

Accord CHAMBERS

INSIGHTS

LEGAL & REGULATORY UPDATES, ANALYSIS AND COMMENTARY

A New Era of Data Governance: Adapting to the Personal Data Protection Act 2026

By Adiba Tarannum

The enactment of Bangladesh's Personal Data Protection Act 2026 ("**PDPA**") fundamentally dictates how organizations must govern data, imposing strict compliance obligations on entities processing personal information. The legislation casts a deliberately wide net with an extra-territorial application, ensuring comprehensive oversight regardless of the breaching entity's nationality or location. Under the purview of the PDPA, "Personal Data" means any information relating to an individual, such as name, parents' names, identification number, mobile number, financial data, location data or any other similar online identifier; or any physical, physiological, genetic, biometric, psychological, financial data of an individual, or any such element that helps to identify an individual as determined by regulations. In addition to this, Financial Data, Genetic Data, Biometric Data and Sensitive Personal Data are also all defined terms under the purview of the PDPA.

Personal Data Breach under the PDPA includes a breach of security of personal data resulting in unauthorized access to, or unlawful transfer, disclosure, alteration of, or loss of, any personal data processed, or in the absence of the necessary equipment for proper processing and storage, resulting in the occurrence of accidents, destruction, loss, or intrusion. Where such a breach is likely to cause significant harm to the data subject *i.e.* to whom personal data relates, the PDPA obliges the data

fiduciary *i.e.* the one who processes personal data, to notify the authority in the prescribed form and timeframe; a duty that arises independently of any complaint by the affected individual.

The cornerstone of the PDPA is a rigid consent architecture built on core principles of fairness, reasonableness, and purpose. Section 16 of the PDPA gives effect to such principles by restricting the disclosure of personal data, without the data subject's consent, for any purpose other than that for which the data was originally collected. For instance, where personal data is collected for an administrative purpose, such as issuing individual invitation letters, its subsequent disclosure for a different purpose, would be subject to the strict consent requirement under the PDPA. This sits alongside Section 15 of the PDPA, which requires a data fiduciary to proactively inform data subjects, before any significant processing activity, of the categories of data collected, its purpose and the risk of harm involved. The law also mandates that consent itself must be free, specific, unambiguous and easily revocable. Furthermore, Section 5(3) permits processing without explicit consent only under specifically narrow exceptions, such as contractual necessity, defense of legal rights, protection of vital interests, or voluntary publication by the data subject.

The PDPA reserves heightened protection for a defined category of Sensitive Personal Data, including genetic data, biometric data, data concerning ethnicity or community, political or religious belief, trade union membership, health data, sexual orientation, and data relating to the commission or alleged commission of an offence. Processing any of these categories requires satisfying the further conditions over and above the general consent framework, such as explicit consent, contractual necessity, or performance of a legal duty.

In parallel, the PDPA confers a defined set of rights on every data subject, which Section 10(4) of the PDPA declares to be universal, inherent, non-waivable and which shall not be cancelled or restricted by contract or notice. These include the right of access to data held by a fiduciary along with its purpose, recipients and retention period under Section 11; the right to correction, completion or updating of inaccurate or outdated data under Section 12; and the right to withdraw consent, object to processing, and seek erasure under Section 13, subject to grounds on which a fiduciary may decline such a request, such as an existing legal obligation or archival necessity.

Failing to secure personal data under the PDPA triggers severe financial and operational repercussions. Section 32 of the PDPA outlines that non-compliance with data subject rights constitutes a direct violation, while further provisions create a separate track of liability for failure to maintain the security standards prescribed under the PDPA. The authority may impose administrative penalties of twenty-five lakh taka on data fiduciaries, scaling up to fifty lakh taka for significant data fiduciaries, with compounded fines possible for repeated violations. Entities that qualify as a significant data fiduciary as defined under Section 2(5) of the PDPA, determined by factors including but not limited to the volume of data processed and the risk to data subjects' rights, must also appoint a Chief Data Officer under Section 23 of the PDPA, who acts as the point of contact for data subjects and is responsible for the timely redress of complaints. Any administrative penalty under the PDPA remains appealable to the Tribunal

constituted under Section 68 of the Information and Communication Technology Act 2006, within thirty days of the date of the order imposing such penalty.

Taken together, the PDPA marks a decisive shift away from a self-regulatory approach to data governance in Bangladesh. Thus, organizations that collect, store or transfer personal data, whether as data fiduciaries or processors, must proactively update its consent processes, document its grounds for using such data, and implement robust security measures to ensure compliance with the law.

How can we assist?

Successfully navigating the Personal Data Protection Act, 2026 requires strict regulatory compliance. Accord Chambers provides comprehensive legal support to advise on matters such as consent processes for data usage, the robust security measures required to prevent severe financial and operational repercussions and also on the legal remedies for unauthorized disclosures or breaches. For any strategic assistance in ensuring compliance with the law, please feel free to reach us any time.

For any query, feel free to contact us: assistance@accordchambers.com.

This publication is the property of Accord Chambers and may not be distributed without expressly attributing it to the author and publisher. Accord Chambers fully reserves the rights of disclosure, publication and/or distribution of the contents of this publication. This is not a piece of legal advice.

For any query or legal advice on this topic, feel free to contact us: assistance@accordchambers.com