National Artificial Intelligence Policy 2025

Analysis by Digital Rights Foundation

August, 2025

https://digitalrightsfoundation.pk/

For more details, contact info@digitalrightsfoundation.pk

About

The Digital Rights Foundation ("**DRF**") is a women-led, not-for-profit organization that has been working since 2013 to advance digital rights and online freedoms across South Asia and the broader Global Majority. DRF advocates for inclusive, rights-respecting digital spaces by driving policy change through strategic engagement with relevant stakeholders. DRF's work focuses on making digital platforms and emerging technologies more equitable, accessible, and accountable. At the grassroots level, we empower individuals, particularly women, marginalized communities, and human rights defenders, with the tools and knowledge to navigate the Internet safely and assert their rights online.

Introduction:

Pakistan's bold leap into the future with its newly passed National Artificial Intelligence Policy 2025 (**"AI Policy 2025"**) promises transformative growth and innovation. At DRF, we have taken a close look at this landmark policy that aims to train one million AI professionals by 2030, fuel AI startups through Innovation and Venture Funds, and foster thousands of civic and local AI projects. While the vision is ambitious and inspiring, serious questions linger around transparency, ethical safeguards, and protecting marginalized communities from discrimination. In this analysis, we highlight the critical gaps that must be addressed to ensure Pakistan's AI journey respects human rights and fosters trust for all. This submission builds on previous detailed analysis of the Draft National Artificial Intelligence AI Policy 2023, particularly concerning international best practices and structural concerns.

Consultation Process:

In 2023, DRF developed a detailed analysis of the National Artificial Intelligence Policy, an analysis[1] that remains relevant in light of the newly released National AI Policy 2025. As an organization committed to inclusive, rights-respecting technology governance, DRF recognizes the transformative potential of Artificial Intelligence (AI) for Pakistan. With a young, digitally connected population and expanding technological infrastructure, the country is well-positioned to leverage AI for national development and social progress. We acknowledge that the Ministry of Information Technology and Telecommunication (**"MoITT"**), through the adoption of this AI Policy 2025, has taken

[1]Digital Rights Foundation, Feedback on the National Artificial Intelligence Policy (DRF, July 2023) https://digitalrightsfoundation.pk/wp-content/uploads/2023/07/Feedback-National-AI-Policy-DRF-July-2023.pdf

an important step toward articulating a vision for responsible and strategic AI adoption in Pakistan.

However, we remain deeply concerned that the process leading to the policy's adoption did not meet the standards of inclusivity, transparency, and public participation that should underpin a national initiative of this magnitude. While the policy refers to stakeholder consultations and international best practices, it fails to disclose key details, such as which stakeholders were consulted, the nature and number of consultations conducted, or how feedback was incorporated into the final draft. Critically, civil society, including organizations focused on human rights, digital freedoms, marginalized communities, and academic research, was excluded from the core consultation process. This exclusion is particularly troubling given the policy's stated aim to "fundamentally rethink AI adoption in the local context," a goal that cannot be achieved without input from a diverse cross-section of society.

The absence of inclusive consultation has resulted in a policy that, while ambitious in scope, lacks meaningful engagement with the unique socio-political challenges and human rights risks present in the Pakistani context. Although the policy acknowledges the need for interdisciplinary and multi-stakeholder risk assessments, especially concerning human rights, information integrity, and democratic governance, no such assessments appear to have been conducted.

Below is the detailed analysis of the AI Policy 2025, followed by a comparative assessment against leading global AI frameworks to identify gaps and provide recommendations for enhancement.

Objective

- The inclusion of the statement *"to preserve Pakistan's cultural identity by leveraging AI in context-sensitive ways that empower communities and promote local narratives"* in the objective raises concerns due to undefined terms like "cultural identity", "context-sensitive", and "local narratives". Such vague terms may allow broad interpretations, which could lead to censorship, and risk reinforcing interpretations that often silence voices challenging harmful norms of society. (Ethical Objectives (Ensuring Ethical and Responsible Use of AI) - Clause (d)

First Pillar: AI Innovation Ecosystem

- Although the formation of a National AI Fund Committee is proposed, its legal status, composition, decision-making process, and accountability measures remain undefined. This raises concerns about transparency, discretion, and public trust in the allocation of funds. To address this, the AI Policy 2025 should clearly outline its structure, powers, how its members will be appointed, its reporting mechanisms, and the remedies available in case of misappropriation of funds. (Clause 1.1(c))
- The AI Policy 2025 proposes a large-scale allocation of public funds through various initiatives (e.g., Innovation Fund, Venture Fund, and CoE-AI), but there is no mention of how project selection, fund disbursement, or procurement will be carried out in an accountable and transparent manner. It is recommended that the Policy provide safeguards by clear selection processes, incorporate transparent procedures, and ensure independent oversight to maintain public trust in the management of these funds. (Clause 1.2, 1.3. and 1.4) Furthermore, if AI tools or related infrastructure are procured from international companies or exporters, this information should be made public to ensure that no procurement

is carried out from entities known to be complicit in human rights violations, such as cyber intelligence firms producing spyware.

- The Policy does not define how intellectual property rights created through public funds will be owned or licensed, particularly those in collaborations with academia and startups. This could lead to disputes over ownership. The Policy should clarify intellectual property rights ownership in projects funded through the National AI Fund or CoEs and adopt a licensing model that balances public interest with incentives for innovators. (Clause 1.1, 1.3, and 1.4)
- The reference to funding AI solutions in the "national interest" lacks a clear definition, which may lead to arbitrary or politically motivated interpretations. This ambiguity may also result in biased fund allocation and undermine transparency. Defining "national interest" through clear, inclusive, and rights-based criteria is important to ensure fairness and accountability (Clause 1.3(a)).
- The AI Policy 2025 does not clarify how the Pakistani diaspora's involvement in AI development will be regulated, especially in terms of cross-border data flows, sensitive data security, or financial regulations related to taxes. (Clause 1.6)
- The proposal to create centralized, high-quality datasets for AI model training raises privacy violation concerns. Without clear definitions of data ownership, user consent, and anonymization protocols, such centralization risks violating privacy rights and enabling misuse. In a legal vacuum lacking strong data protection laws, this approach could undermine public trust and accountability. Any move toward centralization must be grounded in a clear, rights-based data governance framework. (Clause 1.5(b))

Second Pillar: Awareness and Readiness

- The Policy highlights the importance of protecting personal data and privacy in the use of AI, but does not refer to any legal mechanism or enforceable framework to uphold this right. At present, the current Personal Data Protection Bill draft ("**Data Protection Bill"**), which has not even passed yet, falls short of anticipating the unique privacy and security issues raised by AI and emerging technologies, including a lack of consideration of the privacy aspects of the datasets employed by, used to train and develop AI. (Second Pillar, first para)

Third Pillar: Secure AI Ecosystem

- The use of the term 'guidelines' about AI-based cybersecurity solutions raises concerns about their enforceability. If these guidelines are non-binding, they may fall short in ensuring accountability and compliance. (Clause 3.1(a))
- The deployment of AI-driven threat detection systems for real-time monitoring must be governed by a clear legal framework to ensure they do not allow unchecked surveillance. Without data protection laws, independent oversight, and clearly defined limitations, such systems risk infringing on individuals' right to privacy and enabling mass surveillance. (Clause 3.1(b))
- The Policy proposes AI-based cybersecurity protocols and threat detection systems; however, it does not reference any existing national structures that could serve as a legal foundation. This omission raises concerns about enforceability, scope, and overlapping institutional responsibilities. To avoid over-legislation, the Policy should align AI cybersecurity measures with existing regulatory bodies or upcoming legislation, such as the data protection bill. (Clause 3.1)

- The clause on transparency and human oversight rightly emphasises audits, public disclosure, and accountability in the use of AI, especially for high-impact systems. However, it lacks a binding legal framework to define key terms, such as "high risk," and outline enforcement pathways. For these safeguards to be effective, legal provisions must mandate third-party audits, establish redress mechanisms, and guarantee rights such as explanation and appeal in cases of harm or bias. Without such clarity, the clause risks being ineffective in practice. (Clause 3.2(a))
- To develop a comprehensive and rights-respecting national data security policy, it is essential to engage independent legal and technical experts with proven experience in data governance. The AI Policy 2025 should not only address security standards, auditing mechanisms, and training protocols, but also be grounded in globally recognized legal frameworks. In particular, inspiration should be drawn from the European Union's General Data Protection Regulation (GDPR), which provides robust guidelines on data minimization, privacy by design, breach notification, and accountability. (Clause 3.3)
- While the AI Policy 2025 emphasizes controlled data sharing and collaborative innovation, it lacks clear definitions of what constitutes "sensitive personal," "organizational," and "national" data. This definitional gap creates legal ambiguity and grants excessive discretion to authorities, undermining consistent enforcement of data protection standards and accountability mechanisms. A clearly defined threshold is essential to establish what is included and excluded under each category to safeguard against arbitrary interpretations. (Clause 3.6(b))
- The directive for the AI Directorate to provide regulatory guidelines to address disinformation, data privacy breaches, and fake news raises concerns. The terms "disinformation" and "fake news" remain legally ambiguous and, without precise

definitions, risk being misused. Additionally, there is potential overlap with existing or developing laws on data protection and cybersecurity, necessitating legal coherence and institutional coordination. Therefore, any regulatory role of the Directorate should be grounded in law, limited by well-defined scopes, and aligned with constitutional and other obligations. (Clause 3.7(a))

- The AI Policy 2025 promotes the use of regulatory sandboxes for AI deployment but does not describe their legal status, authority, or data protection safeguards during sandbox trials. There must be a dedicated legal framework for AI regulatory sandboxes, specifying how it will be governed, how participant liability is managed, and how ethical or legal violations during the trial phase will be handled. (Clause 3.8)

Fourth Pillar: Transformation and Evolution

- The Fourth Pillar, while ambitious in promoting AI adoption across sectors, lacks clarity on ethical safeguards and fails to include mandatory human rights and risk assessments. It overlooks protections against misuse in high-risk areas like policing, justice, and governance. There is no mention of public oversight mechanisms or grievance redressal for harmful AI applications. Additionally, the absence of AI-specific legal accountability and comprehensive data protection laws raises concerns. Alignment with international human rights and AI ethics frameworks is also missing, weakening safeguards for vulnerable groups. (Clause 4)
- While the Policy outlines ambitious timelines for sectoral AI integration and maturity assessments, it lacks a risk-tier classification system, a critical feature in international frameworks like the EU AI Act and UNESCO AI Ethics Recommendation. Without a structured risk-based approach, high-impact sectors such as justice, policing, and healthcare remain exposed to unchecked

algorithmic harm. The absence of stratified obligations based on risk levels weakens safeguards, legal accountability, and due process. Although it references "*international auditing and accountability standards,*" it omits explicit commitment to key frameworks such as the EU AI Act, OECD AI Principles, UNESCO AI Ethics Recommendation, and the Council of Europe AI Convention. (Clause 4)

- The inclusion of medical data in the AI Policy 2025's digitization efforts raises concerns due to a lack of safeguards. Medical data is among the sensitive types of personal information. If clear policies are not in place to define how this data is collected, categorized, accessed, and shared, with explicit user consent, there is a threat of privacy violations. This could lead to exploitation, i.e, by insurers, and may damage public trust in digital systems. The AI Policy 2025 must include defining strict protocols for data collection, categorization, access, and sharing, all based on informed user consent. (Clause 4 (b),(c))
- Despite referencing AI adoption in decision-making across ministries and the public and private sectors, the Policy omits any legal mechanisms for accountability or liability. There is no clarity on who bears responsibility when AI systems cause harm, make biased decisions, or violate rights. (Clause 4(d))
- The proposal to develop a Ranking Management System (RMS) and establish a government oversight body lacks specificity and depth. The oversight mechanism is limited to conducting a trust index survey, which falls short of ensuring genuine transparency and accountability. Crucially, the Policy does not address essential aspects such as algorithm explainability or mandate independent public audits. (Clause 4.1)

Fifth Pillar: AI Infrastructure

- The Policy focuses on centralized datasets and a national and provincial AI data repository, but it lacks a legal framework governing data collection, ownership, anonymization, access rights, and consent mechanisms. Without such safeguards, large-scale data centralization may violate individual privacy and constitutional rights. It is recommended to align it with the upcoming Data Protection Bill, detailing data usage rights, security obligations, cross-border flow rules, consent procedures, and accountability mechanisms. (Clause 5.2)
- The AI Policy 2025 proposes contributing 50 AI models annually to open platforms, but fails to clarify whether these models are subject to licensing or protected by copyright/patent law. There is a risk of unlicensed use or international IP disputes. It is recommended to establish a clear IP management framework for AI models developed using public funds, establishing licensing protocols, and measures to prevent misappropriation of Pakistani innovations. (Clause 5.4)
- While regulatory sandboxes are essential for experimentation, the AI Policy 2025 does not define the legal status and liability during testing. (Clause 5.5)

Sixth Pillar: International Partnerships and Collaborations

- The Policy promotes joint research and cross-border AI collaborations; however, without a data protection framework, such collaborations pose significant risks to Pakistani citizens' data, including potential misuse, surveillance, or breaches. This concern is particularly pertinent in projects involving sensitive datasets (biometric, health, financial data), which may be processed abroad. (Clauses 6.3 and 6.4)
- Collaborative AI research initiatives, especially those involving international

partners, raise issues around ownership, licensing, and commercialization of co-developed technologies. However, the Policy does not mention any intellectual property-related protocols to govern such collaborations. In the absence of such frameworks, there is a risk that Pakistan's contributions may not be protected and lead to ownership disputes over innovations. Therefore, the Policy should promote the development of standard IP-sharing protocols and model clauses to be used in international research agreements. Also, clarify commercialization rights and revenue sharing for co-developed AI technologies, and ensure recognition for local researchers and institutions. (Sections 6.1 and 6.3)

Policy Implementation:

- The statement that a "*structured implementation mechanism will be established*" is vague without specifying how this mechanism will be legally constituted. Without clear statutory backing or regulation, the mechanism may lack enforceable authority over federal and provincial bodies, limiting its effectiveness and creating jurisdictional ambiguities.
- While the mechanism aims to unify federal and provincial efforts, the AI Policy 2025 does not clarify how conflicts between federal and provincial jurisdictions will be resolved legally. Pakistan's constitutional framework grants significant autonomy to provinces, so effective coordination requires clear legal protocols to prevent jurisdictional disputes.
- The AI Policy 2025 highlights transparency and accountability but does not specify legal frameworks to enforce these principles. Without statutory mandates for public reporting, independent oversight, or mechanisms to address grievances, these commitments risk being merely aspirational.

- Promoting public and civil society participation is commendable, yet without legally mandated consultation procedures or mechanisms ensuring meaningful input, this may not translate into effective influence on policymaking. There is no mention of rights-based approaches to participation or legal safeguards for marginalized groups.
- The AI Policy 2025 refers to "*ethical oversight"* but lacks clear legal provisions to enforce ethical standards, monitor compliance, or impose sanctions for violations. This gap could allow unethical AI practices to persist without legal consequences.

AI Council:

- The AI Council is positioned as the apex body overseeing AI Policy 2025 implementation, but there is no indication of a legal or statutory basis establishing the Council's authority, powers, and governance. Without formal legal backing, such as an act, ordinance, or government notification with a clear mandate, the Council's decisions and directives may lack enforceability and be open to challenge.
- There is no clarity on how decisions will be made, whether by majority vote, consensus, or otherwise, and what the quorum requirements are. The absence of defined procedures can lead to ambiguity in governance, accountability, and the legitimacy of the Council's resolutions.
- Moreover, the Policy provides a list of members for the AI Council, including representatives from academia, industry, civil society, and key sectors like healthcare and agriculture. However, it fails to outline the specific process for appointing both governmental and non-governmental members. This lack of procedural clarity raises serious concerns regarding transparency, merit-based selection, and accountability.

- The Council is responsible for providing strategic direction and overseeing the AI Policy 2025 implementation process, but it does not empower it to enforce compliance, penalize violations, or conduct thorough human-rights impact assessments. Without enforcement mechanisms embedded in law, ethical guidelines risk being purely advisory and ineffective.

Policy Implementation Cell:

- There is no clarity on how the PIC will be formed, its internal hierarchy, member qualifications, tenure, or rules of procedure. This can lead to ambiguity in accountability and potential jurisdictional overlap with other bodies. AI Policy 2025 should outline how the PIC will be constituted, who appoints its members, what qualifications or expertise are required, and how representation from key stakeholders will be ensured
- The phrase "Administrative reporting to Member D&ET" is vague. The AI Policy 2025 should elaborate on the scope and timeline of reporting and the role of Member D&ET in decision-making or oversight.

AI Policy Action Matrix:

The short- and medium-term goals outlined in the AI Policy 2025 matrix appear overly ambitious and, in some cases, impractical. For example, pointer 1 sets targets that are unlikely to be met, particularly given that eight months of 2025 have already passed with little indication of progress. Such timelines suggest a lack of alignment between AI Policy 2025's ambition and ground realities, including institutional readiness, resource availability, and implementation capacity. When goals are set without realistic timelines or clear accountability mechanisms, they risk becoming symbolic rather than actionable.

This disconnect may ultimately hinder the credibility and effectiveness of the broader AI Policy 2025 framework.

Pakistan National AI Policy vs. Global AI Governance Frameworks

Risk-based regulation and AI Categorization

Pakistan's National AI policy lacks an explicit risk-based classification of AI systems. Unlike the EU's AI Act, which defines tiers of AI risk (unacceptable, high, limited, minimal) with corresponding obligations. The National AI policy does not categorize AI by risk level. This omission means that there are no clear prohibitions on the most harmful AI practices (e.g., social scoring or exploitative manipulation, which the EU AI Act bans under Article 5).[2] The OECD's AI principles also urge a systematic risk management approach throughout an AI system's lifecycle[3], but the National AI policy only offers general cautions about AI's challenges and risks and high-level ethical aims without a structured risk assessment framework.

Ethical Human Rights Safeguards

While Pakistan's AI Policy emphasizes "responsible and ethical" AI and even cites alignment with UNESCO's Recommendation on the Ethics of AI, it does not embed binding human-rights safeguards. Global frameworks place human rights at the core, UNESCO's Recommendation (2021) makes the protection of human rights and dignity its cornerstone, backed by principles like fairness, transparency, and human oversight.[4] The Council of Europe's (CoE) 2024 AI Framework Convention similarly obligates Parties to ensure AI systems are developed and used consistently with human rights,

[2] Regulatory Framework for Artificial Intelligence — AI Act and Risk-Based Classification (European Commission, accessed 2025)
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[3] OECD AI Principles (Organisation for Economic Co-operation and Development, 2019)
https://www.oecd.org/en/topics/sub-issues/ai-principles.html
[4] Recommendation on the Ethics of Artificial Intelligence (UNESCO, November 2021)
https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

democracy, and the rule of law and enshrines principles of equality/non-discrimination, human dignity, and accountability.[5] Pakistan's policy remains a non-binding strategy and lacks legal prohibitions against AI that infringes fundamental rights or explicit requirements to prevent discrimination and bias. There is no equivalent to the CoE Convention's mandate for non-discrimination and equality in AI or UNESCO's call for avoiding biases that harm vulnerable and marginalized groups.

Transparency, Explainability, and Auditability Requirements

The National AI Policy calls for transparency and accountability (e.g., human oversight for "high-risk" scenarios and a public register of public-sector AI systems). However, these provisions are broad and lack detailed mechanisms. Internationally, transparency is a core requirement; UNESCO's principles stress that transparency and explainability are "essential preconditions" for protecting rights.[6] The OECD AI Principles likewise demand that AI actors provide meaningful information about AI systems' logic, data, and outputs to enable understanding and challenge of decisions.[7] The EU AI Act imposes concrete transparency obligations, e.g., requiring users to be informed when they interact with an AI (for chatbots or deepfakes), and mandating documentation, traceability, and explainability for high-risk AI.[8] Pakistan's policy does not yet require such granular disclosure or independent audits for private-sector AI. Its proposed

[5] Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (Council of Europe, May 2024)
https://opiniojuris.org/2024/11/05/understanding-the-scope-of-the-council-of-europe-framework-convention-on-ai/

[6] Recommendation on the Ethics of Artificial Intelligence (UNESCO, November 2021)
https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence

[7] OECD AI Principles – Transparency and Explainability (Organisation for Economic Co-operation and Development, 2019)
https://www.oecd.org/en/topics/sub-issues/ai-principles.htm

[8] Limited Risk and Transparency Provisions in the EU AI Act (European Commission, accessed 2025)
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai

audits and penalties for non-compliance are positive, but without codified standards or an oversight authority, enforcement is uncertain.

Enforcement and Compliance Mechanisms

Pakistan's AI policy is a roadmap that lacks a firm enforcement architecture. It proposes an "AI Directorate" to guide AI adoption and hints at a legal framework with penalties for violations, but specific compliance mechanisms or oversight bodies are not yet established. In contrast, the EU AI Act creates a robust compliance regime; providers of high-risk AI must undergo conformity assessments, and each Member State will designate authorities for market surveillance and enforcement, coordinated by a European AI Office.[9] The Council of Europe's AI Convention likewise introduces an obligatory monitoring mechanism and requires Parties to adopt legislative measures to give effect to its provisions.[10] OECD and UNESCO both emphasize accountability, calling on governments to ensure appropriate oversight and remedies for AI harms.[11] [12]. Without a dedicated enforcement body or clear legal mandates, Pakistan's well-intentioned principles may not translate into practice.

[9] Governance and Implementation of the EU Artificial Intelligence Act (European Commission, accessed 2025)
https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
[10] The World's First Binding AI Treaty (Future of Privacy Forum, June 2024)
https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/
[11] Accountability Principle in OECD AI Principles (Organisation for Economic Co-operation and Development, 2019)
https://www.oecd.org/en/topics/sub-issues/ai-principles.html
[12] "Recommendation on the Ethics of Artificial Intelligence" – gender, sustainability, and global inclusion focus (UNESCO, November 2021)
https://www.unesco.de/assets/dokumente/Deutsche_UNESCO-Kommission/02_Publikationen/Publikation_UNESCO_Recommendation_on_the_Ethics_of_Artificial_Intelligence.pdf

Global Alignment and Cross-Border Data Governance

Pakistan's policy acknowledges the importance of global AI norms and seeks "alignment with global standards" through international partnerships. However, there is room for stronger integration with evolving international frameworks. The OECD AI Principles urge governments to co-operate across borders to promote interoperable governance frameworks and coherent standards for trustworthy AI.[13] The Council of Europe's Convention, open to non-European signatories, is explicitly designed to set a common baseline and advance interoperability in AI governance.[14] Moreover, cross-border data flows and AI supply chains mean Pakistan must consider data governance and privacy standards internationally (e.g., the EU's GDPR and upcoming global arrangements). Pakistan's AI Policy does not yet detail how it will handle cross-border issues like data sharing, AI ethics in international AI services, or recognition of other jurisdictions' certifications.

Environmental Realities and Pakistan's AI Ambitions

The fourth and fifth pillars of the AI policy emphasize climate change mitigation by committing to recognizing, protecting, and promoting environmental sustainability across the AI system lifecycle, several proposed infrastructure developments, such as:

- High-Performance Computing (HPC) resources
- National and sectoral data repositories
- AI Hubs and institutional infrastructure

[13] Shaping an Enabling and Agile AI Policy Environment (OECD, 2019/2024) https://www.oecd.org/en/topics/sub-issues/ai-principles.html

[14] Non-Discrimination, Privacy, and Personal Data Safeguards in the CoE AI Framework (Future of Privacy Forum, 2024) https://fpf.org/blog/the-worlds-first-binding-treaty-on-artificial-intelligence-human-rights-democracy-and-the-rule-of-law-regulation-of-ai-in-broad-strokes/

This could have significant adverse environmental impacts. In a country like Pakistan, which is already at the frontline of the global climate crisis, the energy-intensive nature of data centres, large-scale computing, and storage infrastructure raises serious concerns about increased carbon emissions, water consumption, and electronic waste.

Moreover, provisions in the draft Personal Data Protection Bill around data localization, requiring certain data to be stored within national borders, could further increase these environmental risks by accelerating the demand for domestic data centers without robust environmental assessments or sustainability safeguards

Recommendations:

1. AI model training data should be subject to regular evaluations to ensure that such modules do not contain unethical, biased, unfair, and discriminatory information. This evaluation be conducted by independent industry experts, and findings from reports should be made transparent and available to the public, including civil society.
2. The functions, composition, and scope of the AI Directorate must be made explicit and identifiable. Since it falls under the NCPDP, a regulatory body to be established under the proposed Data Protection bill, comprehensive provisions must be provided in the Data Protection Law to protect personal data and ensure consent against AI-based automated systems.
3. The AI Directorate's regulatory powers and legal standing must also be made explicit, including available mechanisms for compliance with the ethical use of AI. The use of vague phrases such as "Public Safety" or "Disinformation" must be properly defined within the context of AI to

ensure that this body has limited space for discretion when it comes to arbitrarily flagging AI use.

4. AI systems must meet relevant transparency and data security requirements at each step of the supply chain before deployment. Producers of General AI models must be mandated to provide technical documentations that allow for an evaluation of their training and evaluation methods. For data security, it must be ensured that all deployers and producers act in accordance with a comprehensive data protection governance framework. Ensure algorithmic transparency and auditability as a matter of regulation. For significant AI systems, developers and deployers should be compelled to conduct Algorithmic Impact Assessments (akin to UNESCO's recommended ethical impact assessment) and to explain AI decisions affecting individuals. Pakistan can institute standards for AI record-keeping, third-party audits, and user notification when AI is in use, drawing on OECD guidance for traceability and accountability.
5. The AI Council and its appointed members should be kept independent from the state to ensure independent oversight of the state's policy. This body should not only be responsible for reviewing implementation but should also be authorised to conduct human-rights impact assessments against policy actions, allowing for transparency and accountability.
6. Context-specific use of AI must also remain sensitive to prevalent issues of marginalization and discriminatory profiling within the existing security infrastructure. AI use in law enforcement must be legally bound to establish an independent reporting mechanism for aggrieved individuals to seek legal redress.
7. When employing Generative AI (GenAI) specifically, in addition to copyright infringement and intellectual property law, special legal measures

should be made to ensure GenAI tools are not used against the privacy, dignity, and inviolability of man. Proper redress and recourse should also be made available to potential victims of GenAI.

8. While the policy mentions "High-risk" scenarios and the need for human oversight in these areas, it should also provide a comprehensive categorization of AI-use scenarios based on the type and extent of risks posed. A thorough identification and hierarchy of risks should be created in accordance with global standards, and dispersed among intended users allowing for a better understanding of ethical considerations in each sector where AI systems are deployed. Introducing a tiered, risk-based regulatory scheme for AI would align with global norms by focusing oversight on high-risk AI uses, mandating stricter requirements (e.g. pre-deployment impact assessments and certification) for systems that pose greater threats to safety or rights
9. The policy should contain clear and explicit descriptions of ethical vulnerabilities posed by the use of AI in "High-risk" scenarios. In addition to human oversight, further requirements must also be mandated in these critical sectors. This would include subjecting data sets to independent scrutiny, transparency of information with users, and regular evaluation reports to ensure regulatory compliance. The policy should consider legislation or regulations that ban AI applications violating human rights (e.g. social scoring or pervasive unlawful surveillance) and require AI developers to implement fairness measures.
10. Those AI systems identified as a clear threat to fundamental constitutional protections should be prohibited entirely. This would include any use of AI that involves the non-consensual targeting or processing of an individual's personal data or facial features for the purpose of surveillance and profiling.

Security imperatives must not be used to justify the deployment of these systems.

11. The AI Policy should explicitly mandate environmental impact assessments for all large-scale AI infrastructure projects and ensure sustainable benchmarks, such as energy efficiency and renewable energy use for e-waste management in AI development and deployment processes. Climate mitigation must also not be reduced to rhetoric and built into technical and governance frameworks for AI implementation.
12. Pakistan currently lacks a dedicated legal framework to govern the ethical and accountable use of AI. With no AI-specific laws or comprehensive data protection legislation in place, the misuse of AI, particularly in surveillance, deepfakes, and misinformation, poses serious risks. The absence of regulation leaves citizens vulnerable and undermines trust in AI systems. To address this, Pakistan should draft a National AI Law, modeled on the EU AI Act, which categorizes AI systems by risk and enforces stricter rules for high-risk applications. This can be further strengthened by enforceable data protection laws. Aligning with global standards, such as the UNESCO AI Ethics Recommendation and OECD AI Principles, will also enhance credibility and responsible adoption.
13. While policies often present an overarching vision, their successful legal enforceability and practical implementation depend on adoption by both provincial and federal authorities, which may unfold in practice.