Asia Internet Coalition (AIC) Industry Submission on Pakistan Draft National Artificial Intelligence Policy

---

10 July 2023

To
Honourable Mr. Syed Amin Ul Haque
Federal Minister for Information Technology and Telecommunication
Ministry of Information Technology and Telecommunication (MoITT)

Cc:
Mr. Syed Junaid Imam, Member (IT), Ministry of Information Technology & Telecommunication (MoITT)

On behalf of the Asia Internet Coalition (AIC) and its members, we are respectfully submitting our recommendations on the Draft National Artificial Intelligence (AI) Policy, which was published by the Ministry of Information Technology and Telecommunication (MoITT). The Artificial Intelligence (AI) Policy is a pivotal milestone for transforming Pakistan into a knowledge-based economy as it spells out a national strategy to establish an ecosystem necessary for AI adoption by harnessing an agile framework for addressing different aspects of unique user journeys encompassing different market horizontals and industry verticals by ensuring responsible use of AI. While we welcome the National AI Policy, support its goals, and appreciate its balanced approach to innovation and ethics, we are nevertheless concerned by its dependencies and conflicts with other laws, particularly the Draft Personal Data Protection Bill (PDPB). This situation is further complicated by the need for the National AI Policy to harmoniously coexist with the Pakistan Cloud First Policy (PCFP) and the Digital Pakistan Policy initiatives. Unlike the PDPB, the PCFP allows cross-border flows of data in certain situations.

As responsible stakeholders, we appreciate the ability to participate in this discussion and the opportunity to provide inputs into the policy-making process in Pakistan. **As such, please find attached to this letter detailed comments and recommendations, which we would like to respectfully request the Ministry to consider. Importantly, we would also like to request for a virtual meeting with you and your team to further offer our inputs and go through the submission on industry best practices.**

Should you have any questions or need clarification on any of the recommendations, please do not hesitate to contact me directly at Secretariat@aicasia.org or +65 8739 1490. Thank you for your time and consideration and we look forward to hearing from you.

Sincerely,

Jeff Paine
Managing Director, Asia Internet Coalition (AIC)

Detailed Comments and Recommendations

Key comments on drafting the National Artificial Intelligence Policy

1. Overlap and intervention with existing regulations

According to the Draft Policy, it "coherently interlaces" with both the Cloud First Policy (CFP) and the Personal Data Protection Bill (PDPB). The PDPB may conflict with the CFP since it is still in the draft stage and because of the limitations it lays on specific categories of personal data. Section 29(4) of the current PDPB draft of the PDPB imposes additional constraints on automated decision-making without human involvement. The ideas to implement and promote AI are incompatible with this restriction according to the Policy.

The PDPB contains data localization mandates including local storage requirements for "critical personal data" (CPD) and external transfer restrictions for personal data and potentially sensitive personal data. If the National AI Policy is to "coherently interlace" with the PDPB, as claimed on page 5 of the draft policy, the data localization mandates in the PDPB will apply to data used by Pakistani developers to build AI technologies. Such restrictions would splinter the global pool of data available to AI developers, and, if other countries adopted similar policies, Pakistani businesses would find it difficult to build AI technologies because their potential training data would be restricted to data stored in-country. It would also prevent foreign businesses from training their AI models on data from Pakistan, which would result in AI tools that don't speak to Pakistan's cultural context.

This situation is further complicated by the need for the National AI Policy to harmoniously coexist with the Pakistan Cloud First Policy (PCFP) and the Digital Pakistan Policy initiatives. Unlike the PDPB, the PCFP allows cross-border flows of data in certain situations. If the National AI Policy is subject to the PDPB's data localization mandates, Pakistani AI developers might find their ability to access data in a foreign cloud similarly impeded by corresponding measures in the cloud host jurisdiction.

The situation is more complex in the case of CPD because it is undefined. Since sectoral regulators have prospective powers to notify certain kinds of data as CPD on an ongoing basis, the PDPB's local storage requirements may be triggered at any time. Such an unpredictable and fluid policy situation disincentivises businesses from innovation and would make it difficult for Pakistani businesses to build AI tools.

- Recommendation: We strongly advise against tying the Policy to the proposed PDPB.

2. Requirements for localised hosting and use of international AI platforms

The National/Provincial IT Boards will act "as controllers and processors of public data while assisting the concerned department(s) in secure and effective service provisioning,"

according to the policy, which mandates that copies of "public data must be hosted on the National Telecom Corporation (NTC) cloud infrastructure nationwide." The need that a copy of any publicly accessible data hosted in the cloud be kept locally with NTC would appear to be mandated if the inference that the same regulation should apply under this Policy is true. But in another place in the Policy, it says that "CoE-AI shall provide the necessary infrastructure and partnerships with international AI platforms for secure and monitored public data processing by providing ARD with critical insights." This would imply that public data may be processed via global platforms so long as the Artificial Intelligence Directorate is "provided with essential insights".

Moreover, AI relies on and is closely connected to automated decision making without human intervention. While the National AI Policy seeks to encourage AI, the PDPB does exactly the opposite by placing restrictions on the ability of businesses to deploy automated decision making technologies. These tensions are best resolved by amending the PDPB to (i) completely remove data localization mandates, (ii) remove all restrictions on automated decision making that would impact AI development, and (iii) make it interact harmoniously with the National AI Policy.

Recommendation:

- We request clarification on the Policy's requirements for local hosting and use of "international AI platforms".
- We also recommend, particularly given the limitations of local computational resources noted in the Policy itself, that the policy not require the use of local cloud infrastructure. Cloud infrastructure is at its strongest, most secure, and most economical when it is not subjected to forced localisation. Although data localisation may offer governments the perception of control over sensitive data, it involves a necessary trade-off against resilience to external threats and risks.

3. Importance of engaging the industry for a meaningful policy development

In accordance with the policy, "the CoE-AI shall put particular emphasis on indigenous research innovation with respect to generative AI and, in this regard, engage with the OpenAI platform and allocate a special quota for start-ups/R&D institutions/companies working in this space."

Recommendation:

- We recommend that the Policy not single out or otherwise privilege a single company but rather leave such engagement open to industry, especially with regard to potential future public-private collaborations, given the dynamic developments in this sector.

4. The Policy should align with international best practices and ensure interoperability

According to the Policy, "the local/international private sector entities offering AI-led tools and services for data controlling and processing shall be provided with necessary

instructions/regulations concerning data orchestration by the AI Directorate functioning under NCPDP." This seems to establish a mandate for the adoption of legal frameworks, giving the Commission established under the PDPB the authority to give directives to CSPs providing AI-based services. This could be difficult because these guidelines/requirements might force CSPs to adhere to standards specific to Pakistan, which might not be compatible with global best practices.

Recommendation:

- We recommend the implementation of standard methods for AI governance and regulation, as well as a common language, based on the OECD's work.

Recommendations for responsible AI policy

1. Enhancing global security while preventing malicious actors from exploiting this technology

AI has significant effects on the stability and security of the world. AI has the ability to both identify and track modified and false information. Through sophisticated security operations and threat intelligence, it can also power a new generation of cyber defences. The problem is to maximise the potential benefits of AI while putting the right safeguards in place to stop the malicious use of AI and working together to deal with bad actors. Governments, academia, public society, and industry all need to have a deeper understanding of the dangers posed by strong AI systems as well as how to make more complex AI systems consistent with human values.

a. *Safeguarding international security interests in advanced technologies:*

- Create the best "next-generation" trade control regulations for certain AI-powered software programs that are considered security threats, as well as for certain organizations that fund AI-related research and development in ways that could jeopardize international security.
- To facilitate information exchange between governments and the commercial sector about AI security vulnerabilities, strengthen international collaborations and public-private forums.
- Investigate techniques for spotting and thwarting disinformation efforts, such as meddling in elections, when nefarious individuals create or manipulate media using generative AI (deepfakes/cheapfakes).
- Establish joint AI research centres to advance AI research and adoption amongst like-minded countries.

b. *Streamline government adoption of AI technologies:*

- Reform government acquisition policies to take advantage of and foster world-leading AI. This includes investments in the most-needed, future-facing capabilities and expanding the aperture of companies that can deliver innovation.

- Examine institutional and bureaucratic barriers that prevent governments from breaking down data silos and adopt best-in-class data governance to harness the full power of AI.
- Capitalise on data insights through human-machine teaming, building nimble teams with the skills to quickly build/adapt/leverage AI systems which no longer require computer science degrees so that these teams can — in hours or days — address problems like responding to an active threat event.

2. Unlocking opportunity by maximising AI's economic promise

Economies that embrace AI will see significant growth, outcompeting rivals that are slower on the uptake. Adopting AI in existing industries represents an opportunity to move up the value chain, producing more complex and valuable products and services. AI also promises to help increase productivity despite growing demographic challenges. Governments, the private sector, educational institutions, and other stakeholders will need to work on joint and separate strategies to enable businesses, workers, and communities to capitalise on AI's benefits. Governments should increase investments in fundamental AI research, studies of the evolving future of work to help with labour transitions, and programs to ensure strong pipelines of STEM talent. Governments and industry need to deepen their efforts to upskill workers and support businesses meeting changing demands and new ways of producing goods and services.

2.1. *Invest in innovation, awareness building and human capital competitiveness:*

- Grow investments in fundamental AI research through national labs and universities, and research foundations.
- Complementing the development of centres of government expertise, expand AI research in sectoral agencies to address key societal challenges, for example agencies overseeing environmental protection, public health, and disaster prevention and relief.
- Maintain and expand technology transfer frameworks to help universities both obtain government funding and progress new AI applications, pursuing AI innovations produced with federal funding and partnering with private tech companies to develop advanced AI applications.

2.2. *Promote an enabling legal framework for AI innovation*

a. Advance regulation and policies that help support AI innovation and responsible deployment.

- Adopt or maintain proportional privacy laws that protect personal information and enable trusted data flows across national borders, and establish a legal framework for AI models' incidental use of such data on the open web for training purposes.
- Establish competition safe harbours for open public-private and cross-industry collaboration on AI safety research.

- Adopt or maintain copyright systems that enable appropriate and fair use of copyrighted content, while giving publishers and content creators choice and control over reproduction of their works.

b. Clarify potential liability for misuse/abuse of both general-purpose and specialised AI systems (including open-source systems, as appropriate) by various participants – researchers and authors, creators, implementers, and end users.

2.3. *Prepare the workforce for an AI driven job transition and promote opportunities to broadly share AI's benefits:*

a. Create a strong pipeline of local STEM and computer science talent.
b. Invest in alternative pathways for non-college-degree holders.
c. Invest in community infrastructure to enhance economic mobility and inclusion (broadband, transportation, regional innovation hubs, affordable housing, transportation),improving labour market mobility.

3. Promoting responsibility while reducing risks of abuse

Businesses and consumers will be unwilling to deploy AI systems without trust and confidence, which will limit their ability to reap the benefits of AI. AI is already assisting in the fight against global issues like disease and climate change, and it has the potential to be a strong force for progress and fairness. However, if not created and implemented properly, AI systems may also increase societal problems. It will take a multi-stakeholder approach to governance to meet these difficulties. While standards and widely used best practices will be more effective in addressing some of these issues, others will call for legislation, such as mandating high-risk AI systems to go through expert risk assessments customized to particular applications. In collaboration with communities and civil society, fundamental research will be needed to better understand potential consequences and mitigations for other concerns.

3.1. Pursue proportionate, risk-based regulation that enables responsible development and application of next-generation technologies

a. Encourage regulators to take a proportionate, risk-based approach to "high-risk" AI
   - Define "high-risk AI systems" as those intended for use in applications that pose a material risk of significantly harming people or property or imperilling access to essential services.
   - Establish proportionate penalties for non-compliant deployments, with reasonable opportunities to cure issues given the novel nature of the technologies.

b. Require organisations that deploy high-risk AI systems to:
   - Provide documentation describing how the system is intended to be used, known inappropriate uses, known risks, and

recommendations for independent deployers and users to manage risk.

- Undergo risk assessments by independent internal or external experts.
- Disclose the results of capacity and risk assessments, with protection for trade secrets and controlled technologies as appropriate.
- Align documentation, risk assessment, and management practices with relevant standards, frameworks, and industry best practices as those standards develop.

c. Require regulatory agencies to issue detailed guidance on how existing authorities (e.g., those designed to combat discrimination or protect safety) apply to the use of AI.

- Direct sectoral regulators to update existing oversight and enforcement regimes to apply to AI systems, including on how existing authorities apply to the use of AI, and how to demonstrate compliance of an AI system with existing regulations using international consensus multi-stakeholder standards like the ISO 42001 series.
- Instruct regulatory agencies to issue regular reports identifying capacity gaps that make it difficult both for covered entities to comply with regulations and for regulators to conduct effective oversight.