority to establish unspecified penalties through rules (section 60), removing provisions allowing data protection agencies and designated authorities to receive compensation for data breaches (section 61).