April 2026

CCIA Views on Bangladesh's Personal Data Protection Ordinance

On November 6, 2025, the President of Bangladesh enacted the **Personal Data Protection Ordinance, 2025** (PDPO), establishing a legal framework for data ownership, privacy, and security.[1] The PDPO was subsequently amended in February 2026,[2] with a revised text published in March 2026 that remains under consideration for Parliamentary approval. The March 2026 revision addresses several earlier concerns, notably removing data localization mandates and criminal liability for company officials, but retains provisions that warrant further amendment. As Bangladesh advances the revised PDPO, CCIA recommends targeted amendments to the articles addressed below to align the law with industry concerns and Bangladesh's commitments under the February 2026 US-Bangladesh Agreement on Reciprocal Trade.[3]

Specific comments on the March 2026 PDPO are as follows.

Compelled Cloud Relocation or Revocation Authority

Article 29(7) authorizes the Authority to order any data fiduciary or its processor to reconfigure, relocate, or cease using cloud infrastructure, domestic or foreign, within 60 days upon finding evidence of activities it determines constitute a breach of personal data and a threat to national interest or public security.

The provision's broad and loosely defined trigger conditions, encompassing factors as vague as "commercial variant" or "any other aspect" of cloud infrastructure, do not offer an evidentiary threshold or proportionality requirement, making compliance difficult. The 60-day relocation window is operationally unrealistic for enterprises with integrated cloud architectures, creating significant exposure to service disruption and data loss. More broadly, the absence of independent judicial review or a defined appeals mechanism, combined with the scope of the Authority's discretion, introduces substantial uncertainty.

To address these concerns, Article 29(7) should be amended to constrain the government's ability to compel relocation or termination of foreign cloud services to cases of gross negligence, subject to due process.

---

[1] *Personal Data Protection Ordinance, 2025* [Bangladesh] Ordinance No. 61. (2025). http://bdlaws.minlaw.gov.bd/act-1574.html.an

[2] *Personal Data Protection (Amendment) Ordinance* [Bangladesh] Ordinance No. 23. (2026). http://bdlaws.minlaw.gov.bd/act-details-1616.html.

[3] *Agreement Between the United States of America and the People's Republic of Bangladesh on Reciprocal Trade*. (2026). https://ustr.gov/sites/default/files/files/Press/Releases/2026/U.S.%20BGD%20Agreement%20on%20Reciprocal%20Trade%20Final%2009FEB2026%20LETTER.pdf.

March 2026 PDPO	Proposed Edits
Article 29(7): In the case of transfer, storage, processing, etc. of any personal data to any domestic or foreign cloud computer, if the Authority finds evidence of or identifies activities causing a breach of the personal data of a citizen of Bangladesh constituting a threat to the national interest or public security of Bangladesh regarding the geographical location, commercial variant, or any other aspect of the cloud used by a data fiduciary themselves or their processor, it may issue orders to such institution to reconfigure, relocate the cloud infrastructure, or revoke the use of such cloud within 60 (sixty) days.	*Article 29(7): In the case of transfer, storage, processing, etc. of any personal data to any domestic or foreign cloud computer, if the Authority finds evidence ~~of or identifies activities~~* ***gross negligence*** *causing a breach of the personal data of a citizen of Bangladesh constituting a threat to the national interest or public security of Bangladesh ~~regarding the geographical location, commercial variant, or any other aspect of the cloud used by a data fiduciary themselves or their processor~~, it may* ***direct such a data fiduciary or processor*** *~~issue orders to such institution~~ to reconfigure, relocate the cloud infrastructure, or revoke the use of such cloud****,*** *~~within 60 (sixty) days~~* ***provided that: (i) the data fiduciary or processor has been served written notice specifying the grounds for the proposed order and afforded a reasonable opportunity to be heard; (ii) the Authority has determined that less restrictive remedial measures are inadequate to address the identified breach; and (iii) any such order shall be subject to independent judicial review before taking effect****.*

Personal Liability for Company Officials in Data Violations

Article 36 allows the Authority to impose administrative fines on individual company officials, including board members, the managing director, other management office-bearers, or employees involved in daily operations, who are personally implicated in a violation of a data subject's rights.

Article 36 exposes a broad class of individuals to personal administrative liability, meaning board members, officers, and employees could face fines based solely on their organizational involvement with a violation rather than any culpable conduct or knowledge. This creates significant governance risk, as directors and senior officers with fiduciary oversight responsibilities but no direct operational role in a given data processing activity may nonetheless face personal liability. The provision also lacks proportionality safeguards, offering no framework for distinguishing degrees of individual culpability or calibrating fines accordingly, which compounds exposure for lower-level employees carrying out routine operational tasks.

To address these concerns, Article 36 should be amended to limit personal liability for directors, officers, and employees to cases of willful misconduct.

March 2026 PDPO	Proposed Edits
Article 36: If any data subject under this Act raises a complaint of violation of their rights against any company, the Authority may impose an administrative fine in accordance with the provisions against any member of the board of directors, managing director, or any office-bearer associated with the management of the company or any employee engaged in executing the daily activities of the company who is involved with the said violation.	*Article 36: If any data subject under this Act raises a complaint of violation of their rights against any company, the Authority may impose an administrative fine in accordance with the provisions against any member of the board of directors, managing director, or any office-bearer associated with the management of the company or any employee engaged in executing the daily activities of the company who is involved with the said violation* ***and who is found to have engaged in willful misconduct directly contributing to the said violation****.*

Cross-Border Transfer Conditions and Bilateral Cooperation Framework

Articles 29(4) and 30 establish complementary frameworks for cross-border data transfers: Article 29(4) restricts outbound transfers to jurisdictions with “suitable” infrastructure and technology for data protection, while Article 30 authorizes the Government to negotiate bilateral or multilateral arrangements with foreign governments or international bodies to govern cross-border data exchange and cooperation under the Act.

Article 29(4)'s conditioning of transfers on "suitable technology and equipment prescribed by regulations" provides no criteria for evaluating the adequacy of foreign jurisdictions' data protection infrastructure, and offers no mechanism for mutual recognition or equivalency determinations that would allow transfers to well-regulated markets to proceed with legal certainty. This gap is particularly consequential given the US-Bangladesh Agreement on Reciprocal Trade, which obligates Bangladesh to recognize Global CBPR and PRP certifications as valid transfer mechanisms under its domestic legal framework, yet Article 29(4) contains no implementing machinery for that commitment. Article 30, while permissive in authorizing bilateral and multilateral arrangements, establishes no timeline, criteria, or procedural framework for concluding such agreements.

Articles 29(4) and 30 should be amended, or supplemented with appropriate administrative measures, to establish a transparent adequacy determination framework with defined criteria for evaluating foreign jurisdictions' data protection infrastructure, explicit recognition of internationally accepted certification mechanisms, including the Global CBPR and PRP Systems as qualifying transfer pathways, and a mandatory timeline and procedural framework for concluding bilateral and multilateral arrangements.

March 2026 PDPO	Proposed Edits
Article 29(4): Legally transferable personal data may only be transferred to those locations or countries where suitable technology and equipment for preserving personal data prescribed by regulations exist.	*Article 29(4): Legally transferable personal data may only be transferred to those locations or countries where suitable technology and equipment for preserving personal data prescribed by regulations exist* ***or where the Authority has issued an adequacy determination confirming that the recipient jurisdiction maintains a level of data protection equivalent to that required under this Act, including through recognition of internationally accepted certification frameworks such as the Global Cross-Border Privacy Rules System and Global Privacy Recognition for Processors System as valid transfer mechanisms****.*
Article 30: The Government may connect with any other country or multilateral organization or consortium or forum for the purpose of fulfilling the objectives of this Act, bilateral, multilateral, and cross-border personal data exchange, and other cooperation.	*Article 30: The Government may connect with any other country or multilateral organization or consortium or forum for the purpose of fulfilling the objectives of this Act, bilateral, multilateral, and cross-border personal data exchange, and other cooperation****, and shall establish by regulation a procedural framework and timeline for initiating, concluding, and giving domestic legal effect to such arrangements, including mechanisms for recognizing equivalent data protection standards maintained by partner jurisdictions****.*

Data Classification Tiers and Cross-Border Transfer Conditions

Articles 29(1) and 29(3) establish the classification and transfer conditions for personal data: Article 29(1) empowers the Government to classify personal data into four tiers (public, internal, confidential, and restricted) based on schedule-defined characteristics, while Article 29(3) permits cross-border transfer of classified data only where at least one of three conditions is met: the data subject's consent, a contractual relationship involving goods or services, or activities tied to the data subject's interests such as business, education, or immigration.

Article 29(3) conditions all cross-border transfers on consent or contract-based grounds, with no provision for transfers based on legitimate interests, legal obligations, or compatibility with the original processing purpose, departing from global frameworks such as the APEC CBPR

system that recognize a broader range of lawful transfer bases.[4] This creates significant friction for routine operations where individual consent is impractical, such as intragroup transfers or fraud prevention, which may involve foreign processing.

Furthermore, this Article does not specify the compliance requirements for several key terms. Article 29(1)'s delegation of classification criteria entirely to an undefined schedule leaves the practical consequences of "confidential" and "restricted" designations opaque. Likewise, the interaction between data tiers and transfer conditions is wholly unspecified.

Article 29(3) should be amended to recognize additional lawful transfer bases beyond consent, including transfers compatible with the original processing purpose, necessary for contract performance, or required by legal obligation, consistent with globally recognized frameworks. Where consent is retained, it should not serve as the default mechanism for routine commercial transfers consistent with the original purpose of processing. Article 29(1) should codify more specific classification criteria in the Act or implementing regulations, with the "confidential" and "restricted" categories defined narrowly to avoid overbroad transfer restrictions.

March 2026 PDPO	Proposed Edits
Article 29(1): Considering the characteristics described in the schedule, the Government may classify personal data as follows, namely:- (a) Public or open personal data; (b) Internal personal data; (c) Confidential personal data; (d) Restricted personal data.	*Article 29(1): Considering the characteristics described in the schedule**, as further defined in implementing regulations which shall narrowly construe the categories of confidential and restricted personal data**, the Government may classify personal data as follows, namely:- (a) Public or open personal data; (b) Internal personal data; (c) Confidential personal data; (d) Restricted personal data.*
Article 29(3): Any personal data classified under sub-section (1) may be transferred abroad subject to fulfilling the conditions of this section, if it involves- (a) consent of the concerned data subject; or (b) matters of exchanging goods or services through any contract to which the data subject is a party; or (c) matters related to business, education, departure, immigration, etc. associated with the data subject's interests with their consent.	*Article 29(3): Any personal data classified under sub-section (1) may be transferred abroad subject to fulfilling the conditions of this section, if it involves- (a) consent of the concerned data subject; or (b) matters of exchanging goods or services through any contract to which the data subject is a party; or (c) matters related to business, education, departure, immigration, etc. associated with the data subject's interests with their consent**; or (d) transfers necessary for compliance with a legal obligation applicable to the data*

[4] *APEC Cross-Border Privacy Rules System: Policies, Rules, and Guidelines*. (2019). https://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf

	fiduciary; or (e) transfers compatible with the purpose for which the personal data was originally collected, having regard to the nature of the data, the consequences of the transfer, and the existence of appropriate safeguards.

Taxation Authority Over Commercialization of Personal Data

Article 29(5) authorizes the Government to levy fees or charges on institutions based on annual profits derived from the use of Bangladeshi citizens' personal data, with rates to be set by official Gazette notification.

This provision's broad framing, applying to any institution deriving commercial profit from personal data use, would capture a wide range of digital business models and could function in practice as a *de facto* levy on data-driven commercial activity. This raises a direct concern under the US-Bangladesh Agreement on Reciprocal Trade, which prohibits Bangladesh from imposing digital services taxes or similar taxes that discriminate against US companies in law or in fact: depending on how fees are structured in implementing regulations, a charge calibrated to profits derived from personal data use could constitute a "similar tax" under Article 3.1, particularly if its incidence falls disproportionately on large technology and data-intensive firms, many of which are US-headquartered.

Article 29(5) should be deleted in its entirety.

March 2026 PDPO	Proposed Edits
Article 29(5): The Government may, by notification in the official Gazette, determine fees or charges on the annual business or commercial profit of any institution arising from the use of personal data of Bangladeshi citizens.	~~*Article 29(5): The Government may, by notification in the official Gazette, determine fees or charges on the annual business or commercial profit of any institution arising from the use of personal data of Bangladeshi citizens.*~~