Digital Public Goods Alliance

Enhanced Privacy Framework for the DPG Standard

About the Digital Public Goods Alliance

Established in 2019, the Digital Public Goods Alliance is a multi-stakeholder initiative with a mission to accelerate the attainment of the sustainable development goals in low- and middle-income countries by facilitating the discovery, development, use of, and investment in digital public goods. Digital public goods are open-source software, open data, open AI systems, and open content collections that adhere to privacy and other applicable laws and best practices, do no harm, and help attain the SDGs. To learn more, visit digitalpublicgoods.net or contact hello@digitalpublicgoods.net.

Executive Summary

Privacy compliance is a critical foundation for the success, credibility, and long-term sustainability of digital public goods (DPGs). By implementing robust privacy measures, DPGs can build user trust, mitigate potential risks, and ensure alignment with regional and international privacy and data security regulations. For this reason, in April 2024, the DPGA Secretariat along with the Open Knowledge Foundation gathered a set of privacy professionals from the legal, technical, multilateral and industry sectors as a Privacy Expert Group with the goal to strengthen the privacy components of the DPG Standard. This report presents both the recommendations of the Privacy Expert Group and the updated requirements under Indicator 7 and Indicator 9A as determined and approved by the Standard Council, which are designed to safeguard privacy while fostering transparency, accountability, and ethical data practices.

These updated requirements aim to embed privacy protections into the design and development of DPGs, enabling them to better serve users and communities. By incorporating these practices, DPGs can enhance their societal impact, uphold user rights, and contribute meaningfully to global development goals.

The recommendations from the expert group were submitted to the Standard Council as part of the DPG Standard's governance process. The Standard Council, in turn, refined and simplified these recommendations, ensuring they could be effectively incorporated into the DPG review process. This ensures that privacy compliance becomes an integral part of the DPG evaluation, supporting both operational efficiency and high ethical standards across the DPG ecosystem.

In this document

Digital Public Goods Alliance

Introduction

Privacy is critical to protecting user data and ensuring ethical deployment of DPGs, particularly in underserved communities. Weak privacy practices can lead to breaches, exploitation, and loss of trust. Integrating privacy measures helps mitigate these risks, ensuring DPGs empower users without causing unintended harm. Furthermore, aligning DPGs with global privacy frameworks enhances their credibility and facilitates wider adoption.

Privacy safeguards are integral to fostering trust and ensuring the responsible use of technology. Indicator 7 of the DPG Standard addresses the need for DPGs to comply with global privacy laws, mitigate risks, and promote transparency, and Indicator 9A addresses Data privacy and security and mandates DPGs that collect, store and distribute personally identifiable data to demonstrate how they ensure the privacy, security and integrity of this data in addition to the steps taken to prevent adverse impacts resulting from its collection, storage and distribution.

Purpose of the Privacy Expert Group

The Privacy Expert Group was formed to strengthen the privacy components by addressing gaps in compliance and aligning DPGs with global best privacy practices. The group's collaborative efforts aim to establish clear, enforceable criteria that uphold privacy as a fundamental principle of DPGs.

The group, comprising neutral privacy professionals listed below, from the legal, technical, multilateral and industry sectors, was tasked with:

- Conducting a Gap Analysis and Risk Assessment to identify privacy compliance shortcomings in the DPG Standard.

- Defining clear assessment parameters and documentation requirements for privacy compliance.

- Proposing a verification process for evaluating privacy compliance, under the DPG Standard such that it can serve as fair criteria for both small scale and larger DPGs.

Meeting Structure and Collaboration

As per Standard governance processes, the DPG Standard Privacy Expert group was co-convened by the DPGA Secretariat's Standards Lead- Amreen Taneja and the DPGA member organisation- Open Knowledge Foundation, represented by Renata Avila (CEO) and Patricio Del Boca (Technical Lead). In addition, the Expert group comprises 7 subject matter experts who participated in a personal capacity and represented prominent regions from where the highest number of DPG applications are received, enabling them to assess requirements per local legislations and regional privacy ecosystems.

Action Plan and Responsibilities

The group worked towards:

- Developing sub-clauses under Indicator 9A through consultations with legal, technical, and academic experts.

- Establishing a minimal but actionable verification process for DPG applicants.

- Drafting privacy-related annexures to ensure a holistic privacy framework.

This report details the updated minimum criteria under Indicators 7 and 9A for DPG recognition. The group's efforts produced refined requirements, framed as questions, to enhance transparency, accountability, and alignment with global privacy standards.

Current State of Privacy Review in the DPG Standard

The current framework of the DPG Standard, particularly under Indicators 7 and 9A, provided a foundation for addressing privacy and data protection in digital public goods. However, through consultation with the expert group and stakeholders, a need was identified to enhance these indicators to align more closely with evolving global privacy standards and best practices. While the Standard emphasized key principles such as compliance with applicable regulations and basic security protocols, the review process revealed opportunities to strengthen how privacy is integrated into the design and development stages of DPGs.

To address these gaps, updated requirements were developed to embed critical privacy concepts—such as data minimization, transparency in data usage, privacy-by-design, and robust user consent mechanisms—into the application process. This refinement ensures that applicants not only meet regulatory expectations but also demonstrate adherence to ethical data governance practices. By introducing simplified, targeted questions, the updated process effectively captures essential privacy information traditionally found in more extensive documentation like Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs), ensuring accessibility for a diverse range of applicants. These updates represent a concerted effort to uphold trust, inclusivity, and global recognition of DPGs while fostering responsible and transparent data governance practices.

Recommendations & Updated Requirements

To uphold robust privacy and data governance practices, the expert group has identified essential elements that applicants must address during the application process to be recognized as digital public goods. The application process is thoughtfully designed to accommodate the diverse range of applicants, from large organizations to small-scale innovators, ensuring both inclusivity and enhanced quality.

The expert group highlighted key privacy concepts that should be integral to assessing the privacy aspects of a DPG, drawing from global privacy frameworks. These concepts ensure that DPGs comply with regulatory requirements and adhere to ethical data protection guidelines. The group also recognized specific documentation, such as Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs), which are typically used to evaluate the operational implementation of privacy policies. However, these documents go beyond the scope of the DPG review process, which focuses specifically on the design and development stages of the product. As a result, the Standard Council distilled these privacy concepts into a set of targeted questions. Applicants will now be required to answer these questions, ensuring adherence to best practices and providing proof of compliance through their responses. This approach simplifies the review process while embedding privacy considerations into the design and development of DPGs, specifically under Indicators 7 and 9A. The questions aim to elicit meaningful insights into the privacy practices of applicants while minimizing complexity, ensuring the process is accessible and actionable for all.

This segment further explains how the questions included in the updated requirements for DPG applicants extract the same critical information traditionally derived from privacy-related documentation such as Privacy Policies, Privacy Impact Assessments (PIA), Data Protection Impact Assessments (DPIA), and Data Retention Policies that would be required by the DPG Review team for assessing the design and development aspects of the product.

Below, we detail how these questions capture and address fundamental privacy-related concepts critical to the recognition of a solution as a DPG:

Recommendation 1: Minimize Personally Identifiable Information (PII) in Data Collection

Definition: Data minimization refers to collecting only the minimum amount of Personally Identifiable Information (PII) required for a solution to function effectively.

Key Question to be introduced to the review process: "Is this the minimum amount of PII data required for your solution to function properly?"

Purpose: By addressing data minimization, applicants demonstrate their alignment with global privacy regulations, such as GDPR (General Data Protection Regulation), which emphasize limiting data collection to reduce risks of misuse and enhance user trust. This principle ensures that DPGs prioritize efficiency and ethical handling of data, especially for vulnerable populations.

Recommendation 2: Robust User Consent Mechanisms

Definition: User consent mechanisms ensure that users understand and agree to the collection, use, and processing of their PII.

Key Question to be introduced to the review process: "How does your solution communicate to the user that you are collecting their PII data?"

Purpose: Transparency in obtaining and managing user consent is critical to complying with privacy frameworks such as GDPR and CCPA (California Consumer Privacy Act). This question evaluates how applicants empower users to make informed choices, fostering accountability and user autonomy in data governance practices.

Recommendation 3: Ensure Transparency in Data Usage

Definition: Transparency involves openly communicating the purposes for which PII data is collected and processed.

Key Questions to be introduced to the review process:

- "Please provide your privacy policy or any relevant documentation that outlines consent management procedures, the reasons for collecting and processing PII data, and any processes in place for handling subject requests."

- "Where in the solution is PII data being processed or used? And which components of the solution allow access to this data?"

Purpose: Applicants are required to articulate their data practices clearly. This ensures that solutions comply with the principle of purpose limitation, wherein data is used only for its intended purpose, and demonstrates a commitment to operational transparency.

Recommendation 4: Adherence to Privacy-By-Design Principles

Definition: Privacy-by-design embeds privacy safeguards into the solution's architecture during its design and development stages rather than retrofitting them later.

Key Question to be introduced to the review process: "Is your solution designed with any mechanisms to delete the PII data?"

Purpose: This question evaluates applicants' readiness to handle data retention and deletion responsibly, highlighting mechanisms for addressing user requests and preventing indefinite data storage. Solutions with strong privacy-by-design features reflect a commitment to ethical data practices and regulatory compliance.

Recommendation 5: Transparency Around Data Retention

Definition: Data retention policies dictate how long PII is stored, the rationale for its retention, and the procedures for its deletion.

Key Question to be introduced to the review process: "Is your solution designed with any mechanisms to delete the PII data?"

Purpose: This question also helps convey the solution's clear data retention and deletion procedures that can ensure compliance with laws like GDPR that mandate minimizing risks associated with prolonged data storage. This demonstrates accountability and fosters trust among users, particularly in solutions catering to marginalized communities.

Recommendation 6: Ensure access to PII Data is Securely Managed through Data Governance and Access Controls

Definition: Effective data governance ensures that PII is securely managed, while access controls limit unauthorized access to sensitive information.

Key Question to be introduced to the review process: "Where in the solution, is PII data being processed or used? And which components of the solution allow access to this data?"

Purpose: Evaluating data governance practices helps ensure that PII is protected against breaches and misuse. Applicants who demonstrate robust governance mechanisms align with the principle of data isolation and segregation, reducing risks of unauthorized access.

Conclusion

Privacy and data protection are essential for the ethical and sustainable deployment of DPGs and they play a critical role in DPGs, fostering trust, ensuring equitable impact, and achieving global recognition. Effective or appropriate privacy measures demonstrate transparency and accountability, encouraging user engagement and adoption by ensuring responsible data practices. These measures are particularly vital for protecting marginalized and vulnerable populations, such as children, refugees, and low-income groups, from the risks of data misuse or unethical practices.

Aligning DPGs with global privacy standards enhances their credibility, compliance, and appeal to partners, funders, and international initiatives. By embedding robust privacy safeguards, DPGs strengthen their reputation and ability to drive meaningful impact within the digital development and open-source ecosystem.

The expert group provided valuable inputs in developing updated requirements under Indicators 7 and 9A, offering applicants a clear framework to integrate privacy into their design and operations. These updates address existing gaps and ensure that privacy is treated as a priority in DPG development.

To uphold their integrity, inclusivity, and sustainability, stakeholders must recognize privacy as a fundamental aspect of DPG quality. By adopting these enhanced requirements, applicants and implementers can align with global standards, build user trust, and mitigate potential risks, securing the long-term success and impact of digital public goods.

Acknowledgements

This report was drafted by Amreen Taneja, Standards Lead at the Digital Public Goods Alliance Secretariat. We extend our sincere gratitude to the members of the DPG Standard Privacy Expert Group, whose names are listed below, for their time, expertise, and thoughtful contributions. Their invaluable insights have greatly enhanced our understanding of privacy best practices and have been pivotal in shaping the recommendations outlined in this report.

We would like to thank Renata Avila and Patricio Del Boca from the Open Knowledge Foundation for co-convening this expert group. Their leadership and dedication have been instrumental in fostering collaboration and driving this important work forward.

Expert Group

- Renata Avila, Open Knowledge Foundation
- Patricio Del Boca, Open Knowledge Foundation
- Thomas Shone, Booking.com
- Aparna Bhushan, Wayfair and UNICEF
- Clarissa Luz, Manassero Advagados
- Godfrey Kutumela, The MIFOS Initiative and GH Solutions Consultants
- Marie C. Bonnet, International Association of Privacy Professional and ID Side
- Emma Day, Tech Legality
- Puneet Bhasin, Cyberjure Legal Consulting


Digital
Public
Goods
Alliance