

**Asia Internet Coalition (AIC) Industry Submission to Ministry of Information
Technology and Telecommunication (MoITT) on Pakistan Draft Data Protection Bill
2023**

29 June 2023

Honourable Mr. Syed Amin Ul Haque
Federal Minister for Information Technology and Telecommunication
Ministry of Information Technology and Telecommunication (MoITT)
7th Floor, Kohsar Block, Pak Secretariat,
Islamabad, Pakistan

On behalf of the Asia Internet Coalition (AIC) and its members, we are respectfully submitting our recommendations on Draft Personal Data Protection Bill 2023, which was published by the Ministry of Information Technology and Telecommunication (MoITT), dated 19 May 2023.

There are four key issues with the latest Draft Personal Data Protection Bill 2023, released in May 2023 (the Bill): (1) the Bill mandates that critical personal data must only be processed in Pakistan (the Data Localisation requirement) and the definition of critical personal data is broadly defined such that it may negatively impact private companies; (2) the Bill introduces a requirement to share sensitive personal data with the Government; (3) the age of a child under the Bill should be thirteen, not eighteen; and (4) there should be a set maximum fine payable for breaches of the Bill.

We find that the Draft Bill still does not address a majority of industry's substantive concerns such as stringent limitations on cross-border data flows and mandatory data localization, overbroad and vague definitions of key terms such as sensitive personal data and critical personal data, and globally divergent data subject rights, as well as far-reaching powers of the Commission. These provisions fall short of international standards for data protection (such as GDPR) and will adversely impact Pakistani consumers and businesses. In its current form, the Bill will have a negative impact on the ability of foreign internet companies to trade with and operate in Pakistan, hindering the country's economic recovery and deterring foreign investment. Local Pakistani companies may lose access to cost-efficient global cloud services making them less competitive as they incur substantial costs to operate and maintain servers.

The protection of personal data is an important component of any privacy framework, and we appreciate the opportunity to provide feedback on the Draft Bill. AIC and its members have worked closely with governments around the world in relation to the development of national personal data protection policies and legislation. In doing so, we have witnessed first-hand the potential for such policies and legislation to effectively protect the privacy interests of citizens without hindering innovation and technological advancement. We recognize the on-going efforts of the Government of Pakistan and the Ministry of Information Technology and Telecommunications ("MOITT") in further fine-tuning the draft legislation, but we continue to have concerns, particularly on cross-border transfer of "critical" and "sensitive" personal data.

On this note, the AIC wishes to request for an industry meeting to better understand the views and priorities stemming from the Bill. We also propose to discuss potential

areas of collaboration as well as opportunities for consultation that can further assist the Government's review of the Personal Data Protection Bill 2023. As such, we welcome a video conference meeting with you or your team at a date and time of your convenience.

Importantly, we trust that these comments and recommendations are useful and look forward to working closely with the Government of Pakistan, other industry players, consumer groups and all other relevant stakeholders to help deliver an effective and robust privacy framework for Pakistan based on international good practices.

Thank you for your time and consideration.

Sincerely,



Jeff Paine
Managing Director
Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

1. Data localisation and cross-border data flows

Recommendation: The Data Localisation (DL) requirement should be removed or the definition of critical personal data should be limited to government-held data.

Rationale: Pakistan's economy will benefit from unimpeded cross-border data flows (CBDFs). By contrast, data localisation will stifle the economy and chill foreign investment. Data localisation will also heighten cyber security risks.

1.1. Pakistan's economy will benefit from unimpeded CBDFs

- Cross-border data flows are essential to growing Pakistan's economy and ensuring Pakistani businesses remain competitive in the global economy. Embracing cross-border data flows will: promote productivity, innovation, and efficiency; lower costs for consumers and businesses; **lower barriers to international trade and investment**; increase access to global products and services; and ensure Pakistani businesses can service consumers at home and abroad.
- Economic modeling and independent analyses illustrate the value of embracing CBDFs:

- Increased CBDFs grew global GDP by 10% (\$2.8 trillion) in 2014, with emerging digital markets standing to benefit from 50% GDP growth by embracing CBDFs. These potential gains have grown significantly as the amount of data that transits global networks has since multiplied exponentially [McKinsey 2016].

1.2. Data localization will have a chilling effect on foreign direct investment

- Data localisation requirements **reduce foreign direct investment** and restrict the availability of services to local consumers. Multinationals looking to invest may forgo Pakistan in favor of markets with less burdensome costs of entry. In fact, the US National Trade Estimate identified restrictions on data flows and data localisation requirements as a leading impediment to foreign direct investment by US companies [USTR 2020].
 - The World Economic Forum's recent report on data flows warns that data localisation requirements chill e-commerce, destabilize supply chains, stifle the development of domestic talent, increase compliance costs for SMEs, and cause "local companies and consumers [to] lose access to cloud computing capabilities and other advanced foreign information technologies, pay higher prices and become uncompetitive in global markets" [WEF 2020].

1.3. Evidence suggests that, in China, the government's restrictive approach to data flows and data localization requirements have caused economic harm and limited growth potential. For example, in Oct 2021, LinkedIn announced that it will close its service in China due to the more "challenging operating environment." following China's passage of the Personal Information Protection Law.(PIPL) [NYT 2021].

1.4. DL heightens privacy and security risks

- Requiring that data be exclusively stored in one location puts users' data at greater risk by centralizing data storage and creating a "honey-pot" of data that is vulnerable to unauthorized access and cyber attacks. By contrast, distributed networks are built to be resilient and to allow for redundancy in the event of a network failure and ensure business continuity for organizations. Global companies, and particularly technology-dependent companies, rely on cloud storage solutions for their data management because it allows for an affordable and scalable way to deploy the latest technology and tools across the network to make it secure. This is not possible with data localization.

2. Mandatory Government access to sensitive personal data

Recommendation: The requirement that data controllers must share data with the Government at the request of the Commission should be removed.

Rationale: An unfettered requirement to provide personal data to the Government is inconsistent with the Bill's stated aim of protecting individuals' personal data and guaranteeing their right to privacy (a fundamental right under Article 14 of the Constitution of Pakistan). While we recognise that there are legitimate contexts in which a Government may require access to information held by an organization, legislating mechanisms for Government access should not be done through a privacy law.

Some global privacy laws (such as the GDPR) permit data transfers to third party countries that have an adequate privacy law in place. If Pakistan adopts the PDP Bill with a right for the Government to request unfettered access to individuals' sensitive personal information, this is likely to lead to the conclusion under global privacy law norms that the PDP Bill is *not* adequate and therefore is likely to hamper data transfers into Pakistan.

The Bill as currently drafted will also place foreign companies in an impossible position of being caught between conflicting global laws. Regardless of the location where data is stored, U.S. communications providers are subject to U.S. law, which generally restricts their ability to disclose information about users and prohibits them from disclosing the contents of electronic communications, subject to certain limited exceptions. The location of where data is stored would not resolve this conflict of law.

Instead, **signing a Mutual Legal Assistance Treaty (MLAT) with the United States provides a diplomatic channel for foreign governments to request user data from U.S. based companies without creating a conflict of law.** Many countries with significant Muslim populations have entered into MLATs with the United States, including Egypt, Malaysia, and Turkey. Therefore, to facilitate an improved process and response rate, it is recommended that Pakistan enter into an MLAT with the United States.

Similarly, it is **recommended that Pakistan accede to and ratify the Budapest Convention.** Several countries with significant Muslim populations have either acceded to or ratified the Budapest Convention, including Morocco, Nigeria, Senegal, and Tunisia. Finally, Pakistan should establish a single point of contact for government-to-government requests. This would ensure that requesting agencies are familiar with U.S. legal and constitutional requirements and have reviewed requests to ensure they are compatible with U.S. standards.

3. Children's Personal Data

Recommendation: The Bill should define a "child" as being a person who has not attained the age of thirteen years.

Rationale: The age of consent for accessing online services has to be distinguished from the age of majority which is usually applied in the context of voting, serving in the military, criminal liability, getting married, or similar circumstances, where very different policy considerations are taken into account.

Thirteen has been adopted by several key jurisdictions as an appropriate threshold. Some examples include:

- **US' Children's Online Privacy Protection Act:** restrictions apply to collecting personal data of under 13 year olds.

- **Singapore's PDPC:** advisory guidelines state that a minor who is at least 13 years of age can provide consent on his or her own behalf.
- **EU GDPR:** member states may set the age at which children are able to consent to data processing at an age between 13 and 16. Several countries have adopted 13 as the relevant age of consent, including Belgium, Denmark, Estonia, Finland, Latvia, Malta, Norway, Portugal and Sweden.
- **UK GDPR:** has also adopted 13 as the age at which a person may provide consent.

While parental approval makes sense for children below the age of 13, young adults between the ages of 13 and 18 years should be permitted and empowered to make decisions about their data. Otherwise you risk locking teens out of the digital economy, and overwhelming parents with requests for consent.

Setting the age at 13 would give teens better access to: (a) health information, which are vital at their stage of development; (b) educational resources and tools, which they may use in and out of school; (c) resources that would inform them of relevant and current issues, raising their civic and political understanding and consciousness; and (d) ready support resources and platforms, that are already available online.

4. Fines

Recommendation: There should be a specified maximum fine for breaches of the PDP Bill and the Commission should not have discretion to impose fines above this maximum.

Rationale: Currently the Bill states that the maximum fine under the Bill will be 1% of a company's gross revenue in Pakistan or \$200,000 USD (whichever is higher) "or as may be assessed by the Commission."

This language could be interpreted as providing the Commission with discretion to impose a fine of any amount. It is critical that maximum penalties are clearly articulated in the Bill to provide certainty and transparency to industry. The Commission should not have discretion to impose any fine it sees fit without legislative guardrails.
