TRANSPARENCY INTERNATIONAL BANGLADESH
Social movement against corruption

Comments and recommendations on Data Protection Act, 2023

(Draft as accessed on 14 March 2023)

Submitted by email on 28 March 2023

SL	Topics, sections, sub-sections	Issues/ Comments/Challenges/ Problems	Analysis/ Recommendations
1.	Title	The title of the bill is 'Data Protection Act, 2023, but it should be 'Personal Data Protection Act, 2023'.	Generally, the data protection Act is designed to protect citizens' right to privacy and personal data; regulate the processing of personal data; give individuals more control over the processing of their personal data, and ensure organisations' accountability toward data processing activities. The scope of DPA is restricted to personal data only. Extending the scope beyond personal data will be counterproductive to the purpose of this law. Hence, we recommend renaming the proposed law to be renamed as the 'Personal Data Protection Act, 2023' rather than the 'Data Protection Act, 2023'. It can be called as Data Protection Act only if it contains a specific elaboration that by Data under this Act implies personal data only.
2.	Preambular paragraph	The focus and aims of the bill are not clear.	It is a widely exercised practice for a data protection bill to refer to human rights and fundamental rights as enshrined in the relevant Constitution and international or regional legal or human rights instruments. However, the draft DPA does not make any direct references to the Constitution of Bangladesh or

			any international human rights instruments. We recommend that the draft DPA should include provisions that clearly outline the intentions to protect and promote human rights as pledged by the Constitution and obligations to relevant international conventions.
3.	Anonymized and pseudonymized data (Section 2(a), 4(2))	Treating anonymised and pseudonymised data in the same sense is not desirable, as they are not the same	Section 2(a) treats anonymised and pseudonymised data in the same sense. For instance, section 4(2) reads that the DPA shall not apply to anonymised and pseudonymised data. International best practices suggest that the data protection law applies to pseudonymised data, not anonymised data. Pseudonymised data is personal data processed to replace identifying information with a pseudonym or code. This means that the data can no longer be directly attributed to an identified or identifiable natural person without additional information held separately. Accordingly, pseudonymised data is generally considered personal data under the data protection laws, and hence, organisations that collect, process, or store pseudonymised data must comply with the data protection law. Contrarily, anonymised data is considered outside the scope of data protection law as it is no longer considered personal data. We recommend that the draft DPA should not treat anonymised and pseudonymised data in the same sense. Any such provision in the enactment shall have to be amended accordingly.
4.	Definition of the data subject, section 2(d)	The definition of 'data subject' is too short and unconventional, and accordingly, it should be enlarged by adding some relevant texts	Section 2(d) defines data subjects as 'persons relating to data', and it is comparatively too short and unconventional. The definition of the data subject should at least add some propositions, e.g., identified or identifiable natural person. We recommend that the definition of the data subject may be as follows: '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.
5.	Definition of 'person' in section 2(r) and application of law in section 4(1)(a)	The definition of 'person' in section 2(r) and the application of law in section 4(1)(a) may give effect to apply this law to data of all natural and legal persons. However, data protection law deals only with the protection of the personal data of a natural person, not an organisation.	By interpreting the provisions of these two sections, it can be seen that the DPA shall apply to data about all natural and legal persons, including any single individual, legal entity, organisation, partnership business, company, association, corporation, cooperative society, institution, and statutory body. Generally, data protection rules apply to data about an identified natural person only, not to data about any legal entity discussed above. We recommend removing the definition of 'person' from section 2(r) and incorporating the term 'natural person' in place of any 'person' in section 4(1)(a) and all other places in the draft DPA.
6.	Definition of financial data (section 2(b)), data (section 2 (c)) and personal data	Before defining 'data', the draft DPA defines 'financial data', and there is no definition of 'personal data' so far in the draft DPA, which is a critically risky weakness of the draft, making it open to wide interpretation and potential abuse.	Before defining 'data', there cannot be any definition of 'financial data'; unfortunately, there is no definition of 'personal data' in the draft DPA. We recommend rearranging the draft DPA. Accordingly, the definition of 'data' should be placed in section 2(b) while placing the definition of 'financial data' into section 2(c) of the bill. **More importantly, the term 'data' should be replaced by 'personal data' everywhere in the bill**. And the definition of personal data may be given as follows: "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.
7.	Definition of 'profiling' in section 2(k)	The definition of 'profiling' is inconsistent with international best practices and should include some relevant texts.	It is praiseworthy to include the definition of 'profiling', which reads as follows: profiling means any act of collecting user information or data about a person where the description of necessary information or data of such a person is inserted. However, this definition is not consistent with international best practices. In line with best practices, the definition of 'profiling' may be as follows: *'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.*
8.	Definition of 'agency', section 2(f)	Definition of 'agency' and the lack of independent data protection authority	Under section 2(f), 'agency' means 'Data Protection Agency', composed under section 35 of the draft DPA. Section 36 empowers the Government to appoint the 'Data Protection Agency'. The Data Protection Agency shall have, among other things, investigative, corrective, and advisory, powers but is not independent in activities. There is no statement that the Data Protection Authority shall work with complete independence, but it is indispensable per international best practices. The success of a data protection regime is critically dependent on the independence of the data protection authority. Since the Government is an important user and processor of personal data, any provision of government influence or control shall be a conflict of interest. Therefore, with investigative, corrective and advisory powers, the 'Data Protection Agency' shall have to be an independent authority outside any

			influence or control of the Government. The Act should also have a provision for the Data Protection Agency to be capable of providing expert advice on data breaches and data protection issues to all users and processors of personal data, including the Government.
9.	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, but in the draft DPA, they are not appropriately articulated	As per international best practices, including GDPR and OECD Privacy Guidelines (revised 2013), Convention 108 and Convention 108+ and GDPR, the key data protection principles may be as follows: (a) Lawfulness, fairness and transparency (b) Purpose limitation (c) Data minimisation (d) Accuracy (e) Storage limitation (f) Integrity and confidentiality (security) (g) Accountability. Even the DPA may also be aligned with the flowing Personal Data Protection and Privacy Principles as adopted by the UN High-Level Committee on Management (HLCM) at its 36th Meeting on 11 October 2018: Fair and Legitimate Processing, Purpose Specification, Proportionality and Necessity, No Re-identification, Retention, Accuracy, Confidentiality, Security, Data Sensitivity, Risks, Harms, and Benefits Assessment, Transparency, Technology Collaborators and Data Transfers, Accountability
10.	Processing of sensitive data, section 11	Under section 11, sensitive data can be processed on lawful bases of processing, provided with the written permission of the data subjects and on the conditions of fulfilment of some other conditions.	On the grounds of lawful bases for processing, sensitive personal data may be processed. However, considering the importance and greater impacts, the condition of a written permission from the data subjects should be imposed for the processing of sensitive personal data under section 11. International best practices also suggest that apart from written consent, the principles of purpose limitation, data minimisation, security, retention, transparency, and accountability will also be imposed by law for the processing of sensitive

			personal data.
11.	Data relating to children, section 12	The age of consent to access online services should be distinguished from the age of the majority	The age of consent to access online services should be distinguished from the age of the majority in other contexts. Nonetheless, in the draft DPA, children's age has been fixed at 18 years (section 12(3)(a)). Recent research shows that the EU Member States fix the age of the majority between 13-16 years in case of data processing activities.[1] The Children's Online Privacy Protection Act of 1998 (COPPA) of the USA also postulates that a guardian's consent is required for processing the personal data of children under 13 To consider 18 years as the age of majority may hinder numerous prospects of online activities. For example, the online learning and education process can significantly affect the postulation of 18 years, while the online learning process has been the only feasible alternative to in-person school attendance during and after the Covid-19 pandemic. We recommend that the draft DPA should postulate that the age of the majority for children's consent should be between 13-16 years, not 18 years, which would be consistent with the prevailing international best practices
12.	Right to correction, section 14	Data controllers' refusal to correct misleading personal data of the data subjects or agreeing to correction of such data should be within a specific deadline but not specified in section 14	There is no fixed timeframe in the draft DPA for both of the stated cases, which can create the scope of abuse. In this regard, we recommend that the draft DPA incorporate a precise timeframe to inform the data subject about the decision to refuse such a correction. Similarly, if the data controller decides to correct the misleading data of the data subject, it must also adhere to a specific timeframe for notifying the data subject about the correction.
13.	Right to data portability, section	The provisions of the right to data portability cannot be exercised against	The provisions of a data protection law do not apply against anonymised data but pseudonymised data. Hence, we recommend that the application of the

[1] Ghent University. (2022). A Children's Rights Perspective on Privacy and Data Protection in the Digital Age. Retrieved from https://www.ugent.be/re/mpor/law-technology/en/research/childrensrights.htm

	16 (2)	anonymised data	provisions of the right to data portability against anonymised data will be removed from the draft DPA as anonymised data generally remains out of the application of data protection law.
14.	Rights of foreign data subjects, section 17	Lack of detailed provisions regarding foreign data subjects' rights	Section 17 of the draft DPA affirms that foreign data subjects residing in Bangladesh will enjoy all their data protection rights under this law. It is recommended that the draft DPA clarify whether foreign residents will enjoy the rights in the same manner as the citizens of Bangladesh. The law should also specify whether there is any binding condition for foreign nationals to receive the services under the DPA, including provisions specific to data collection, retention, transfer, and processing principles for refugees hosted in Bangladesh, etc.
15.	Right to erasure of personal data, also known as 'the right to be forgotten', section 18(3)(a)	Freedom of expression is not generally considered an exemption in a data protection law but do in the draft DPA	The right to data protection is recognised as a fundamental human right in most countries and international legal frameworks that protects individuals from having their personal data collected, processed, and shared without their knowledge and consent. Freedom of expression, however, is also a fundamental right but may conflict with the right to data protection if it involves collecting and processing personal data without consent. International best practices suggest that the freedom of expression cannot curtail the protection of the right to privacy and personal data. Moreover, freedom of expression is not an absolute right even in our Constitution but rather subject to any reasonable restrictions imposed by law under article 39.
16.	Excessive Rule-Making Powers, sections 5-8, 10, 12-15, 18-20, 22, 24-32, 38-40, 44-50, 55-56, 58-59, and 72	The DPA has used the term 'rule' almost 96 times and 'by rule' 63 times throughout the regulation. Among others, sections 5-8, 10, 12-15, 18-20, 22, 24-32, 38-40, 44-50, 55-56, 58-59, and 72 have used the term 'by the rule'. This excessive reliance on the rule-	There is always an apprehension of misuse of the rule-making power, which may lead to excessively discretionary and purposive interpretations leading to abuse. We recommend that the parliament should pass the law only after precisely defining all the mentioned sections currently left for rules-making.

		making power is not desirable. The rulemaking power should be specific, purpose-oriented, and limited.	
17.	Accountability and transparency, Chapter Seven	To ensure data security and protection, the draft DPA imposes numerous responsibilities on the shoulders of the data controller in Chapter Seven. It is praiseworthy, although one size will not fit all due to varying implications depending upon socio-economic categories, business size, and factors external to the control of data controllers as evidenced by the Covid-19 crisis, climate change, and international economic crisis.	Accordingly, the data controller's responsibilities must be structured in a varying timeframe to be consistent with varying capacities. The large-scale data processors, e.g., telecom, bank, insurance, education, and health sectors, may be categorised for compliance in the first phase of a reasonable timeframe, subject to consultation with the relevant stakeholders. In contrast, other relevant institutions (medium and small-sized) may come later phase by phase.
18.	Accountability, section 21	The accountability provisions under section 21 may be replaced by the accountability principle as laid down in section 5(a), and it should be clearly articulated as per best practices.	The inclusion of provisions of accountability in section 21 is a redundancy to the accountability principle as laid down in section 5(a). Accordingly, section 21 may be deleted, considered redundant and unnecessary inclusion.
19.	Transparency, section 22	The provisions of transparency under section 22 are highly ambitious in the context of Bangladesh. The fulfilment of specific formalities, such as filling out a form that requires the categorisation of data, purposes of data processing, identification of risk-prone data, data subjects' rights, complaints to the Director General of the Data Protection	The provisions pertaining to transparency under Section 22 are considerably ambitious, as they mandate data controllers to adhere to highly complicated formalities to ensure transparency. Notably, countries with data protection laws in place for several decades have not imposed such rigid and bureaucratic procedures for data transparency; instead, they have focused on easy procedures but ensure strict compliance. It is recommended to drastically simplify the procedure in consultation with stakeholders before making it applicable only to large-scale data processing companies. The provisions may be extended to medium and small-sized data

		Agency, data portability, and informing data subjects may prove to be onerous tasks for many start-ups or small-sized companies.	processing companies at a later stage.
20.	Security standards for data protection, section 24	The minimum standard data security measures have been left to the Rules, which can be problematic.	We recommend that the minimum standard data security measures be specified in the law, which may include – an encryption system, secure network configuration, restrictions on data transfer, restricted employee access, authentication, and authorisation management, information security risk management, physical security, vulnerability management, and awareness, training, and education.
21.	Redundancy of provisions, sections 25 & 26	The provisions under sections 25 and 26 are redundant for purpose limitation and accuracy principles, respectively.	The provisions under sections 25 and 26 are redundant of purpose limitation and accuracy principles. They may be removed, provided these two principles are appropriately articulated in section 5 under the 'Data Protection Principles' heading.
22.	Preservation of records by the data controller, section 27	The provisions for the preservation of records under section 27 are praiseworthy but may appear as burdensome for many small businesses if they are placed under the purview of DPA	Undoubtedly, the provisions for the preservation of records under section 27 are praiseworthy but may prove to be burdensome for many data controllers. The burden of data preservation costs may be shifted to the shoulders of ordinary individuals, which should be prevented by specific incentives like subsidies depending on the size of the data controllers.
23.	Data breach notification, section 28	No specific timeframe has been prescribed in the draft for data breach notification to the data subjects and the	The data breach notification requirement is one of the most exhaustive provisions, with a specific deadline introduced by recent data protection regulations across the globe.[2]

[2] The EU GDPR, for example, asserts that whenever the controller notices any breach, he will inform the supervisory authority without unnecessary delay but not later than 72 hours (GDPR, article 33(1)). Similarly, the processors would also notify the controller without undue delay after getting information about that breach (GDPR, article

		regulatory body.	Although the draft data protection bill of Bangladesh requires the data controller to inform the Director-General of 'Data Protection Agency' immediately regarding the data breach incident, it contains no clarification regarding the term 'immediately'. Consistent with international best practices, we recommend that the data controller inform the regulatory authority about the data breach without undue delay, but not later than 72 hours. In case of causing a high risk to the rights and freedoms of the data subjects, the controller should inform the affected data subjects about such a data breach without further delay. The deadline maybe even longer, e.g., up to seven days, but it should be specific.
24.	Data audit, section 29	The draft provides that to inspect data, the DG of 'The Data Protection Agency' may constitute a panel with individuals with computational, technical, analytical, and communication knowledge and skills.	Qualifications of a data auditor should include not only computational knowledge and skill, technical expertise, analytical skills, and communication skills but also the knowledge of data protection laws and regulations. We recommend that a data protection auditor should have not only computational, technical, analytical, and communication knowledge and skills but also knowledge of recent data protection laws and regulations.
25.	Data protection officer, section 31	Data protection officer appointments are mandatory for all types of businesses, or organisations are not essential.	The simple reading of the provisions of section 31 of the draft DPA demonstrates that appointing a data protection officer is essential for all types of businesses or organisations in Bangladesh. It is noteworthy that only certain organisations are required to appoint a Data Protection Officer (DPO), such as (1) the public authorities and bodies, regardless of their size, (2) organisations that engage in large-scale processing of personal data, and (3) institutions that deal with systematic monitoring of individuals on a large scale. However, if an organisation does not fall under any of the above categories, it may still appoint a DPO voluntarily, but not

33(2)). If it appears that the data breach incident may cause a high risk to the rights and freedoms of the data subjects, the controller is also obliged to inform the concerned persons without further delay (GDPR, article 34).

Likewise, many US States, such as Alabama, Arizona, Colorado, Iowa, Louisiana, Nebraska, Oregon, South Carolina, South Dakota, Vermont, and Virginia expressed adding the data breach notification principles in their future data protection laws together with some other protections available in the GDPR.[2]

			mandatorily, to ensure compliance with data protection laws and regulations. We recommend that there should have clear statements as to what kind of organisations or businesses is required to appoint the DPO. Moreover, there should also be some clear indications of what the DPO should perform for data protection issues. Generally, the DPO perform the following jobs- (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. (vi) Keeping records regarding data protection issues.
26.	Data protection by design, section 32	The overall design for data protection is incomplete in the draft.	The design for data protection measures is a multifaceted and dynamic process that necessitates an ongoing evaluation and enhancement of the obligations and responsibilities of the data controller. While section 32 of the draft DPA includes various obligations of the controller, including technical measures, maintaining rule-bound standards while using technologies for data processing purposes, deletion of data ensuring the right to privacy and personal data of data subjects, and processing personal data in line with the provisions of law and relevant rules, a controller should accomplish some more tasks as indicated

			below. (i) Maintaining records of data processing activities; (ii) Ensuring integrity and security of data; (iii) Restricting unnecessary access to data; (iv) Ensuring appropriate organisational measures along with technical measures; (v) Providing information to data subjects about the data breach notification, associated risk factors, protection mechanisms, and cross-border data transfer; (vi) Conducting privacy impact assessment to learn about the need and proportionality of data processing (vii) Keeping all records up-to-date, and (viii) Ensuring data protection by design and default strictly from the designing stage to the completion stage of any new project, including all other systems and services that involve the processing of personal data of individuals.
27.	Power to make further exemptions, section 34	The draft provides unfettered exemptions to government agencies with regard to data protection issues, which is against international good practice, and may facilitate abuse.	The primary objective of a data protection law is to safeguard the rights and freedoms of individuals regarding the processing of their personal data. This objective is achieved by regulating the collection, use, storage, and disclosure of personal data and by imposing obligations on those who process such data in a lawful, fair, and transparent manner. The government offices are also subject to data protection laws and must comply with the same obligations and requirements as private sector organisations. In some cases, exemptions may be provided to government offices under specific circumstances, such as for the protection of **national**

			security, **public order**, or the **rights and freedoms of citizens** only. Accordingly, we recommend that a limited and specific exemption list be provided in the Act consistent with the relevant Constitutional provisions and international conventions. In addition, even in cases where government institutions are on the exemption list, they are still under obligation to handle personal data responsibly and to ensure that any exemptions granted are justified and necessary and do not compromise the scope of protection and promotion of fundamental rights of data subjects. Exempted entities should also be subject to oversight and review by independent supervisory authorities to ensure that any exemptions granted are being used appropriately and in accordance with the law.
28.	Establishment of data protection agency, office, etc., sections 35 & 36	No reference is found in the draft DPA regarding the independence of the 'Data Protection Agency'.	Under section 35, the Government can, for fulfilling the purposes of this law, form a 'Data Protection Agency'. Under section 36, the Government will appoint and determine, among other things, the terms and conditions of the DG of 'The Data Protection Agency' and other directors. There is no reference regarding the independence of the Data Protection Authority. In contrast, as per international best practices, ensuring citizens' right to privacy in the digital age is indispensable. To perform its duties independently and effectively free from conflict of interest, an independent data protection authority must have sufficient legal powers, resources, and autonomy to carry out its functions. There should have clear provisions regarding the appointment, tenure, and removal of the head and other staff of the Data Protection Authority, along with a specific delineation of the scope of its powers and functions. Moreover, the Data Protection Agency should have operational independence; it must be equipped with relevant professional expertise and experienced staff and be independent in all its actions with in-built provisions of checks and balances against abuse of authority.

29.	Powers of Data Protection Agency, sections 38(2)(b)(iv) & 38(2)(a)(v)	Unlimited powers have been proposed for the Data Protection Agency to access data under the data controller or processor and powers to ban data processing activities of the controller under sections 38(2)(b)(iv) & 38(2)(a)(v), respectively. This is against international best practices and the core objective of this law, e.g., the protection of the privacy of personal data.	Without getting permission from the competent court, the powers of the Data Protection Agency to access data under the data controller or processor under section 38(2)(b)(iv) may hamper the rights of the data controller, processor, and the data subjects. Hence, we recommend that the access to data by government authorities should be subject to judicial oversight, and requests for data access should be published (without identifying individuals) in the Data Protection Authority's monthly transparency report. It should be stated in the law rather than left to the rules. Without allowing the right to self-defence of the controller, the powers of the Data Protection Authority to ban data processing activities of the controller under section 38(2)(a)(v) may cause harm to many stakeholders. Hence, we further recommend that these two sub-sections be removed or at least ensure the self-defence of the data controller.
30.	Functions of data protection office, section 39	The provisions of the powers of the Data Protection Agency to take appropriate measures to enhance the quality of life of the citizens following government policy and program under section 39(b) are not consistent with any provision of a data protection law. There should have more detailed provisions for data protection registration requirements.	The provisions of the powers of the Data Protection Agency to take appropriate measures to enhance the quality of life of the citizens following government policy and program under section 39(b) (available in Bangla draft) is entirely irrelevant to data protection law and will create unrestricted scope of interpretation and abuse. Consequently, this provision should be removed from the text of the draft DPA bill. Section 39(i) of the draft DPA bill includes a provision for data protection registration without providing any details. While it may be appropriate to incorporate a registration requirement in the DPA for certain data controllers, processors, or other natural or legal entities, several questions should be considered before doing so. These questions may include: (a) which entities are required to register? (b) what are the particulars of the registration? (c) is the registration requirement mandatory, and if so, for which data? (d) are there any exceptions to the registration requirement, among others?

			Thus, before introducing a registration requirement, the necessary details must be incorporated into the draft DPA taking these questions into consideration. Doing so will ensure that the registration requirement is straightforward and comprehensive and can achieve its intended purpose of enhancing data protection for citizens.
31.	Standard Operating Procedures (SOPs), or Code of Conduct, section 40	The DG of the Data Protection Agency has been empowered to prepare the standard operating procedures (SOPs), or code of conduct, which is the task of controllers, processors, or data protection officers for a particular organisation or group of organisations.	To ensure the proper implementation of data protection regulations by businesses, regulatory bodies may encourage relevant stakeholders such as controllers, processors, and data protection officers in a particular organisation or group of organisations to prepare codes of conduct tailored to the specific features of their respective processing sectors and the needs of macro, micro, medium, and small-sized enterprises. Best practices indicate that these stakeholders, including businesses, controllers, or processors, should prepare the code of conduct and submit it to the respective supervisory authority for approval. Upon approval, businesses are required to adhere to these codes of conduct to regulate their data processing activities. However, according to Section 40 of the draft DPA, the DG of the Data Protection Agency is empowered to prepare codes of conduct that will appear as binding upon individuals. The DPA considers these codes of practice as regulations, indicating that they will be treated as the law; non-compliance with it resembles non-compliance with the law itself. This treatment of codes of practice as ‘law’ represents a misunderstanding of the data protection framework. Additionally, it raises questions regarding the Director General’s technical knowledge and competence to issue such codes of practice. We, therefore, recommend that the section be amended to entrust the task of adopting SOPs or Code of Conduct in accordance with the provisions of the

			DPA upon the relevant organisations or groups of organisations.
32.	Storage of sensitive data, user-created or generated data and classified data (data localisation policy), section 44	Section 44 of the draft DPA lays down data localisation principles intending to store the citizens' personal data within the geographical boundary of Bangladesh. There are enormous risks in establishing and maintaining the necessary infrastructures for data localisation in a country like Bangladesh. There are also huge risks of losing business opportunities in Bangladesh in the digital sector.	Section 44 of the draft Data Protection Act (DPA) contains data localisation provisions that require sensitive, user-generated, and classified data to be stored within Bangladesh's geographical boundaries. However, there are potential risks associated with establishing and maintaining critical data server infrastructures in Bangladesh. Enforcing strict data localisation regulations may exacerbate citizens' vulnerability to privacy violations and impede their freedom of expression. Moreover, implementing data localisation policies may increase business costs, restrict access to specific services and technologies, have a chilling effect on the free flow of information and freedom of expression, create barriers to innovation and collaboration, and make it more challenging for multinational companies to manage data across different jurisdictions. Additionally, data localisation requirements may fragment the data ecosystem and harm the overall economy. Furthermore, the mandatory data localisation requirements could significantly impede the development of local technology companies in Bangladesh, in conflict with the country's 'Smart Bangladesh' vision. Consequently, we recommend a comprehensive evaluation of data localisation's economic and environmental impacts before enacting legislation. The data localisation provisions should either be made non-obligatory or removed from the draft DPA.
33.	Provisions relating to the transfer of data, section 45	Section 45(1) of the draft DPA permits the transfer of personal data outside Bangladesh for inter-state trade, international relations, or other reasons determined by the Government. Furthermore, the transfer of sensitive data, user-generated data, or any other data outside Bangladesh is permissible	Conditional permission for cross-border data transfer may hamper the intended purposes of the DPA. The procedural constraints as determined by the Rule may pose a significant challenge to cross-border data transfer, as any delay or potential complexities in the rule-making process would also hinder the intended purpose of the Act. Additionally, section 45(2) of the draft DPA stipulates that the Bangladesh Bank, Bangladesh Telecommunication Regulatory Commission (BTRC), and the National Board of Revenue (NBR) would follow their procedure for cross-border data transfer, which could

		with the consent of the data subject and in accordance with the prescribed procedure determined by the Rule (section (3)(b)).	exacerbate the situation. To optimise the efficacy of the draft DPA, we recommend that sections 44 and 45(2) and 45(3) be omitted entirely.
34.	Data protection register, sections 46, 47 & 48	Data protection registration may pose various challenges for the Data Protection Agency.	The requirement for data protection registration may pose various challenges for the Data Protection Agency, including administrative burdens, complexity, data security risks, loosening of liability of data controller, varying requirements, and limited benefits. In light of the strict demands for internal accountability, it is notable that the General Data Protection Regulation (GDPR) and numerous other recent data protection regulations globally do not include such registration requirements. Considering the costs of compliance, administrative burdens, complexity, data security concerns, inconsistent requirements, limited benefits, and a lack of technical expertise, we recommend deleting the data protection registration requirements from the draft DPA.
35.	Inquiry and remedy of the complaints, section 50	In section 50(1), the Director General is mandated to investigate and, where necessary, examine any complaints brought before him under section 49 in accordance with the guidelines prescribed by the Rule. Alternatively, the Director General may assign a subordinate official to conduct the investigation and inquiry.	The question is – whether the Director General or his/ her subordinate officers have the technical, logistic, or administrative capacity to deal with hundreds of complaints that may arise every single day. In case of non-compliance with any provision of this law, the Director General may take the necessary action to file a case or initiate legal proceedings against the controller, processor, collector or authorised person without giving them the right to self-defence. The question is - whether the Director General can proceed with legal actions against an accused data controller or other relevant data processing entity without giving them the right to self-defence. The answer is negative as it breaks the principles of natural justice, i.e., *audi altarempartem,* - none should be condemned unheard/ listen to the other side/ let the other side be heard.

			Hence, it would generally not be fair or lawful for a data protection authority to proceed with legal actions against a data controller without allowing them to defend themselves. Considering the above, we recommend incorporating the right to self-defence of the controller before taking any legal action on the complaint of a data breach.
36.	Imposition of punishments by Rule, section 55	Section 55 empowers the Government to impose punishments by Rule for unknown reasons. This creates the scope of the arbitrary abuse of power.	Imposing punishments without a clear rationale shall create the scope of arbitrary, targeted and discriminatory abuse and hence can be counterproductive and potentially harmful. This approach undermines the principles of fairness and due process, which are fundamental to the legal system. It also undermines the effectiveness of the punishment itself, as individuals may be more likely to resent the punishment and the authority that imposes it. Hence, the imposition of punishments by Rule under section 55 should be either dropped or amended to incorporate provisions of a transparent and fair process, prevent the undue imposition of punishments without a clear rationale and ensure the legitimacy of punishments on concrete, specific grounds.
37.	Compensation for non-compliance to the law, section 56	Section 56 of the draft DPA empowers any secret or hidden data protection agency/ authority to receive compensation for a data breach.	There cannot be any secret or hidden data protection agency/ authority, as this provision will undermine the principles of transparency and accountability, which are essential for building public trust and confidence in a data protection regime. The lack of transparency and accountability can lead to abuses of power, as the authority may operate without oversight or scrutiny. This provision can erode the Rule of law by allowing for arbitrary and capricious decision-making. A hidden data protection authority can also negatively impact the privacy rights of individuals by limiting their access to information and restricting their rights. Therefore, we recommend that section 56 be dropped and all measures be incorporated to ensure that the data protection authority operates fully transparently and subject to appropriate levels of oversight and accountability.

38.	Violations of certain provisions of this Act by a foreign company, section 57	Any foreign entity registered under Chapter 10 of the Companies Act, 1994 (Act No. XVIII of 1994) that contravenes the provisions outlined in sections 51, 52, 53, 54, and 55 shall be subject to an administrative fine. The fine may extend up to 5% (five per cent) of its total turnover from the preceding financial year in Bangladesh.	It is unclear why the proposed bill does not address data breach incidents committed by unregistered foreign companies. Although regulating the data processing activities of unregistered foreign companies presents a formidable challenge, it is crucial to outline regulatory measures against such actions. We also recommend incorporating a provision under which the relevant data protection authority in the jurisdiction where the company is registered is notified of any data breaches to take appropriate legal and technical actions.
39.	Appeal to the Government, section 59, application to the Government for an appropriate remedy, section 60(3).	Under section 59 and section 60(3), the Government has been proposed as the appeal authority. The logic is not clear.	According to the prevailing international best practices, the Government is not the appeal authority for remedy on a matter relevant to DPA. Since the Government is a data subject as well as a data controller, there will be a conflict of interest if it is entitled to be the appeal authority. We recommend that this provision be dropped, and remedial measures be left to the judicial process.
40.	Application of the Code of Criminal Procedure, 64	Code of Criminal Procedure has been made applicable for offences for breach of DPA.	International best practices indicate that data protection laws are under the jurisdiction of civil laws rather than criminal laws. The primary aim of data protection laws is to ensure that personal data is processed fairly and lawfully. Therefore, the focus is on imposing administrative fines and other civil remedies to deter non-compliance with data protection rules and regulations. Data protection laws are relatively new, and there is still a lack of uniformity and consensus regarding the nature and scope of criminal offences potentially be applied to data protection breaches. Furthermore, criminal sanctions can be difficult to enforce across different jurisdictions, given that data flows across borders and the legal systems of different countries may not align with each other. The complexity of enforcement and the burden of proof in criminal cases may also make it challenging to establish criminal liability for data protection

			breaches. We, therefore, recommend that the provision for the criminal sanctions be dropped, and civil remedies and administrative fines be incorporated to ensure effective compliance with data protection rules and regulations.
41.	Offences committed by companies, section 65	It is unacceptable to simultaneously impose liability grossly on the owner, chief executive, director, manager, secretary, partner, officer, other staff, or representative.	The responsibility for a data breach within an organisational framework can vary depending on factors such as size, structure, and policies. Generally, the ultimate responsibility for a data breach lies with the organisation's leadership, including the owner, chief executive, director, or manager, who are responsible for ensuring that the organisation implements appropriate security measures and policies to protect sensitive data, not the subordinate. However, other staff members, including officers, partners, secretaries, representatives, and other employees, may also share some limited responsibility for a data breach if they fail to follow established security policies and procedures or engage in behaviour that compromises the security of the organisation's data. Above all, the primary responsibility of data protection lies to the highest authority, not their subordinate. Considering the facts, the relevant section shall have to be amended.