Personal Data Protection Act, 2024 (draft)

Better than Earlier
Still a Tool for Control and Surveillance

28 April 2024

1. INTRODUCTION

The then outgoing Cabinet of Bangladesh approved the draft Personal Data Protection Act, 2024 (PDPA) on 27th November 2023, immediately before the 12th General Election. With the general election concluded the draft law is expected to be placed before the parliament soon. As a clear break from the tradition, this specific piece of legislation has gone through several rounds of revision, and various stakeholders, including Transparency International Bangladesh (TIB) and other civil rights organisations, were involved in the review process. We appreciate that the draft, in its current form, incorporates many recommendations put forward by the stakeholders, including TIB. However, after careful consideration, it has become clear that this review has become a 'number game' where many recommendations have been accepted. In contrast, crucial recommendations involving the safeguarding of fundamental rights remained overlooked. The current TIB and Article 19 South Asia review will only focus on these critical aspects.

TIB and Article 19 are concerned that more than the protection of personal data, the draft PDPA 2024 continues to be a potential tool to legalise control of personal data by the Government, especially by some state agencies, including the proposed Data Protection Authority, which, as per the current draft remains in government control. TIB and Article 19 also hold the view that it provides the scope for more substantial and systematic surveillance in society by state agencies by using personal data for which the draft provides unaccountable authority without judicial oversight, which may lead to violations of the fundamental rights of individuals.

2. REVIEW

2.1 Beyond Necessity: Personal Data Protection Act Needs a Rights-Based Approach

The draft PDPA rightly emphasises the need for data protection due to advancements in research and development, international standards, and the overdue nature of such regulations. However, it does not reference the existing constitutional provisions, which is a more compelling justification. It will also lay out the basis for robust legislation that would ensure and defend fundamental rights like privacy and freedom of expression.[1] This rights-based approach ensures the PDPA prioritises the rights of Bangladeshi citizens, not just keeping pace with progress. It becomes a powerful tool for upholding the very foundation of a free and democratic society in the digital world.

[1] Article 1 of GDPR: (1) This Regulation lays 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. (2) This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data. (3) The free movement of personal data within the Union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.

2.2 Broad Scope and unspecific definition Threaten Core Objective

The draft PDPA's broad reach prioritises extensive control over all data processing, potentially neglecting individual control over personal information deviating from established frameworks like the EU's GDPR. Additionally, the draft's definition of "personal data" lacks specificity.[2] The same applies to the definitions of "data fiduciary" and "processor". The current wording encompasses all data, not just personal, extending their obligations beyond personal data protection.[3]

By narrowing the PDPA's scope to personal data, Bangladesh can align with best practices and ensure a more efficient, effective system prioritising citizens' digital rights. On the other hand, in the absence of specific definition of personal data, there will be a wide scope of arbitrary interpretation of what is personal data and what is not, which may lead to abuse.[4]

2.3 Data Localisation

Section 51 of the draft act stipulates that all classified data must be stored within Bangladesh's territory. The government will occasionally and arbitrarily determine what data type is classified without limitation or reference to objective criteria. Such a vague provision can effectively be used as a tool of digital authoritarianism to limit democracy and human rights.[5]

Data localisation gives governments more control over that data and the companies that handle it. Often presented as protecting privacy or security, this approach is especially concerning as the governments can use it to stifle free speech, privacy, and other human rights.[6] Every online click, swipe, and purchase leaves a digital trail. This data, from location to contacts and purchases, can be incredibly revealing. It could expose the political views, religious beliefs, or even the sexual orientation of the data subjects. The constant collection and use of this data, especially without proper

[2] Article 4 of GDPR: (1) 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

[3] Section 2(d) and 2(j) of the PDPA

[4] We recommend that in line with GDPR, the definition of personal data (art 2na) be more specific enough to include such identifiers as: name and surname; email address; phone number, home address; date of birth; race; gender; political opinions; bank, non-bank and other financial services account numbers, credit card numbers; data held by a hospital or doctor; photograph where an individual is identifiable; identification card number; a cookie ID; internet protocol (IP) address; location data (for example, the location data from a mobile phone); the advertising identifier of phone. We also recommend that information about public authorities and companies should not be treated as personal information, nor such entities be treated as persons under this Act, and Art 2(dha) be accordingly amended.

[5] https://www.csis.org/analysis/real-national-security-concerns-over-data-localization

[6] https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

safeguards, seriously threatens privacy. In their comments on the earlier draft, the Global Alliance for Data Protection (GADP) raises concerns about the lack of independent oversight for data localisation decisions.[7]

With data stored locally and limited oversight, the government's data practices become less transparent. Holding them accountable for potential breaches or misuse becomes difficult. Moreover, Bangladesh may not have the same expertise or resources as international cloud service providers for data security. Localising data can create a single point of access for hackers or even government surveillance. A successful breach could compromise the sensitive information of journalists, CSOs and data subjects.[8]

Data localisation also effectively ignores the accountability principle. International regulations might have limited enforcement power within a country, especially if data is stored locally. This can create a situation where a government can potentially disregard international best practices regarding data protection with minimal consequences.

Therefore, it is indispensable to undertake a further review of the data localisation question in consultation with relevant experts, sector specialists and human rights defenders.

2.4 Data Protection Authority is not independent

We have long advocated for an independent Data Protection Authority and independent Commission outside Government control, which has been ignored even in the latest draft. Instead, the draft proposes that a Data Protection Board be appointed by the government and an appellate authority adjudicate grievances based on the decision of the Data Protection Board, which is again directly appointed by the government. This will place the government firmly in control of all citizens' data. This is particularly peculiar given that the government is the most significant data processor and must be bound by data protection law without any scope of conflict of interest.[9]

The draft proposes to entrust the Data Protection Board with a wide range of authority, including investigating, accessing the data, entering the establishment and taking control of the data storage facilities, banning data processing, ordering the cessation of sending data to any recipient from another country or international organisation, etc.[10] To further solidify total governmental control over citizens' data,

[7] https://globaldataalliance.org/wp-content/uploads/2022/09/09072022gdabgdpa.pdf
[8] https://ijoc.org/index.php/ijoc/article/viewFile/3854/1648
[9] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4251540
[10] Section 40 of the draft Personal Data Protection Act

section 65 stipulates that the government can, amongst other reasons, to preserve public order, instruct the Board to comply with any instruction it deems fit.

The government must consider that an independent Data Protection Authority (DPA), free from political, governmental or commercial influence, can act as a neutral arbiter between individuals and data controllers (organisations collecting and processing data). This fosters public trust that the DPA will enforce data protection laws fairly and objectively.[11] Furthermore, an independent DPA is more likely to be transparent in its decision-making processes and hold data controllers accountable for non-compliance with data protection laws.[12] This also ensures effective enforcement and deters data controllers from violating individual privacy rights.[13]

Therefore, we recommend that, consistent with global best practice, the draft PDPA 2024 be amended to provide for an Independent Data Protection Commission outside the control of the Government or any other state agencies.

2.5 Unfettered access to personal data without judicial oversight

Section 10(2-d) stipulates that personal data can be accessed from any data processor to ensure national security or to prevent/identify/investigate any crime. The process of such access will be determined by rules formulated by the Data Protection Board, which is effectively another institution firmly under the government's control. In the absence of judicial oversight and an independent DPA, this provision effectively frustrates the very objective of a data protection law by making ways to access personal data and further strengthening the surveillance apparatus.

Access to personal data must be subject to judicial oversight. So that a judge can assess the legitimacy of a data access request and ensure it complies with data protection laws, minimising the risk of unnecessary intrusion into someone's privacy and meeting the test of proportionality. The judiciary can weigh competing interests and provide an independent check on the power of government agencies or other entities seeking access to personal data. This helps prevent abuse and ensures due process.[14]

2.6 Broad exemptions diminishing data protection

The draft PDPA proposes wide-ranging exceptions for activities deemed to be in the "public interest" (Section 7(6)), which could enable public authorities to circumvent the requirement for meaningful consent. This undermines the PDPA's envisioned mechanisms for transparency and accountability, ultimately reducing individual control over personal information.

[11] https://commission.europa.eu/law/law-topic/data-protection_en (Article 57 - Independence)
[12] https://www.dataprotection.ie/ (About Us - Our Approach)
[13] https://www.bfdi.bund.de/EN/Home/home_node.html
[14] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3599201

Furthermore, Sections 33 and 34 of the draft PDPA grant exemptions from "relevant provisions" in various scenarios, including law enforcement activities, Tax collection, Court-ordered disclosures, Broadly defined "regulatory functions", and any additional purposes deemed necessary by the government.

The extensive scope of these exemptions, particularly the open-ended nature of "regulatory functions" and "any other purpose" clauses, raises concerns about potential loopholes allowing government activities to bypass most, if not all, PDPA protections. This includes safeguards like the notice principle ensuring transparency in data processing and data security measures aimed at protecting information confidentiality and integrity.[15] [16]

We believe that the PDPA's current broad scope and lack of clear definitions in its exemption clauses pose a significant risk. A more refined approach that balances the need for legitimate public functions with robust data protection safeguards is essential to ensure that the PDPA effectively protects the fundamental right to privacy in the digital age.

2.7 Unrealistic enforcement

Section 1(2) stipulates that the law will be effective from the date of publication of the gazette notification. Without a staggered approach, data protection law enforcement will become unrealistic. Many smaller entities might not have the financial and logistical resources or technical expertise to comply with all aspects of a data protection law immediately. A staggered approach allows them time to adjust their practices, invest in the necessary technology, and develop compliance procedures. Furthermore, immediately imposing all regulations on all data processors can create a significant administrative burden. A staggered approach allows data protection authorities to prioritise enforcement efforts on high-risk data processors, such as those handling sensitive personal data or those with a history of data breaches. This ensures that the most critical areas are addressed first.

3. CONCLUDING REMARKS

The draft Personal Data Protection Act (2024) represents a positive step towards safeguarding personal data in Bangladesh. However, significant concerns remain regarding the lack of robust safeguards for fundamental rights.

[15] https://gdpr-info.eu/art-13-gdpr/
[16] https://gdpr-info.eu/art-32-gdpr/

3.1 Critical areas for improvement include

Focus on Rights, Not Control: The PDPA needs a fundamental shift. Referencing existing constitutional provisions on privacy and freedom of expression establishes a rights-based foundation. A more precise definition of "person" and "personal data" and a focus on robust data security, including clearly defined exceptions, are also crucial.

Data Localisation: The current approach risks hindering free speech and information access. Alternatives that prioritise data security without compromising human rights should be explored.

Independent Data Protection Authority: Establishing an independent DPA (e.g., Independent Data Protection Commission), free from government influence, is crucial for ensuring fair and impartial enforcement of the proposed data protection law.

Judicial Oversight: Data access requests should require mandatory judicial approval to prevent unwarranted intrusion into personal privacy and ensure compliance with data protection principles.

Staggered Enforcement: A phased implementation approach allows businesses, particularly smaller entities, to adapt and comply with regulations more effectively.

Addressing these critical aspects, the current draft of the Personal Data Protection Act 2024 can evolve into a powerful tool for protecting individual privacy in the digital age. We urge the government to consider these recommendations and remain available to engage in further dialogue with stakeholders to ensure a data protection law that upholds fundamental rights and fosters trust in the digital ecosystem.

END