



Digital
Public
Goods
Alliance



A Practical Guide to the **DPG Standard**



Digital
Public
Goods
Alliance



A Practical Guide to the **DPG Standard**

Authors

Amreen Taneja

Ricardo Miron

Published by **Digital Public Goods Alliance Secretariat**

Version 1.0 | October 2026

Licence

This work is licensed under the Creative Commons Attribution 4.0 (BY) license, which means that the text may be remixed, transformed and built upon, and be copied and redistributed in any medium or format even commercially, provided credit is given to the authors. For details go to creativecommons.org/licenses/by/4.0/. Creative Commons license terms for re-use do not apply to any content (such as graphs, figures, photos, excerpts, etc.) not original to the publication and further permission may be required from the rights holder. The obligation to research and clear permission lies solely with the party re-using the material.



Disclaimer

This document was drafted and edited by the authors with assistance from generative AI for language refinement and structural feedback. All arguments, sources, and factual claims were reviewed and verified by the author and editorial team.

Contents

4	Introduction
5	The Nine Questions Every DPG Must Answer
6	1 Does the Solution Contribute to the Sustainable Development Goals (SDGs)?
7	2 Is the Solution Released Under an Approved Open License?
8	3 Is Ownership Clearly Documented?
9	4 Can the Solution Operate Independently of Proprietary Platforms?
10	5 Is the Solution Thoroughly Documented?
11	6 Can Non-personal Data Be Extracted in an Open Format?
12	7 Does the Solution Comply with Privacy and Applicable Laws?
13	8 Does the Solution Follow Open Standards and Best Practices?
14	9 Does the Solution “Do No Harm” by Design?
14	9A Data Privacy and Security
14	9B Inappropriate and Illegal Content
14	9C Protection from Harassment
15	Keeping the DPG Standard Updated

Introduction

Digital public goods (DPGs) are open digital solutions that help deliver public value. They support everything from health systems and education services to humanitarian response, climate action, and government services. As countries increasingly rely on digital technologies to deliver essential services, there is growing interest in identifying digital solutions that are not only open, but also trustworthy, well-governed, secure, and designed for public benefit.

At the heart of every digital public good is the DPG Standard. Managed and maintained by the Digital Public Goods Alliance (DPGA) Secretariat, the DPG Standard provides a shared framework to evaluate whether a DPG

along with being open, is also accessible and intentionally designed to benefit people and communities. Composed of nine indicators, it defines the safeguards, practices, and evidence that governments, funders, and implementers are looking for to build confidence in adopting and investing in a DPG.

But what does meeting the DPG Standard actually look like in practice? The nine indicators provide a practical way to assess how a digital solution is built, governed, and designed. Below, we unpack each indicator through a guiding question and highlight a DPG that demonstrates it in practice.

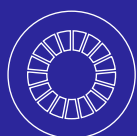
[Learn More](#)

Digital Public Goods Decoded



The Nine Questions Every DPG Must Answer

Below are the 9 indicators and requirements that determine if nominated software, data, AI systems, or content collections can be considered a DPG.



1 SDG Relevance



2 Open Licencing



3 Clear Ownership



4 Platform Independence



5 Documentation



6 Non-PII Data Extraction



7 Privacy & Applicable Laws



8 Standards & Best Practices



9A Data Privacy & Security



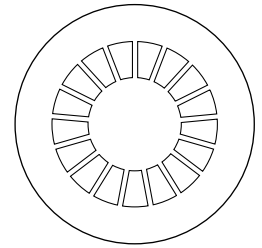
9B Inappropriate & Illegal Content



9C Protection from Harassment

SDG Relevance

Does the Solution Contribute to the Sustainable Development Goals (SDGs)?



A digital public good must address a real-world challenge and contribute to one or more Sustainable Development Goals. Reviewers look for evidence that demonstrates both relevance and impact.

What We Review

Description of the solution and how it contributes to each selected SDG.

Evidence of positive social or developmental outcomes or impact.

Case studies, blog posts, media coverage or implementation examples.

Why It Matters

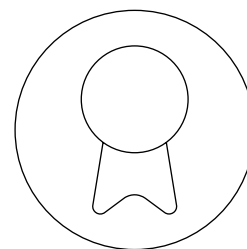
Openness alone does not verify a solution as a digital public good. To qualify, a solution must demonstrate a credible contribution to one or more SDGs – the globally recognised framework for addressing social, economic, and environmental challenges. Requiring this link ensures that DPGs extend beyond open access to reflect a shared understanding of public value.

Learn More
SDG Relevance Guide



Open Licencing

Is the Solution Released Under an Approved Open License?



Open licensing is a core requirement. Implementers and users must be able to legally access, use, modify, and share the solution. Open-source software, content, data, and AI systems must use the appropriate open license for their category.

What We Review

Public link to the solution's approved open license.

Verification that the license is approved for the right category: open software, open data, open content, or open AI system.

Why It Matters

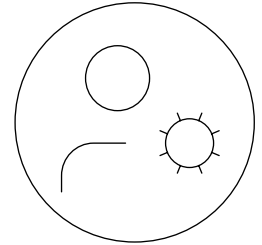
Openness is foundational to a DPG, and an approved open license gives others the legal right to use, adapt, and build on a solution rather than simply making its code, content, or data visible.

Learn More
Open Licensing Guide



Clear Ownership

Is Ownership Clearly Documented?



Transparency about ownership and governance helps users understand who is responsible for maintaining the solution and making decisions about its future. It also ensures accountability for the solution's data, code, and model, enabling users to know who owns, stewards, and is responsible for these components.

What We Review

Information on the accountable entity/owner.

Copyright, terms of use, or trademark documents.

Data governance or stewardship documentation.

Other publicly available documentation such as license, website, repository, etc.

Why It Matters

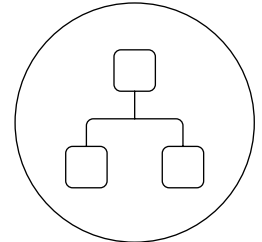
A DPG must be transparent about who owns and stewards it so that adopters know who is behind the solution and the decisions and governance that shape its development.

Learn More
[Clear Ownership Guide](#)



Platform Independence

Can the Solution Operate Independently of Proprietary Platforms?



Digital public goods must disclose any mandatory dependencies (libraries, software, hardware) that could impose more restrictions than the DPG's own open license. For any closed or proprietary component, they must show either that the solution is independent of it or that a functional open alternative exists.

What We Review

Technical architecture documentation.

List of dependencies and third-party components.

Explanation of any closed or proprietary components.

Open alternatives to proprietary components.

Documentation on how the solution can be deployed and operated.

Why It Matters

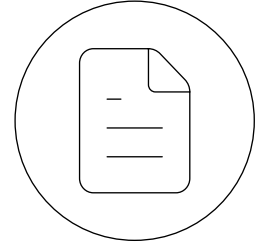
A DPG should give adopters meaningful choice and control, rather than locking them into proprietary dependencies or services that the DPG itself is dependent on, and therefore an adopter would need to use as well.

Learn More
Platform Independence Guide



Documentation

Is the Solution Thoroughly Documented?



Digital public goods must provide documentation detailed enough that someone unfamiliar with the project can understand how to use, deploy, and modify it. Clear documentation makes it easier for others to adopt, maintain, improve, and scale the solution.

What We Review

User guides and instructions.

Developer documentation.

Data descriptions and collection methods.

Access and usage instructions.

Links to all relevant documentation.

Why It Matters

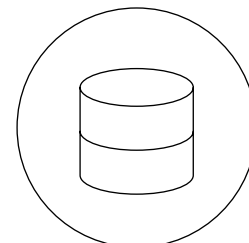
A solution cannot meaningfully be open if others cannot understand how to deploy, use, maintain, or adapt it. Documentation helps turn openness into practical reuse.

[Learn More](#)
[Documentation Guide](#)



Non-PII Data Extraction

Can Non-Personal Data Be Extracted in an Open Format?



Where a digital public good collects or uses non-personally identifiable information (non-PII) data or content, it should provide a practical way to import or export that data in a non-proprietary format, such as CSV, JSON, XML, or through an API.

What We Review

Data export in open formats.

Data import in open formats.

API access to non-personal data.

Explanation of how data can be downloaded or shared.

Links to relevant documentation or technical guidance.

Why It Matters

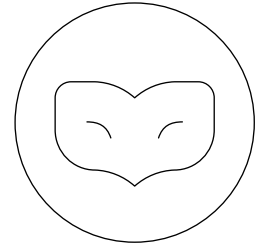
This helps adopters retain access to and control over their data, exchange it with other systems, adapt or migrate the solution when needed and reduce avoidable vendor or platform lock-in without requiring the extraction of personal data.

Learn More
Non-PII Data Extraction Guide



Privacy & Applicable Laws

Does the Solution Comply with Privacy and Applicable Laws?



Digital public goods are designed and managed to meet privacy and legal requirements. This requirement enables users to understand how their personal information is collected, used, shared, and protected.

What We Review

Privacy policy.

Terms of service.

Data collection and use practices.

User consent procedures.

Applicable privacy laws.

Why It Matters

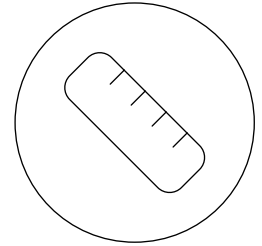
Creating public value also means protecting the people a solution serves. DPGs must handle personal information responsibly and operate in accordance with applicable laws.

Learn More
[Privacy and Applicable Laws Guide](#)



Standards & Best Practices

Does the Solution Follow Open Standards and Best Practices?



Following open standards and best practices helps a solution work well with other systems and makes it easier to use, maintain, and improve over time. It also helps ensure the solution is reliable, secure, accessible, and sustainable.

What We Review

Information on interoperability standards.

Technical specifications.

API standards.

Accessibility practices.

Security best practices.

Relevant certifications or assessments.

Why It Matters

DPGs are intended to be reusable across different contexts, making interoperability, accessibility, security, and other recognised best practices essential to their broader adoption and sustainability.

Learn More
Open Standards and Best Practices Guide



Do No Harm

Does the Solution “Do No Harm” by Design?

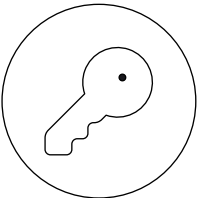
“Do No Harm” means identifying and reducing any risks the solution may create for users or communities. In the context of DPGs, it assesses whether potential harms, such as privacy risks, security issues, harmful content, exclusion, or misuse, have been identified and addressed through appropriate safeguards.

To make this indicator more measurable, the DPG Standard delineates it into three sub-indicators that assess specific risks and protections.

9A

Data Privacy and Security

If a solution collects personal data, it must demonstrate how that information is protected.



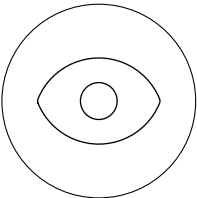
What We Review

- Information on interoperability standards.
- Technical specifications.
- API standards.
- Accessibility practices.
- Security best practices.
- Relevant certifications or assessments.

9B

Inappropriate and Illegal Content

If a solution hosts or distributes content, it must demonstrate how harmful, inappropriate, or illegal material is managed.



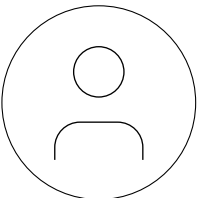
What We Review

- Content moderation policies.
- Reporting processes.
- Community guidelines.
- Procedures for reviewing and removing content.

9C

Protection from Harassment

If users interact through the solution, there must be safeguards to protect them from abuse and harassment.



What We Review

- User safety policies.
- Codes of conduct.
- Reporting mechanisms.
- Moderation procedures.
- Online safeguarding measures.

Why It Matters

The DPG Standard turns “openness” from an unverified claim into a trusted standard. As a result, governments and funders can confidently build on open software, data, AI, and content, assured of their reusability, vendor independence, and safety.

Learn More
Do No Harm by Design Guide



These nine indicators move the conversation beyond the question of whether a solution is open source. They assess whether it is accessible, trustworthy, and capable of creating meaningful public value. For applicants and implementers, meeting the DPG Standard requires clear evidence that the solution is open, well-managed, documented, safe, and ready for others to use and adapt.

Keeping the DPG Standard Updated

Rather than a static checklist, the DPG Standard is a living framework that evolves alongside changes in technology, policy, and digital development priorities. Two complementary

processes, top-down and bottom-up feedback, help ensure that the DPG Standard remains both practical and relevant while staying grounded in its core principles.

 Stewardship Process	This process is coordinated by the DPGA Secretariat and the DPG Standard Council. Feedback is collected from applicants, reviewers, governments, funders, implementers, and ecosystem partners. The DPG Secretariat identifies recurring challenges, emerging issues, and areas where the DPG Standard may need improvement. Proposed updates are reviewed by the DPG Standard Council. Once approved, changes are incorporated into the DPG Standard through the public review process.
 Community-Informed Process	This process allows the wider community to participate directly in improving the DPG Standard. Anyone can propose changes, raise issues on GitHub, or suggest clarifications. Contributors may include product owners, governments, researchers, implementers, civil society organisations, and community members. Suggestions are submitted through public channels, such as GitHub. The DPG secretariat reviews these contributions and escalates significant proposals to the DPG Standard Council for consideration.
 Expert Group Contributions	Expert groups bring together independent subject matter experts to discuss potential updates to the DPG Standard. Working in their personal capacity to maintain neutrality, they research issues, create annexures of best-practice guidance to support applicant compliance, and recommend changes to the DPG Standard. These recommendations are submitted to the DPG Standard Council for review and consideration. Once reviewed, proposed changes are published on GitHub for public consultation, allowing individuals, organisations, and experts to provide feedback. The consultation period varies depending on the significance of the proposed updates.

Updates generally fall into three categories:

Minor Changes

Clarifications, corrections, examples, and guidance improvements that do not alter the intent of an indicator.

Major Changes

Revisions that affect how requirements are interpreted or assessed and may require consultation and additional review.

Fundamental Changes

Significant updates to indicators, assessment criteria, or requirements in response to major technological or policy developments.

These approaches and changes help ensure the DPG Standard reflects real-world

implementation, keeps pace with evolving technologies and policies, and remains shaped by the communities that use and implement DPGs.

One example of this evolution can be seen in the growing focus on artificial intelligence. Questions about AI systems, open data, transparency, and responsible use are prompting new conversations about how DPGs can remain both innovative and accountable. These discussions demonstrate how the DPG Standard adapts to emerging technologies while preserving the principles that make DPGs trusted and credible in the first place.

Ultimately, the DPG Standard provides more than an assessment framework. It creates a common foundation of trust, helping governments, funders, implementers, and communities identify digital solutions that are accessible, open, and designed to deliver meaningful public good.



Digital
Public
Goods
Alliance



A Practical Guide to the **DPG Standard**

If you think there's a mechanism that is missing from this overview, please reach out to hello@digitalpublicgoods.net. Your feedback will help inform future updates to the DPG Standard and its accompanying guidance.