Legal Research & Analysis

Innovative

Research Article

The Personal Data Protection Act, 2026 of Bangladesh, Privacy and Global Data Governance

Mafruza Sultana* and Md. Sobhan Ali

Department of Law, Uttara University, Dhaka 1230, Bangladesh; sobhan.ali@uttarauniversity.edu.bd
* Correspondence: mafruza1716@gmail.com

Abstract: Bangladesh has entered a transformative phase in its digital governance journey with the enactment of the Personal Data Protection Act, 2026, which evolved from the Personal Data Protection Ordinance, 2025, and its subsequent amendment in February 2026. Current research is a comprehensive analysis of Bangladesh's data protection framework, examining its legislative evolution, key statutory provisions, institutional architecture, and implementation challenges. Based on comparative analysis with the European Union's General Data Protection Regulation (GDPR), documented breach incidents involving Bangladesh's National Identity database and private-sector data-fiduciaries, and scholarly and civil-society critiques, the study explores significant structural concerns including regulatory independence, state surveillance risk, and the balance between individual rights and state prerogatives. While the Act is a historic shift by recognizing citizens' personal data as their own property, substantial gaps exist between legislative text and effective implementation, in the absence of a mandatory breach-notification duty to affected individuals and Prime Minister's Office as the enforcing Authority. Strengthening Bangladesh's data protection framework through enhanced institutional independence, and transparent safeguards on state exemptions will offer closer alignment with international human-rights standards.

Keywords: data protection; privacy; GDPR; surveillance; digital rights; data governance

Citation: Mafruza Sultana and Md. Sobhan Ali. 2026. The Personal Data Protection Act, 2026 of Bangladesh, Privacy and Global Data Governance. *Legal Research & Analysis* 4(3), 1-8. https://doi.org/10.69971/lra.4.3.2026.195

1. Introduction

The rapid digital transformation of Bangladesh, characterized by widespread smartphone adoption, expanding digital financial services, and the integration of artificial intelligence into daily life, has generated unprecedented volumes of personal data. This datafication of society has created both opportunities and vulnerabilities, prompting urgent questions about how to protect citizens' privacy rights in an era of algorithmic governance. The Personal Data Protection Act, 2026 (Law 63 of 2026), is Bangladesh's most significant legislative response to these challenges, establishing a comprehensive legal framework for the processing, storage, and transfer of personal data across both the public and private sectors.

This legislative intervention was necessary due to high-profile data-security failures which preceded the law's evolution phase. In 2023, a vulnerability in a government partner website exposed the names, addresses, phone numbers, and National Identity (NID) numbers of more than fifty million citizens, data that subsequently circulated on Telegram channels.1 In August 2025, hackers exfiltrated 410 gigabytes of customer data, including the purchase histories of forty lakh registered customers, from the retail chain Shwapno, and the breach was not disclosed to affected customers for roughly seven months (Halder 2026). An investigation by the fact-checking outlet Dismislab highlighted that the final voter list for Bangladesh's thirteenth parliamentary election, containing names, voter numbers, parents' names, dates of birth, occupations, and permanent addresses, was sold openly on Facebook for a few dozen taka per record.2

This background frames the central question this paper investigates: will the new statutory architecture constrain the misuse of personal data, particularly by the state itself, or does it primarily formalize obligations for private actors while leaving the most consequential data holder, i.e., government, largely self-regulated? Current study explores the Act's development from its origins as an ordinance promulgated under emergency executive authority to its current status as an Act of

1 https://www.thedailystar.net/tech-startup/news/over-5-crore-bangladeshi-citizens-data-remains-exposed-online-3363866
2 https://en.prothomalo.com/bangladesh/crime-and-law/bjbguaev03

Parliament. It analyses the substantive provisions of the legislation, evaluates its institutional framework, and identifies critical implementation challenges. The act is compared with comparative perspectives, particularly the European Union's General Data Protection Regulation (GDPR), which has become the global standard for data protection standards.

2. Legislative History of Act

Prior to this comprehensive data protection legislation, Bangladesh's approach to privacy and data protection was fragmented and inadequate. The Constitution of the People's Republic of Bangladesh provides a right to privacy of correspondence and other means of communication under Article 43[3], but this constitutional guarantee is largely unenforceable in the digital context. Sectoral legislation in the financial sector-imposed data retention requirements and restrictions on data transfers, (Constitutional Right to Privacy and Data Protection in Bangladesh: A Living Originalist Interpretation 2025), while the Information and Communication Technology Act, 2006, and the Digital Security Act, 2018, contained provisions related to cybersecurity and personal information protection in relation to critical information infrastructure. The Digital Security Act itself empowered the government to take arbitrary action against online dissent rather than protecting citizens' data as such. (Hasan 2023; Rahman 2022; Zafarullah and Sabrina 2026). Bangladesh's data-privacy legal regime, while sharing several common principles with the GDPR, suffered from a fundamental absence of data subjects' ownership recognition, rendering it less comprehensive in scope and providing fewer rights and protections (Haq et al. 2025). Due to this absence of ownership recognition, individuals had limited control over how their personal information was collected, processed, and shared by both public and private entities.

In November 2023, the then-cabinet approved a draft Personal Data Protection Act, 2024, which underwent multiple revisions throughout 2024.[4] Rather than prioritizing the privacy and rights of users, the draft meant to function as a potential tool to legalize government control of personal data, in part because it contained a broad exemption for data processed "for the prevention or detection of crime or for the purpose of investigations" without any accompanying requirement for judicial authorization or a stated justification.[5]

The legislative journey accelerated dramatically in late 2025 with the promulgation of the Personal Data Protection Ordinance, 2025 (PDPO)[6], appeared in gazette on November 6, 2025, by the interim government, under the President's ordinance-making power in Article 93(1) of the Constitution, which authorizes the issuance of ordinances when Parliament stands dissolved and "circumstances exist which render immediate action necessary (Al Rohan 2025). This executive action, was accompanied by a companion National Data Management Ordinance (NDMO), later reconstituted as the National Data Governance Ordinance, creating a twin framework for data governance and national digital identity. Scholars observed, while "ordinances are constitutionally valid, they are simply not constitutionally deliberative".[7] The lack of parliamentary debate indicated that the relationship between citizen and state in the digital era were decided by executive rather than through democratic deliberation. The drafts had reportedly been approved despite repeated concerns raised by civil society and industry stakeholders, reflecting a broader pattern of accelerated policy-making without sufficient transparent consultation.[8]

The ordinance established several key definitions and principles that were incorporated into the subsequent Act. Section 2 of the ordinance defined "personal data" as any data relating to a person by which that person can be identified, such as name, parent's name, identification number, financial data, location data, or any other similar online identifier or material comprising the physical, physiological, genetic, or economic characteristics of an individual. The ordinance also introduced the crucial distinction between "data-fiduciary" (the person who processes personal data for a specific purpose or supervises such processing) and "processor" (any person who processes data on behalf of a data-fiduciary), terminology that departs from the GDPR's "controller/processor" framing and instead borrows the fiduciary language used in India's Digital Personal Data Protection Act (Haq and Zainal et al. 2025).

On February 5, 2026, the President promulgated the Personal Data Protection (Amendment) Ordinance, 2026 (Ordinance No. 23 of 2026), which made two consequential changes to the original text ("President Implemented Personal Data Protection (Amendment) Ordinance 2026).[9] It narrowed the ordinance's data-localization mandate: rather than requiring broad in-country storage, the amendment required only that at least one synchronized, real-time copy of data categorized as "restricted" or processed by Critical Information Infrastructure, as defined under the Cyber Security Ordinance, 2025, be maintained within Bangladesh's borders. It replaced the threat of imprisonment for managing directors of companies found to violate data-subject rights under section 48 of the original ordinance with monetary fines only. Industry groups, including the Computer & Communications Industry Association, welcomed these changes as addressing some of their earlier concerns (Computer & Communications Industry Association[10]). Parliament of Bangladesh enacted the Personal Data Protection Act, 2026 (Law 63 of 2026), repealing the Personal Data Protection Ordinance, 2025, and the subsequent Amendment Ordinance.[11] The Act was deemed to have come into effect retroactively on November 6, 2025, although sections 23 and 31–35, relating to the appointment of chief data officers and to the filing of complaints and administrative penalties, were delayed pending further government notification. Full enforcement mechanisms, including the complaint, investigation, and penalty procedures, were not expected to activate until on or around May 13, 2027, roughly eighteen

---

3 The Constitution of the People's Republic of Bangladesh, art. 43, http://bdlaws.minlaw.gov.bd/act-367/section-24591.html

4 https://securiti.ai/bangladesh-personal-data-protection-act-overview/

5 Personal Data Protection Act, 2024 (Draft) (Bangladesh), https://www.ti-bangladesh.org/en/articles/law-review/6965

6 https://www.thedailystar.net/tech-startup/news/bangladeshs-personal-data-protection-ordinance-2025-key-takeaways-4015401

7 https://www.thedailystar.net/law-our-rights/news/new-data-laws-bangladesh-critique-4038266

8 https://techglobalinstitute.com/announcements/joint-statement-on-emerging-digital-laws-in-bangladesh/

9 https://www.dataguidance.com/news/bangladesh-president-bangladesh-enacts-personal-data

10 https://commission.europa.eu/topics/strengthening-european-competitiveness/eu-competitiveness-looking-ahead_en

11 https://www.dataguidance.com/news/bangladesh-parliament-bangladesh-enacts-personal-data

months after the original ordinance's gazetting, leaving organizations a compliance runway rather than an indefinite grace period (Bangladesh Data Privacy Laws 2026)

Concerns remained about the rushed legislative process and the limited opportunity for meaningful parliamentary scrutiny. The hasty approval process without adequate expert consultation, raised questions about whether the final legislation adequately reflected international best practice or adequately protected citizens' rights.[12] The Business Standard characterized the net effect more charitably, noting that "given the slow pace of enacting time-sensitive, fit-for-purpose laws in Bangladesh, the quick adoption of the Act deserves recognition before scrutiny".[13]

3. Key Provisions of the Personal Data Protection Act

The Act has an expansive territorial scope, applying to any data-fiduciary or processor that is domiciled, ordinarily resident, or operating in Bangladesh, as well as to entities processing personal data outside Bangladesh in connection with offering goods or services to, or monitoring, data-subjects located within Bangladesh. [14] This extraterritorial application aligns with the GDPR approach and reflects an understanding that data protection cannot be limited by national boundaries. The Act applies to the processing of personal data of any person and to any data-fiduciary, processor, or other person engaged in such processing. The Act was influenced by civil society advocacy for the term "personal data" to be emphasized over "data" more broadly.[15]

3.1 Core Definitions and Data Protection Principles

Section 2 of the Act provides comprehensive definitions of key terms that establish the foundation for its substantive provisions. Under subsection 17, section 2 of the Act, Personal Data is defined as any data relating to a person by which that person can be identified, including name, parent's name, identification number, financial data, location data, online identifiers, and physical, physiological, genetic, and economic characteristics. This definition was one of the most contested aspects of the legislative process. Civil society organizations had argued that the definition should explicitly reference "an identified or identifiable natural person" to align with international standards and ensure the Act's focus on protecting natural persons rather than legal entities.[16] Sensitive Personal Data receives enhanced protection under the Act and includes genetic or biometric data, data relating to ethnic minority or race and community, philosophical or political opinions, religious beliefs, trade union membership, health data, data relating to sexual life, and data relating to criminal offences. The Act also allows for additional categories of sensitive data to be prescribed by rules, a provision that raised concerns among civil society advocates who argued that declaring sensitive data by rule rather than by statute could lead to arbitrary expansion without adequate safeguards (Adnan and Adib 2025) .Data-Subject means the individual to whom the personal data relates, while Data-Fiduciary is defined as a person who alone or jointly processes personal data for any specific purpose or supervises such processing.

The Act establishes seven core data protection principles that guide all processing activities. Fairness and Reasonableness requires that personal data be processed in a fair and reasonable manner that respects the provisions of the Act. Integrity mandates that no additional or unnecessary personal data be processed and that data remain accurate and up to date. Retention limits data storage to the period authorized by the Act and requires permanent destruction of data when retention is no longer permitted. Access and Data Quality grant data-subjects the right to access their data and correct inaccuracies. Disclosure requires accountability in data disclosure and prohibits disclosure for purposes other than those specified at collection without consent. Security mandates proper security measures to prevent damage, misuse, or unauthorized access. Enforceable Standards requires adherence to standards set by regulatory authorities or covered by international treaties.

3.2 Grounds for Processing and Data Subject Rights

Section 5 establishes consent as the primary legitimate ground for processing, requiring that consent be free, specific, clear, and capable of withdrawal. The burden of proving valid consent rests with the data-fiduciary. This represents a significant shift from previous practice, where data could be collected and processed without meaningful consent mechanisms. However, the Act also provides numerous exceptions where processing may occur without consent, including for the performance of a contract, compliance with legal obligations, establishing or defending legal rights, public health and medical emergencies, court orders, government functions, and employment-related matters. Critics have argued that these exceptions are broad enough to allow significant state processing without independent oversight[17]

The Act confers several rights on data-subjects that empower individuals to exercise control over their personal information. Right of Access under sections 10 and 11 allows data-subjects to submit written requests to access their personal data, obtain copies, and understand how their data is being used. Right to Correction enables data-subjects to request correction of inaccurate, incomplete, or misleading data. Right to Portability allows data-subjects to have their data transferred to another data-fiduciary. Right to Withdraw Consent grants data-subjects the ability to withdraw consent for storage, processing, or automated decisions. Right to Deletion allows data-subjects to request erasure of their personal data under certain conditions. The Data Guidance summary of the Act further notes an explicit opt-out right alongside these access, correction, and portability entitlements.

3.3 Security, Data Retention, Cross-Border Data Transfer and Enforcement

---

12 "The Revised Draft Data Protection Act (DPA) 2023: Review and Recommendations in Light of Submissions on the Earlier Version," n.d.

13 https://www.tbsnews.net/thoughts/personal-data-protection-ordinance-law-protects-you-everyone-except-state-1416106

14 Personal Data Protection Act, 2026 (Bangladesh), § 4.

15 https://www.article19.org/resources/bangladesh-draft-data-protection-law-must-protect-freedom-of-expression/

16 https://www.thedailystar.net/law-our-rights/news/revisiting-the-draft-personal-data-protection-act-2023-3780596

17 https://www.thedailystar.net/law-our-rights/news/new-data-laws-bangladesh-critique-4038266

The Act imposes affirmative obligations on data-fiduciaries to implement appropriate technical and organizational security measures to protect personal data from loss, misuse, unauthorized access, destruction, or alteration. Required security measures include pseudonymization and encryption, system security measures, the ability to restore data availability after incidents, and regular testing and evaluation of security measures. Section 20 requires data-fiduciaries to notify the Authority of personal data breaches within the prescribed time and manner. While the Act itself does not specify a fixed notification timeline, legal analysis suggests that a seventy-two-hour notification requirement to the regulator, as established in the ordinance, represents a sensible default aligned with global practice. However, the Act, unlike the GDPR, contains no freestanding, unconditional duty for a data-fiduciary to notify affected individuals themselves of a breach.

Section 18 prohibits data-fiduciaries from retaining personal data longer than necessary for the purpose for which it was collected. Records related to personal data processing must be preserved for at least five years. However, the Act permits exceptions for public interest, scientific research, historical research, or statistical purposes, where data may be retained beyond the prescribed retention period.

The Act categorizes personal data into four classes: public open, internal, confidential, and restricted. Confidential and restricted personal data must be stored within Bangladesh's jurisdiction. Internal and confidential data may be transferred abroad with data-subject consent or for contractual purposes, but only to countries with appropriate data protection standards.

The government initially proposed broad data-localization requirements, but these were significantly scaled back following concerns about their impact on investment and digital services. By early 2026, the government had removed broad localization requirements for technology companies generally, applying an in-country synchronized-copy requirement more narrowly to restricted data and to operators of Critical Information Infrastructure under the February 2026 amendment ordinance ("President Implemented Personal Data Protection (Amendment) Ordinance 2026).

4. Institutional Framework: The Data Protection Authority

The Act establishes a Data Protection Authority responsible for ensuring proper implementation of the law, protecting data-subjects' rights, preventing violations, issuing directions to data-fiduciaries and processors, and taking enforcement measures. The Authority is established under the companion National Data Governance and Interoperability Authority Ordinance, 2025 (the successor to the original NDMO), and is statutorily attached to the Prime Minister's Office (Manab 2026). Under the governance ordinance, the Authority is responsible for designing and operating the nation's data architecture, including digital interoperability systems and an identity layer linking core registers, while also enforcing compliance and imposing administrative penalties. The ordinance further establishes the National Responsible Data Exchange (NRDEX), a platform for secure data sharing between government agencies and approved private institutions intended to reduce data duplication and improve interoperability, and a Unified Digital Identity system connecting a citizen's National ID, passport, tax identification number, and other key registers into a single authenticated identity layer (Bangladesh Data Privacy Laws 2026). This combination of roles, i.e., architect, operator, and enforcer has raised concerns about the concentration of power and potential conflicts of interest.

The Act lacks explicit guarantees of the agency's independence, with major actions requiring prior government approval, including standard operating procedures and core classifications. Section 49 of the Act explicitly states that the government may issue directions to the Authority in the interests of national security or public order, and that the Authority is legally bound to comply (Manab 2026). Establishment of an independent data protection commission is being emphasized, as a government-appointed board could be biased and unable to hold the government accountable. Critics observed, "since the government itself is a user of personal information, a government-controlled board may lead to conflict of interest".[18] A government-appointed data protection board "could be biased and unable to hold the government accountable."

This institutional design contrasts starkly with the EU GDPR model, under which Member States must create independent supervisory authorities that act "with complete independence" in monitoring the law's application under Article 52.[19] The Court of Justice of the European Union has held that such authorities must act with complete independence from any external influence, including direct or indirect influence of the state. By contrast, one Business Standard analysis of the Bangladeshi framework observed that, compared with the GDPR's independence mandate or Singapore's Personal Data Protection Commission, a statutory body anchored in parliamentary accountability, “Bangladesh's Data Protection Ordinance falls short in granting the National Data Management Authority institutional autonomy" (Aziz 2026).

Similarly, there is asymmetry in enforcement capacity. The Authority may sanction private-sector entities such as banks or technology companies for data protection violations, but when government ministries misuse citizen data, the Authority, seated within the Prime Minister's Office, may be institutionally constrained. This creates what one commentator described as "a paradox: Big Tech may now face tighter rules, but Big State remains largely self-regulated".[20] Bangladesh's data protection framework operates alongside a set of pre-existing surveillance, telecommunications, and criminal-procedure laws that continue to govern the interception, monitoring, and disclosure of communications data, so that "the practical regulation of state surveillance continues to occur largely through these existing mechanisms rather than through the safeguards established within the data protection framework" (When Data Protection Fails to Protect 2026)

Bangladesh Telecommunication Regulation Act, 2001 (section 97) and the Cyber Security Ordinance, 2025 (Section 35), authorize interception of, or access to, traffic data and communications content on "reason to believe" that an offence has occurred,

---

18 https://www.newagebd.net/post/country/233876/independent-commission-demanded

19 Regulation (EU) 2016/679 (General Data Protection Regulation), art. 52, https://gdpr-info.eu/art-52-gdpr/

20 https://www.thedailystar.net/law-our-rights/news/new-data-laws-bangladesh-critique-4038266

is occurring, or may occur, a materially lower threshold than the safeguards contemplated within the data protection statute itself, and one that operates through parallel legal channels the PDPA does not reach.[21]

5. Critical Analysis and Challenges

The most significant concern is the potential for the Act and its companion governance ordinance to facilitate state surveillance rather than protect citizen privacy. Section 3 of the governance ordinance declares that its provisions shall take precedence over any other law, contract, or instrument in matters relating to the collection, storage, processing, security, and identification of persons, and the overall management and interoperability of national data . This supremacy clause effectively subordinates other legal protections to the data-governance framework, a design with no direct analogue in the GDPR, which instead operates under the European Charter of Fundamental Rights.

The identity layer mandated by the governance ordinance and its schedule is an ambitious technical unification of citizen data across multiple registers, i.e., National ID, passport, tax identification number, and other key databases. While advocates emphasize administrative efficiency and easier access to public services, critics warn that "when every register speaks to every other, the State gains the capacity to reconstruct a person's entire life-trajectory, where one lives, travels, works, banks and interacts online.[22] Under GDPR Articles 5 and 25, personal data must be collected for specific, explicit, and legitimate purposes and be limited to what is necessary. By contrast, the Bangladeshi framework contains no explicit general-purpose duties of purpose-limitation and data-minimization binding on state processing. This absence of constraints creates the risk that what is presented as "frictionless governance" could evolve into "frictionless surveillance."

The results of these institutional gaps are illustrated by a series of large-scale breach incidents involving Bangladeshi personal data, several of which predate or directly overlap with the Act's passage. In July 2023, a government website belonging to the Office of the Registrar General, Birth and Death Registration had exposed the personal data of more than fifty million citizens through a straightforward Google search; the exposed fields included names, addresses, phone numbers, and NID numbers.[23] From October 2023 onward, this leaked NID data became openly accessible on Telegram channels, and the Election Commission's NID division initially denied any breach of its servers before later investigations confirmed leaks at multiple institutions.[24] A separate incident in July 2025 involved an alleged sale of the personal data of 4.1 million citizens, including NID numbers, that security researchers flagged as raising serious compliance questions under the then-newly promulgated ordinance's breach-notification requirements to the National Data Protection Authority.[25] In August 2025, hackers breached the retail chain Shwapno's customer database, taking 410 gigabytes of data covering roughly forty lakh customers and demanding a $1.5 million ransom; when Shwapno refused to pay, the stolen data was published on the dark web in March 2026, seven months after the company first learned of the intrusion and without having notified affected customers in the interim (Halder 2026). In June 2026, the final voter list for the thirteenth parliamentary election comprising names, voter numbers, parents' names, dates of birth, occupations, and permanent addresses for crores of citizens was being sold openly on Facebook for amounts ranging from roughly thirty to two hundred fifty taka per record.[26] Commentary on this episode observed pointedly that Bangladesh's newly enacted data protection law "contains no mandatory breach notification requirement" obliging a fiduciary to inform affected individuals directly, meaning "there was nothing that required Shwapno to tell you sooner" and, at the time of writing, "apparently, nothing yet to stop someone from selling your address and date of birth for forty taka" (Manab 2026). All these incidents demonstrate two recurring patterns relevant to the framework's credibility. First, the state itself, through the NID database maintained by the Election Commission, which holds records for approximately twelve crore citizens, has been a repeat source of the most consequential breaches, undercutting the claim that the Act's principal function is to discipline private-sector misuse of data. Second, the absence of an individual-notification duty means that data-fiduciaries, whether public or private, have faced limited legal pressure to disclose breaches promptly to the people actually affected, as opposed to the regulator alone.

Concerns about surveillance infrastructure extend beyond the identity layer itself. The National Equipment Identity Register (NEIR), introduced as a technical solution for blocking stolen or illegally imported mobile handsets, is built on device and subscriber identifiers, IMEI, SIM card number, and International Mobile Subscriber Identity and has prompted recurring questions about whether it could function as a surveillance tool notwithstanding its stated regulatory purpose. Industry voices have offered divergent assessments: former Bangladesh Association of Software and Information Services president Fahim Mashroor characterised NEIR as "not a surveillance tool, as it is not a targeted system but rather general in scope," while cautioning that it must nonetheless "be done in strict accordance with the law" and subject to judicial or quasi-judicial oversight over any access, blocking decisions, or cross-system integration. The broader point for present purposes is that Bangladesh's national ID system is, as of 2026, still not fully and systematically linked with mobile numbers and device identities meaning that the identity layer contemplated by the governance ordinance remains a work in progress whose ultimate surveillance potential will depend heavily on implementing rules not yet finalized.

Section 24 of the framework creates a wide exemption for crime-fighting, investigations, regulatory work, statistics, and other government functions, on grounds including national security, public order, and crime prevention (Personal Data Protection Ordinance 2026). Critics have noted that the government can also issue directives to the Authority on grounds such as sovereignty, security, and public order, and issue orders related to data storage or transfer in urgent cases, which critics argued could grant

---

21 Bangladesh Telecommunication Regulation Act, 2001, § 97; Cyber Security Ordinance, 2025, § 35.

22 https://www.thedailystar.net/law-our-rights/news/new-data-laws-bangladesh-critique-4038266

23 https://www.bssnews.net/news/135324

24 https://en.prothomalo.com/bangladesh/ni5m1c1s4m

25 https://www.brinztech.com/breach-alerts/alleged-government-of-bangladesh-data-for-sale-4-1-million-citizens-at-risk/

26 https://en.prothomalo.com/bangladesh/crime-and-law/bjbguaev03

unchecked power without judicial oversight. The scope of exemptions has raised particular concern given Bangladesh's history of legal abuse and political repression under predecessor statutes such as the Digital Security Act. Without clear safeguards and effective independent oversight, activists, journalists, and minority communities may remain exposed to abuse and retaliation. Legal experts have called for every exemption to comply with the principles of legality, necessity, and proportionality, supported by judicial approval, clearly defined purposes, independent audit mechanisms, and regular public transparency reports.

The Act's institutional design places the Data Protection Authority within the executive branch, structurally inseparable from the government it is meant to regulate. Legal scholars have called for appointment of the Authority by Parliament with cross-party consent, fixed terms, protected budgets, and transparent rule-making that cannot be vetoed by the Cabinet Division. The GDPR model enshrines independence in its supervisory framework under Article 52, requiring that supervisory authorities act with complete independence (Giurgiu and Tine 2016). By contrast, Bangladesh's Authority sits within the executive branch, "simultaneously an architect, operator and enforcer, effectively acting as the referee and a player at once". This structural configuration is a fundamental departure from international best practice.

A significant gap identified by legal scholars is the absence of explicit general-purpose duties of purpose-limitation and data-minimization binding on state processing. Under the GDPR, these principles are fundamental to the entire regulatory framework, ensuring that data collection is limited to what is necessary and used only for specified purposes. The absence of these principles in Bangladesh's framework means that government agencies may collect and use personal data for purposes that were not specified at the time of collection, potentially leading to function creep and expanded surveillance capabilities. This gap is particularly significant given the expansive data consolidation enabled by the identity-layer and NRDEX provisions described above.

International best practice recommends a substantial grace period for organizations to prepare for compliance with comprehensive data protection legislation; the EU GDPR, for instance, was adopted in April 2016 but did not take effect until May 2018, providing more than two years for preparation. Bangladesh's framework, by contrast, deemed itself retroactively effective from the date of the original ordinance's gazetting, with only a subset of enforcement provisions delayed to mid-2027, creating a compressed timeline for businesses and government agencies to implement the necessary technical and organizational measures (Bangladesh Data Privacy Laws 2026).

Industry commentary has also warned that, if enforced rigidly, the compliance burden including data-localization obligations, mandatory Chief Data Officer appointments for significant data-fiduciaries, and restrictions on cross-border data transfer , could lead multinational companies to scale back operations or withdraw from the Bangladeshi market if global systems cannot be readily adapted to country-specific requirements, undermining a country "striving to diversify beyond traditional industries and attract foreign direct investment" (Rashid 2025).

The framework excessively relies on rule-making powers, which may lead to broad, potentially misused interpretations. Without mandatory publication requirements and legislative oversight, there is a risk of executive overreach. Rule-making provisions be limited, well-defined, and transparent before parliamentary approval. Accelerated drafting meant significant provisions changed between draft versions without documented public consultation, and that the ordinance in its earlier form "omits key principles considered the lifeblood of such laws."

6. Comparative Analysis with the GDPR

Bangladesh's data protection framework shares several common principles with the GDPR. Both establish consent as a primary basis for processing, provide data-subject rights including access, correction, and deletion, impose security obligations on data controllers, require breach notification to the regulator, and establish extraterritorial scope. The Act's data protection principles, fairness, integrity, retention, access, disclosure, security, and enforceability, parallel the GDPR's principles of lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability. The penalty structure, too, mirrors GDPR practice, with fines calculated as a percentage of annual turnover rather than fixed sums.

6.1 Critical Differences

Despite these commonalities, significant differences remain. Regulatory Independence: the GDPR requires independent supervisory authorities free from external influence, while Bangladesh's Authority is statutorily attached to the Prime Minister's Office and subject to direct government instruction under section 49. Purpose Limitation: the GDPR imposes a duty of purpose limitation that constrains how data can be used, while Bangladesh's framework lacks an explicit general-purpose limitation binding on state processing. Individual Breach Notification: the GDPR requires controllers to notify affected data subjects directly where a breach is likely to result in a high risk to their rights, whereas Bangladesh's Act requires notification only to the regulator, not to affected individuals.

Data Ownership: a comparative study found that the primary issue stemming from Bangladesh's earlier legal regime was the absence of data subjects' ownership recognition, rendering it less comprehensive in scope and providing fewer rights and protections; the 2026 Act addresses this in principle by recognizing personal data as belonging to the data-subject, though implementation of that recognition remains uneven (Haq and Zainal et al. 2025).

Data Protection by Design: the GDPR mandates data protection by design and by default under Article 25, requiring privacy measures to be integrated from the outset. Bangladesh's Act lacks an equivalent, freestanding obligation. Grace Period: the GDPR provided more than two years for compliance preparation, while Bangladesh's Act provides a substantially compressed timeline, with retroactive effect from the date of the original ordinance.

6.2 Implications for Adequacy

The differences between Bangladesh's framework and the GDPR have significant implications for potential adequacy determinations by the European Commission. An adequacy decision would allow personal data to flow freely between Bangladesh and the EU without additional safeguards. The European Commission's assessment considers whether the third country ensures an adequate level of protection, including effective independent oversight, enforceable rights, and effective legal redress. Bangladesh's

current framework, with its limitations on regulatory independence, its broad state exemptions, and its lack of robust purpose limitation, is unlikely to satisfy these requirements in its present form, a conclusion with direct consequences for Bangladeshi exporters of IT-enabled services who depend on smooth data flows with European counterparties.

7. Civil Society and Expert Perspectives

Transparency International Bangladesh has been a consistent advocate for strengthening Bangladesh's data protection framework. TIB recommended that earlier drafts of the Act be clearly titled to emphasize a focus on personal data, called for clearer definitions and a distinction between anonymized and pseudonymized data, and pressed for an independent data protection authority. TIB expressed concern that "though the government is formulating the law to protect personal data, there is a risk of controlling the personal data," noting that "society is increasingly coming under state surveillance with the enactment of new laws" (Transparency International Bangladesh 2023b).

ARTICLE 19, the international freedom-of- Earlier drafts fell short of GDPR standards in key areas including grace period, data protection principles, independent authority, and protection of foreign data subjects. Concerns exist about the constitutional propriety of using ordinance-making powers for foundational legislation and about the structural weaknesses of the Authority. The NDMO's supremacy clause and the Authority's placement within the Prime Minister's Office create a framework where "the Bangladeshi State [becomes] the most consequential data controller in practice".

A 2026 academic study situated these concerns within a broader postcolonial-governance framework, arguing that Bangladesh's data protection framework must be read alongside a surrounding "surveillance stack" of telecommunications and cybersecurity statutes that continue to govern state access to communications data largely outside the reach of the new data protection.

Dismislab's 2026 investigation into the sale of voter-list data, and The Daily Star's contemporaneous synthesis of the Shwapno breach, the 2023 NID exposure, and the absence of an individual notification duty, collectively argue that " data protection law is only as strong as the institution enforcing it," and that a regulator housed within the Prime Minister's Office and legally bound to comply with government directions on national-security or public-order grounds "is not a data protection authority. It is a complaints desk" (Manab 2026).

Businesses have expressed concern about the compliance burden imposed by the Act, particularly the requirement to appoint Chief Data Officers for significant data-fiduciaries, conduct data audits, and implement security measures. However, the removal of broad data-localisation requirements (Faiaz 2026) and of imprisonment as a sanction for company officials in the February 2026 amendment was welcomed by industry groups such as the Computer & Communications Industry Association as a pragmatic adjustment, even as they continued to flag remaining provisions, including cross-border transfer restrictions and the pace of implementation as warranting further reform.

8. Recommendations

The most critical recommendation emerging from scholarly and civil society analysis is the need to entrench the Authority's independence in statute. This should include appointment by Parliament with cross-party consent, fixed terms for commissioners, protected budgets, and transparent rule-making that cannot be vetoed by the executive. Section 49's blanket direction power should be narrowed so that it cannot be invoked to shield government ministries or agencies from investigation of their own data practices. The Authority should be empowered to enforce rules fairly against both private entities and state agencies, as modelled on the GDPR's independent supervisory authority requirement.

The Act should be amended to impose a freestanding duty on data-fiduciaries to notify affected data-subjects directly, and within a defined period, whenever a breach is likely to result in a material risk to their rights, not merely to notify the Authority. The Shwapno case demonstrates that regulator-only notification leaves affected individuals uninformed and unable to protect themselves for months at a time.

The Act should be amended to include explicit general-purpose duties of purpose-limitation and data-minimization binding on state processing. These principles should apply to government agencies as firmly as they apply to private controllers, ensuring that data collection is limited to what is necessary and used only for specified purposes, a particularly urgent priority given the scale of consolidation contemplated by the Unified Digital Identity system and NRDEX.

Government exemptions, including those under section 24, should be narrowed to comply with the principles of legality, necessity, and proportionality. Exemptions should be supported by judicial approval, clearly defined purposes, independent audit mechanisms, and regular public transparency reports. Broad categories such as "public interest" or "public order" should be more clearly defined to prevent abuse.

The Act should clarify enforcement processes for data-subject rights, including clear pathways to complain, statutory deadlines for decisions, meaningful compensation, and collective actions for systemic abuse such as the NID and voter-list leaks. Given the demonstrated pattern of state-linked breaches, affected citizens should have a private right of action independent of the Authority's own enforcement priorities.

Given the documented vulnerabilities in the NID database and the still-incomplete integration underlying systems such as NEIR, further expansion of the Unified Digital Identity layer should be conditioned on independent security audits, mandatory encryption and access-logging standards, and demonstrated remediation of the vulnerabilities that produced the 2023 and 2025–2026 breaches, rather than proceeding on the current administrative-efficiency timeline alone.

Despite the Act's transition from ordinance to statute, the foundational nature of data protection legislation warrants robust ongoing parliamentary deliberation. While ordinances are constitutionally valid, they are, in Hossain's phrase, "simply not constitutionally deliberative." Implementing rules issued under the Act's numerous rule-making powers should undergo thorough parliamentary scrutiny and public consultation before adoption to ensure they adequately protect citizens' rights.

Bangladesh should continue to align its framework with international standards to secure adequacy decisions from the European Commission and facilitate cross-border data flows, which matter directly to its IT-enabled services export sector. This requires

strengthening regulatory independence, clarifying definitions, implementing data-protection-by-design provisions, and ensuring robust enforcement mechanisms reaching both private and state actors alike.

9. Conclusion

The Personal Data Protection Act of Bangladesh, 2026, represents a significant step toward establishing a comprehensive data protection regime in a country undergoing rapid digital transformation. The Act establishes key principles, confers rights on data-subjects, imposes obligations on data-fiduciaries, and creates an institutional framework for enforcement. However, significant gaps remain between the text of the law and its practical implementation enhanced by a sequence of large-scale breaches involving both government-held National Identity data and private-sector customer databases, and by the absence, at the time of writing, of any legal requirement that affected citizens be told directly when their data has been compromised. The Act's greatest strength is also its greatest vulnerability. By recognizing personal data as belonging to the data-subject, the Act signals a fundamental shift from treating citizens as passive data sources to rights holders. Yet the institutional framework established to protect these rights, a regulator seated within the Prime Minister's Office, legally bound to follow government direction on national-security or public-order grounds, and structurally inseparable from the government it regulates raises serious questions about whether the Act will protect citizens from state surveillance or facilitate it. As Bangladesh navigates the complexities of digital governance, it faces a fundamental choice. It can treat the Personal Data Protection Act as the culmination of its digital governance journey, accepting a framework in which the state retains ultimate control over personal data even as it formally recognizes that data as belonging to the individual. Alternatively, it can view the Act as the beginning of an ongoing process, a chance to craft, through public debate, democratic deliberation, and the hard evidence supplied by incidents such as the 2023 NID exposure, the Shwapno breach, and the 2026 voter-list sale, a data regime that protects citizens not only from corporations but from overreach of the state itself. The success of Bangladesh's data protection framework will depend not only on the text of the law but on how effectively it is implemented, how seriously organizations, public and private alike safeguard personal information, how well citizens understand and exercise their privacy rights, and whether the institutional framework can constrain powerful institutions, including the state, when they violate these rights. Bangladesh must move beyond legislation and build a culture in which personal data is treated with the same care and respect as any other asset, and in which the entities most capable of large-scale harm are not, by institutional design, the hardest to hold to account.

References

Al Rohan, Md. Rahim. 2025. Constitutional Legitimacy in Crisis: Interim Governance and Executive Ordinances in Bangladesh. https://next-lms.sgp1.digitaloceanspaces.com/pdf/O0zGLcsOeoMX9y6uBcpdyPbXY4x6qNx0.pdf

Aziz, Shafqat. 2026. Personal Data Protection Ordinance: A Law That Protects You from Everyone except the State. *The Business Standard*. https://www.tbsnews.net/thoughts/personal-data-protection-ordinance-law-protects-you-everyone-except-state-1416106

Faiaz Zarif. 2026. Data Frontiers : Where Does Bangladesh Fit in the Global Privacy Debate? *The Daily Star*. https://www.thedailystar.net/news/data-frontiers-where-does-bangladesh-fit-the-global-privacy-debate-4085556

Giurgiu, Andra, and Tine A. Larsen. 2016. Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency? European Data Protection Law Review (EDPL) 2. https://doi.org/10.21552/EDPL/2016/3/9

Halder, Sukanta. 2026. Shwapno's Database Hacked; 40 Lakh Customers' Details at Risk. *The Daily Star*. https://www.thedailystar.net/business/news/shwapnos-database-hacked-40-lakh-customers-details-risk-4137566

Haq, Md Zahurul, and Zainal Amin Bin Ayub et al. 2025. GDPR and Bangladesh's Data Privacy Laws: A Comprehensive Analysis. *International Journal of Public Law and Policy* 11: 192–209. https://doi.org/10.1504/IJPLAP.2025.145300

Hasan, Md. Nymul. 2023. The Digital Security Act 2018 & Freedom of Expression. *EWU Institutional Repository*. http://103.133.167.11:8080/handle/123456789/3924

Manab, Arafat Meem. 2026. Bangladesh Personal new Data Protection Law to Protect your Data. *The Daily Star*. https://asianews.network/why-bangladeshs-new-data-protection-law-may-fail-to-protect-your-data/

Rahman, Tasnuva. 2022. The Impact on Freedom of Expression in the Age of Digital Security Act, 2018 of Bangladesh. http://103.133.167.11:8080/handle/123456789/3626

Rashid Mamun. 2025. Do Our New Data Protection and Governance Ordinances Align with Growth Ambitions? *The Business Standard*. https://www.tbsnews.net/thoughts/do-our-new-data-protection-and-governance-ordinances-align-growth-ambitions-1302666

Riaduzzaman, Md. 2024. Constitutional Right to Privacy and Data Protection in Bangladesh: A Living Originalist Interpretation. *University of Dhaka*. https://share.google/IOTiD8JG49gqoQq8J

Zafarullah, Habib and Sabrina Nughat. 2026. Regulatory Control and Self-Censorship in Social Media: Stifling Freedom of Expression in Bangladesh. *Journal of Asian and African Studies*. https://doi.org/10.1177/00219096261437744