

# DATA FRONTIERS

## Where does Bangladesh fit in the global privacy debate?

ZARIF FAIAZ

Zarif Faiaz is a journalist at The Daily Star and a tech policy fellow at Tech Global Institute.

Data has become the raw material of modern power. It fuels artificial intelligence, guides advertising, shapes credit decisions, and underpins everything from ride hailing to national identity systems. Yet the same data can also be weaponised, mishandled, leaked or quietly traded. Around the world, governments are trying to answer a question that sounds technical but is deeply political: who gets to collect data, who gets to use it, and what rights do ordinary people have when their lives are reduced to records, profiles and predictions?

Bangladesh is stepping into this debate at a moment of unusual intensity. In late 2025, the country moved towards its first comprehensive privacy framework with a Personal Data Protection Ordinance and a National Data Governance Ordinance, both gazetted in November. And in early January 2026, the government approved amendments that, largely removed broad data localisation requirements for technology companies and dropped jail terms for violations by tech firms.

That combination tells us almost everything about where Bangladesh sits in the global privacy argument. It is trying to build a modern data regime quickly, under pressure from citizens who want protections and businesses that need workable rules. It is also doing so in a world where privacy law is increasingly tied to trade, geopolitics, national security and the question of whether data should flow freely across borders or be kept at home.

The result is a genuine crossroads: Bangladesh can become a credible,



IMAGE: FLYD/ UNSPLASH

rights-based player in the global data economy, or it can drift into a model where "protection" is promised but "control" becomes the lived experience.

#### A WORLD SPLITTING INTO PRIVACY BLOCS

The global privacy debate is no longer about whether privacy matters. Most governments now accept, at least rhetorically, that it does. The argument is about the model.

Europe has tried to set the standard

with the General Data Protection Regulation, which builds privacy around rights and obligations. The European Commission presents the GDPR as technology-neutral and applicable across sectors, focusing on how data is processed rather than what tools are used. Its principles, including lawfulness, fairness, transparency and purpose limitation, have become a reference point for regulators worldwide.

The United States, by contrast, has

tended to rely on a patchwork of sector rules and state laws, with enforcement and consumer remedies often varying depending on where someone lives. California's consumer privacy regime has become one of the most influential US examples, with the state attorney general's office setting out rights such as opting out of sale or sharing and requesting corrections to inaccurate data. In early January 2026, California launched a government-run tool designed to help residents request

deletion of personal information held by data brokers, underlining how the US debate is increasingly focused on the commercial trade in personal data.

China's approach sits in a different category, shaped by a strong emphasis on sovereignty and state oversight, especially for cross-border transfers. The direction of travel has been towards more structured compliance pathways for exporting personal information, including certification regimes and, in some cases, assessments and contractual tools. Reuters reported in October 2025 that Chinese regulators announced new rules for certifying cross-border transfers of personal data, scheduled to take effect on January 1, 2026.

Then there are the bridge models, including India's, which combine individual rights with a strong state role and a growing desire to manage strategic data without cutting off global commerce. In November 2025, India notified its Digital Personal Data Protection Rules, presented by the government as operationalising the Digital Personal Data Protection Act and creating a citizen-centric privacy framework.

Beneath these headline models sits the real battleground: cross-border data. Modern economies run on global cloud infrastructure, international payments, outsourced processing, and multinational platforms. But governments also worry about surveillance, foreign access, and dependence on overseas infrastructure. Data localisation measures have

SEE PAGE 34

**US-BANGLA AIRLINES**

**WINGS BEYOND BORDERS**

DUBAI | SHARJAH | ABU DHABI | JEDDAH  
RIYADH | BANGKOK | KUALA LUMPUR | SINGAPORE  
MALDIVES | MUSCAT | DOHA | KOLKATA  
CHENNAI | GUANGZHOU



MOBILE APP  
DOWNLOAD NOW  
Available on the  
App Store  
GET IT ON  
Google Play

Serving Bangladesh & Beyond

**Renata PLC at the forefront**

Present in  
**65**  
Countries

**7**  
International  
Accreditations

**80+**  
Bioequivalent  
Products

**2**  
International  
Subsidiaries

**RENATA PLC**