How the DPG Standard and the Universal DPI Safeguards Framework are charting a safe and inclusive digital future

Jan 14, 2025 - New York

Authors:

- Amreen Taneja, Standards Lead, Digital Public Goods Alliance Secretariat,
- Francesco Stabilito, Project Manager, Office of Digital and Emerging Technologies
- Naveen Varshan Illavarasan, DPI Specialist, United Nations Development Programme

Digital systems are shaping how millions of people access essential services, from healthcare and education to financial inclusion. The stakes for getting these systems designed and implemented right from the outset have never been higher. This was evident during the recent Annual Members Meeting of the Digital Public Goods Alliance (DPGA) in Brazil, which highlighted how countries are increasingly leveraging open, interoperable building blocks to power their digital infrastructure.

Digital public goods (DPGs) sit at the heart of this digital transformation. When integrated into the Digital Public Infrastructure (DPI) approach, these technologies can unlock unprecedented opportunities for inclusive development. But opportunity alone is not enough. The technologies and systems being built must be inherently safe and inclusive, and uphold fundamental human rights from the ground up.

This article explores how recent updates to the DPG Standard and the Universal DPI Safeguards Framework are working in lockstep to nurture a cohesive ecosystem where technologies originating from the DPG community are designed to be safe and inclusive by default.

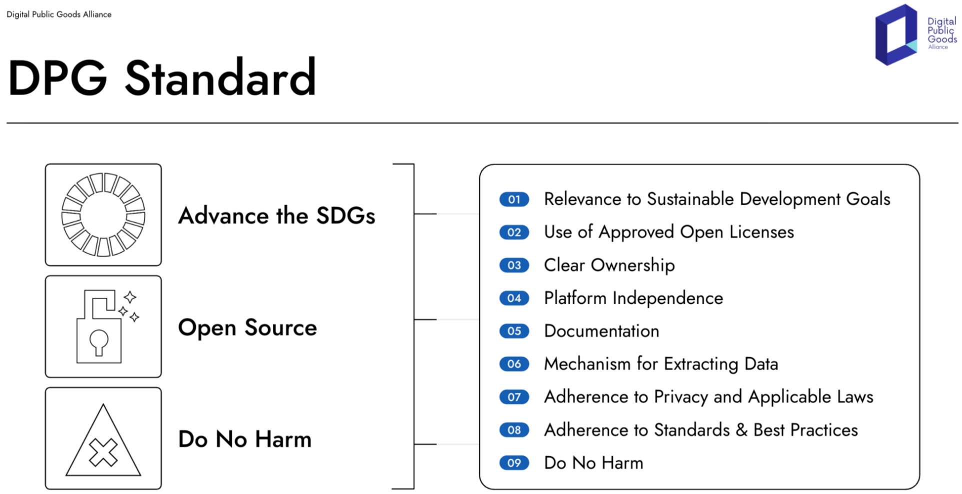
Digital Public Goods Alliance

DIGITAL PUBLIC INFRASTRUCTURE
Universal Safeguards

United Nations
Office for Digital and
Emerging Technologies

UN
DP

- The **DPG Standard** serves as the global benchmark for recognizing not only digital public goods, but technologies that can be safely adopted, adapted and scaled to advance sustainable development. To qualify as a DPG, a solution must be open source, contribute to advancing SDGs, and meet rigorous additional criteria outlined across nine indicators in areas such as licensing, documentation, privacy, security, and platform independence. Recent updates to the DPG Standard establish a stronger, more explicit safety-by-design foundation. The revised criteria clearly articulate expectations for privacy, security and responsible AI, ensuring these safeguards are integral to how DPGs are assessed. As a result, technologies recognized as DPGs demonstrate, from the outset, clear baseline commitments to user protection, data transparency and accountability.



Digital Public Goods Alliance

DPG Standard

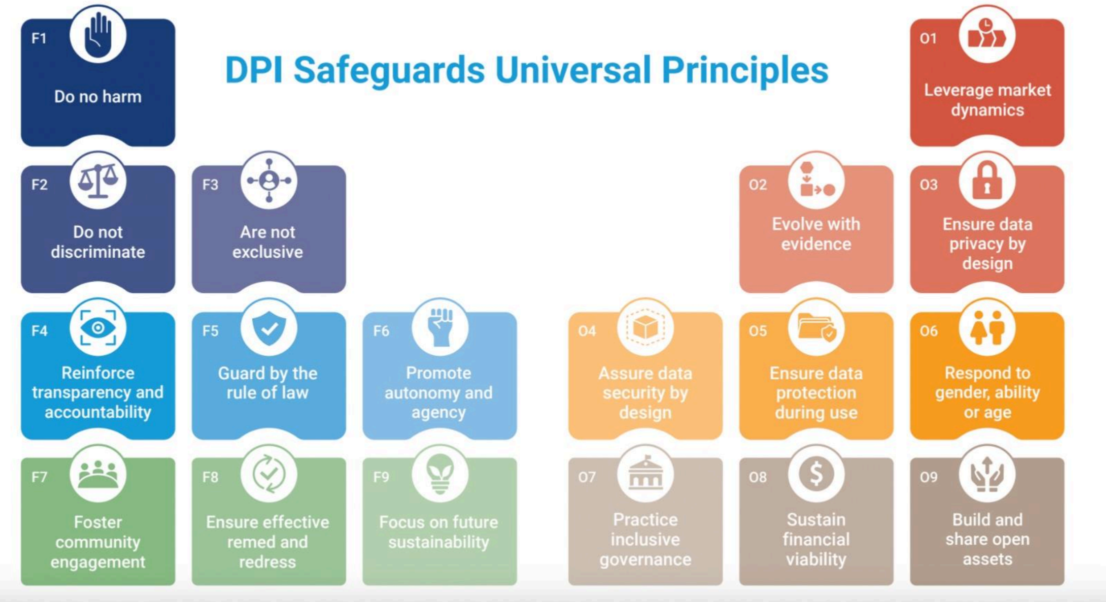
Advance the SDGs

Open Source

Do No Harm

01 Relevance to Sustainable Development Goals
02 Use of Approved Open Licenses
03 Clear Ownership
04 Platform Independence
05 Documentation
06 Mechanism for Extracting Data
07 Adherence to Privacy and Applicable Laws
08 Adherence to Standards & Best Practices
09 Do No Harm

- The **Universal DPI Safeguards Framework**, first released in 2024 by the DPI Safeguards initiative is the result of extensive global multi-stakeholder consultations involving 44 working group members, global convenings, consultations with international organizations, and local in-country engagement. The Framework was updated in 2025 following feedback from the ecosystem to ensure its continued relevance and practicality. It provides a comprehensive, rights-based approach for governing and ensuring responsible DPI implementation across the whole DPI lifecycle. The Framework is structured around 18 Foundational and Operational Principles that are designed to mitigate risks grouped into three core categories: safety, inclusion, and structural vulnerabilities.


DPI Safeguards Universal Principles
F1
Do no harm
F2
Do not discriminate
F3
Are not exclusive
F4
Reinforce transparency and accountability
F5
Guard by the rule of law
F6
Promote autonomy and agency
F7
Foster community engagement
F8
Ensure effective remed and redress
F9
Focus on future sustainability
01
Leverage market dynamics
02
Evolve with evidence
03
Ensure data privacy by design
04
Assure data security by design
05
Ensure data protection during use
06
Respond to gender, ability or age
07
Practice inclusive governance
08
Sustain financial viability
09
Build and share open assets

Two mutually reinforcing frameworks

The recent privacy and data security updates to the DPG Standard uphold a core principle: *key guardrails must be integrated at the design and development stage rather than being retrofitted during implementation.* With revisions to Indicators 7 (Adherence to Privacy and Applicable Laws) and 9A (Data Privacy & Security under the Do No Harm by design criteria), the DPG Standard now requires applicants seeking DPG accreditation to demonstrate concrete practices, such as data minimization (collecting only what is necessary), robust and informed user consent mechanisms, transparent disclosure of data use and access, well-defined data retention and deletion rules, and strong access controls and governance frameworks that prevent unauthorized access.

To complement the baseline requirements, the DPGA has introduced an Annex of Privacy & Data Security Best Practices. While these practices are not mandatory, they provide a structured pathway for more mature DPGs to strengthen their privacy and security apparatus in line with international frameworks. The Annex addresses multiple layers of practice, beginning with governance-level measures, such as the appointment of data protection officers, independent ethics review processes, and board-level transparency in key decisions. It also emphasizes documentation and compliance artifacts, including privacy and data protection impact assessments, data flow maps, data retention policies and training records.

On the technical side, the best practices recommend robust measures such as encryption during storage and in transit, role-based access controls, multi-factor authentication, continuous logging and auditing, and proactive vulnerability management. Furthermore, it encourages the adoption of privacy-enhancing technologies, including pseudonymization, differential privacy and federated learning, where relevant. These best practices provide a practical, actionable framework for DPGs to align with international privacy and security standards while supporting responsible and trustworthy deployment.

This comprehensive approach to privacy and security closely aligns with several principles of the Universal DPI Safeguards Framework:

1. **Do No Harm** is supported through data minimization and robust consent mechanisms, which proactively anticipate and mitigate risks of data misuse.
2. **Privacy and Data Protection by Design** is advanced by embedding protections at the design stage for all DPGs, ensuring that these measures are integrated from the outset rather than added later.
3. **Transparency and Accountability** are strengthened through requirements for clear disclosure of data use and access, enabling oversight and mechanisms for redress.

The Best Practices Annex further strengthens this alignment, as the newly introduced governance measures reflect the Universal DPI Safeguards Framework's emphasis on institutional responsibility and structured decision-making: the privacy impact assessments and data flow maps support risk management across the technology lifecycle; technical measures such as encryption, access controls and vulnerability management protect systems from misuse or attacks; and the adoption of privacy-enhancing technologies helps to foster innovation while upholding rights and ethical standards.

AI systems as DPGs

AI systems that aim to be recognized as DPGs must meet rigorous criteria to manage their unique risks. The DPG Standard now requires full transparency around AI training data, including the sources of the data, how the data was collected and processed and any known biases or limitations.

Developers also need to assess potential harms, especially for vulnerable or marginalized groups, and show evidence of testing across diverse populations and scenarios. AI systems must be understandable, with clear explanations of how decisions are made, tools to interpret outputs and disclosure of any limitations. Technical and usage guidelines should clarify appropriate and inappropriate uses, support safe deployment and highlight situations where the system may perform poorly. Finally, mechanisms for monitoring, user feedback and addressing issues must be in place, including processes for reviewing problems and updating models to reduce risks.

These AI-specific requirements align with the Universal DPI Safeguards Framework:

1. **Algorithmic accountability and transparency** ensure that when AI DPGs are incorporated into DPI in the future, they can be explainable, auditable and subject to meaningful oversight rather than operating as opaque 'black boxes'.
2. The **Do No Harm** principle is supported through bias assessments and fairness testing to mitigate discriminatory outcomes. Inclusiveness and equity are reinforced by requiring evaluation across diverse populations and documentation of risks to vulnerable groups.
3. **Purpose limitation** is embedded through usage guidelines that define appropriate applications and restrict potentially harmful use. Continuous monitoring, feedback and model updates reflect the lifecycle approach in the Universal DPI Safeguards Framework, recognizing that responsible AI deployment requires ongoing vigilance and adaptation as systems evolve and encounter new contexts.

Besides the recent updates, the DPG Standard aligns with the Universal DPI Safeguards Framework in key areas like openness, interoperability, documentation and platform independence. By requiring digital solutions to use approved open licenses and adhere to widely recognized standards and best practices, the DPG Standard promotes transparency, reusability and integration across diverse systems. This mirrors the Universal DPI Safeguards Framework's emphasis on open standards and interoperability, helping ensure that DPI remains accessible, auditable and adaptable while avoiding vendor lock-in.

The Standard also requires thorough documentation of source code, use cases and functional requirements, which supports transparency and accountability. This allows implementers and users to understand how a solution works and verify that it meets expected practices. Additionally, the 'Do No Harm by Design' indicator ensures that potential risks and harms are anticipated and mitigated, reflecting the Safeguards' focus on lifecycle risk management and protecting vulnerable populations.

Real-world application

Several widely adopted DPGs already demonstrate how closely the DPG Standard aligns with the Universal DPI Safeguards Framework, especially when used as foundational layers of DPI. The open-source platform Mojaloop, for instance, has publicly articulated its commitment to responsible, inclusive design in a thought piece, 'How Mojaloop Embraces the UN's DPI Safeguards Framework' where it maps its interoperability architecture and operational practices to both Foundational and Operational Universal DPI Safeguards principles. Similarly, MOSIP - the Modular Open Source identity platform - a DPG that has been implemented in over 10 countries, has outlined its adherence to responsible governance, data protection and inclusion principles in their own publications, showing how an open-source identity platform can reflect safeguards in practice.

The Universal DPI Safeguards Framework is dynamic by design and reflects a commitment to continuous adaptation in a rapidly evolving digital landscape. Its initial version evolved in 2025 through extensive multi-stakeholder consultations, incorporating inputs from areas like financial inclusion, children's rights, DPI and AI, and cybersecurity. This collaborative approach ensures the Framework, with its 300 recommendations for the responsible authorities involved, covers concrete, applicable and practical use cases for responsible deployment. This evolution will continue through close collaboration with the ecosystem and in conjunction with the DPG Standard including its recent updates on AI and data security and other key indicators like 'Do No Harm by design'. This requires all DPGs to have policies identifying inappropriate and illegal content including child abuse and protection from harrassment (Indicator 9c), enabling users and contributors to protect themselves against grief, abuse and harassment.

In September 2025, the DPI Safeguards initiative and the 50-in-5 campaign, which is co-led by the DPGA, announced the DPI Safeguards Accelerator. Launched during the high level week of the 80th United Nations General Assembly, the Accelerator is a platform that connects global coordination with local action, with the purpose of moving countries from commitment to full implementation of the Universal DPI Safeguards Framework. The Accelerator operates as a hub for knowledge, experts, tools and templates, offering technical assistance, training on safeguards and various assessments (including digital readiness and inclusion). This structured effort will help countries scale DPI more efficiently and embed a safeguards-by-default approach from the very beginning, ensuring the technologies are safe, trustworthy and inclusive.

A whole of society approach

The DPG Standard helps translate safeguards into concrete product-level requirements, while the Universal DPI Safeguards Framework supports countries in embedding these protections at a system level across the entire DPI life cycle. Together, they help chart a future where scaling DPI is not just faster or more efficient, but fundamentally safer, more trustworthy and centred on the people it is meant to serve.

Across society, everyone has a stake in shaping a safe and inclusive digital future. We invite stakeholders across governments, civil society and the technology community to engage with these frameworks and provide any feedback:

a. **Apply to the DPG Registry:** Listing your solution as a DPG validates its potential for global impact and connects you with governments and organizations looking to adopt proven, open-source technologies that adhere to international standards.
b. **Join the DPI Safeguards Implementors Collective** and contribute to a global community dedicated to promoting responsible and ethical DPI and ensuring that safeguards are at the core of all digital transformation efforts.