UNBOWED
The Daily Star
CELEBRATING
35 YEARS
JOURNALISM WITHOUT FEAR OR FAVOUR

KEEPING UP WITH
THE WORLD

SEGMENT 3
ANNIVERSARY SUPPLEMENTS 2026
DHAKA TUESDAY JANUARY 20, 2026
MAGH 6, 1432 BS
35

Data frontiers: where does Bangladesh fit in the global privacy debate?

The EU-US Data Privacy Framework is one example, with the official programme overview explaining that the adequacy decision enables transfers of EU personal data to participating organisations consistent with EU law. China has tightened oversight while still building pathways for compliant exports. India's DPDP Rules are framed as enabling responsible data use within a new governance structure.

Bangladesh's challenge is that it is trying to land this balance while its Globally, that balancing act has become the norm. The EU promotes strict rights protections while still permitting cross-border transfers through adequacy decisions and legal mechanisms. The United States has focused on enabling data flows for commerce while negotiating safeguards in specific contexts. The EU-US Data Privacy Framework is one example, with the official programme overview explaining that the adequacy decision enables transfers of EU personal data to participating organisations consistent with EU law. China has tightened oversight while still building pathways for compliant exports. India's DPDP Rules are framed as enabling responsible data use within a new governance structure.

Bangladesh's challenge is that it is trying to land this balance while its own regulatory capacity is still developing, and while public trust in digital governance remains fragile.

SO WHERE DOES BANGLADESH FIT?
Bangladesh is unlikely to become a full replica of the European rights-first model overnight, because the GDPR depends on strong supervisory authorities, mature court oversight, and deep institutional capacity. It is also unlikely to adopt the looser US approach, because Bangladesh's political and security context pushes strongly towards state discretion, and because citizens are demanding clearer protections as data becomes embedded in everyday services.

Instead, Bangladesh is positioning itself as a hybrid, a country seeking legitimacy through rights language and modern governance architecture, while retaining broad levers for state intervention. The question is whether those levers will be narrowed and supervised enough to win credibility internationally and domestically.

To fit into the global privacy debate in a way that strengthens Bangladesh's future economy, three tests matter.

The first is independence and enforcement. A privacy regime that cannot constrain powerful institutions will not build trust, and it will not reassure foreign partners. The concern raised by TIB and Article 19 about consultation and executive influence points to a basic requirement: a regulator that can enforce rules fairly, whether the violator is a small business, a multinational platform or a state agency.

The second is cross-border realism. Bangladesh wants to scale digital exports, attract investment, and support startups that serve global markets. That cannot be done with rules that treat every data transfer as inherently suspicious or that force costly duplication without a clear security rationale. The amendments reported in January 2026 suggest policymakers recognise this, but the final shape of the regime will determine whether Bangladesh is seen as open for business or trapped in uncertainty.

The third is the AI connection. Privacy is no longer only about preventing leaks or stopping spam. It is about whether automated systems can profile people, deny them opportunities, or nudge them politically without transparency. Bangladesh's ordinance, as described by BSS, includes the idea that citizens can restrict automated decisions made using their data, which aligns with a wider global shift towards algorithmic accountability. The challenge will be turning that right into something meaningful: requiring explanations, creating appeal mechanisms, and ensuring that both public and private AI systems are auditable when they have serious impacts.

Bangladesh's data frontier is therefore not only about catching up. It is about choosing a global identity. Does Bangladesh want to be seen as a country where personal data is protected in practice, where rules are stable enough for innovation, and where state powers are constrained by law? Or does it want to prioritise rapid control over data flows even if that risks trust, investment and the legitimacy of the framework itself?

The most realistic answer is that Bangladesh will continue to negotiate between these poles, because that is what almost every country is now doing. But there is still a difference between negotiation and drift. The coming year, with amendments already on the table, will show whether Bangladesh can turn its new laws into a credible social contract rather than a contested instrument of power.

SUMMARY

1. Data has become economic and political power, and privacy rules now shape trade, trust and AI adoption.

2. Bangladesh is moving fast, with a new Personal Data Protection Ordinance and National Data Governance Ordinance entering the debate.

3. The global privacy landscape is splitting into models, from Europe's rights-based approach to sovereignty-focused regimes with tighter state control.

4. Bangladesh's biggest fault line is cross-border data, balancing sovereignty and security against investment, cloud dependence and digital exports.

5. The credibility test will be enforcement and oversight: rights on paper must translate into protections in practice, including limits on state discretion.

IMAGE: **TOBIAS TULLIUS/ UNSPLASH**