Digital Public Goods Alliance

Privacy & Data Security Best Practices for Digital Public Goods

In this document

Introduction

This annexure to the DPG Standard provides detailed guidance on privacy and data security best practices for open-source solutions seeking recognition as digital public goods (DPG). While the practices outlined are not mandatory, they represent widely accepted industry standards that support stronger alignment with the DPG Standard's requirements on privacy, security, and data integrity.

This guidance synthesises expert inputs and risk assessment frameworks to establish unified suggestions for applicants wishing to align with industry best practices and can serve as a practical roadmap for both small and large-scale open solutions. By following these best practices, solutions can ensure better compliance with privacy and data security measures while advancing their mission as digital public goods.

Given the diverse nature of digital public goods, these guidelines should be applied within the context of your specific solution. We recognise that not all best practices will be applicable to every DPG category, as organisational responsibilities may vary significantly based on the type of solution and operational model.

When documenting compliance, we therefore recommend clearly identifying which requirements fall within your scope of responsibility and explicitly indicate which fall outside your operational control. This approach ensures transparency and helps evaluators understand the boundaries of your data governance commitments.

1. Privacy Governance and Accountability: Policy-Level Best Practices

1.1. Privacy Policy

Applicants should provide a clear and accessible privacy policy that demonstrates alignment with international privacy standards (e.g., OECD Privacy Guidelines, ISO/IEC 29100). The policy should:

- Identify the types of personal data collected and processed.
- Define, with transparency, the purpose and legal basis for all data processing activities - map local data protection laws (e.g., European Union's General Data Protection Regulation, South Africa's Protection of Personal Information Act, 2013, China's Cybersecurity Law, India's Digital Personal Data Protection Act, 2023 and Personal Data Protection Bill, 2019, Brazil's General Personal Data Protection Law etc.) to privacy policy objectives.
- Describe data minimisation, data retention and purpose limitation practices (e.g., anonymisation and aggregation).
- Establish robust consent mechanisms and transparent procedures for withdrawing consent, ensuring compliance with applicable regulations, including specific provisions for cross-border data transfers, where required.
- Outline the rights of data subjects, including access, correction, deletion, and objection.
- Provide contact information for the privacy officer or data steward.

- Include the retention schedule and justification for data retention.
- Identify any third-party data processors, including their role and access scope.
- For solutions handling children's data, specify consent and age verification mechanisms. Compliance with regulations like the UK Children's Code, the United States' Children's Online Privacy Protection Rule (COPPA) or UNICEF's Responsible Data for Children (RD4C) principles should be encouraged.

1.2. Non-PII and Group Data Risks

While privacy policies traditionally pertain to personally identifiable information (PII), the design phase should also consider non-PII datasets that pose re-identification or group profiling risks (e.g., aggregated behavioural or location data). Solutions intended for use in high-risk or vulnerable contexts (e.g., humanitarian settings, child-focused applications) should explicitly outline harm mitigation strategies under the 'Do No Harm by Design' approach in line with Indicator 9 of the DPG Standard.

1.3. Governance Accountability Best Practices

Designate a Data Protection Officer (DPO):

Appoint a Data Protection Officer (DPO) or an equivalent role to ensure accountability for data governance and compliance with privacy regulations. For smaller projects, this role can be filled by a designated team member or external consultant.

Establish an Independent Ethics Review Process:

Implement an independent ethics review process, such as an Ethics Review Board (ERB), to regularly assess and oversee AI/ML practices and their ethical implications. For larger projects, external experts can be invited to ensure impartiality and responsible AI development.

Promote Explainable AI (EAI):

Incorporate transparent and explainable AI techniques into your system design to enhance trust and accountability. Leverage available libraries and tools to ensure that AI decisions are interpretable by users and stakeholders.

Foster Public Transparency in Governance:

Ensure public transparency in data governance practices. This includes making board meeting summaries, decision-making processes, and community consultations publicly available, especially for projects that serve critical infrastructure (e.g., identity systems, healthcare, etc.).

2. Compliance Documentation and Proofs

To demonstrate privacy-by-design, DPG applicants should provide the following documentation, via an industry-recognised template:

2.1. Data Protection Impact Assessment (DPIA) or Privacy Impact Assessment (PIA)

Strongly recommended for high-risk processing activities. A DPIA should include:

- Overview of data processing activities
- Risk identification and mitigation strategies
- Legal and regulatory alignment
- Stakeholder engagement and approvals

Smaller-scale solutions may provide a PIA, using recognised industry templates focusing on transparency, data minimisation, and security

2.2. Data Flow Map

A current map showing

- Collection points, transfers, processing locations (including any automated or algorithmic processing of personal data), and data storage
- Identification of data domains and categories
- Relationships with third-party processors

2.3. Data Retention and Disposal Policy

This document should include clearly defined:

- Retention timeframes
- Rationale based on legal, contractual, or operational needs
- Secure deletion processes and verification methods

2.4. Communication of Security Issues for Solutions

Recommendations for clear and effective communication of security issues should be focused on ensuring that stakeholders can report and respond to risks efficiently. This includes:

- **Published Security Contact:** Ensure there is a designated, publicly accessible security contact for reporting security issues. This contact should be easy to find and actively monitored to ensure quick responses to any security-related concerns.

- **Clear Risk Communication to Solution Operators:** Establish clear and predefined channels for communicating security risks to those operating the solution. These channels should provide a structured way to assess, classify, and escalate risks, ensuring that operators can respond promptly and effectively.

- **User and Regulator Notification Pathways:** Define well-established notification pathways for users and regulators in the event of a security breach or significant risk. Ensure that these pathways are aligned with breach reporting timelines and applicable regulatory requirements to guarantee timely and compliant communication.

- **Roles and Responsibilities for Communication:** Clearly outline roles and responsibilities for communication during security incidents. This ensures that internal teams, solution operators, and other relevant stakeholders understand their obligations to communicate issues quickly and consistently.

2.5. Training Records

The solution should maintain comprehensive records of privacy training activities, capturing the training content, delivery frequency, and participant attendance, to support compliance with privacy obligations.

2.6. Third-Party Vendor List

- Names and roles of external data processors or a vendor list with the nature of their activities
- Types of data shared and the purpose of sharing
- Contractual safeguards in place, e.g., Data processing agreements or Standard Contractual clauses
- Data security risk assessment of third-party vendors

3. Technical and Organisational Safeguards

Applicants should demonstrate the implementation of minimum data protection controls, including:

3.1. Authentication and Access Controls

- Role-based access using unique credentials
- Multi-factor authentication for sensitive systems
- Implement least privilege access - ensure users and systems are granted only the necessary access when needed
- Regular reviews of privileged access and the revocation of access from users and systems when it is no longer required
- Enforce continuous authorisation to ensure access is not permanently granted after login, but it is continuously evaluated based on user behaviour, context, and risk

3.2. Logging and Auditing

- Implement robust logging mechanisms to record and monitor access to systems and personal data. Logs should capture relevant metadata such as user identity, timestamp, actions performed, and access levels.
- Establish clearly defined protocols for breach detection that trigger an immediate investigation and response when suspicious behavior is identified.

3.3. Encryption

All personal data should be protected through state-of-the-art encryption techniques, both in transit and at rest, in accordance with internationally recognised cryptographic standards.

Encryption measures should be:

- Consistently applied across all relevant systems and environments where personal data is stored or transmitted.
- Reviewed and updated periodically to reflect evolving security best practices and regulatory requirements.
- Implemented in a manner that ensures the confidentiality, integrity, and availability of data in compliance with applicable data protection legislations (e.g., GDPR Article 32).

3.4. Vulnerability Management

- Periodic vulnerability assessments, for example, via automated dependency monitoring and auditing using static analysis tools and supply chain checks
- Monitor and remediate supply chain vulnerabilities in 3rd party dependencies
- Documentation of identified risks and corrective actions taken
- Set up communication channels for escalating security issues

3.5. Data Isolation and Localisation

- Geographic segregation of datasets, where applicable - use traffic steering rules to ensure user requests are handled only by in-region infrastructure
- Justification for cross-border transfers and measures to ensure compliance
- Use tenant-specific databases, schemas, or environments in multi-tenant architectures

3.6. Privacy-Enhancing Technologies

Use of differential privacy, legislatively-compliant pseudonymisation, federated learning, Secure Multi-Party Computation (SMPC), or Zero-knowledge proofs (ZKPs) based authentication, where appropriate to minimise privacy risks, especially in AI systems applying for DPG recognition.

4. Lifecycle Management and Oversight

Solutions should embed privacy into all stages of the data lifecycle:

- **Ongoing Risk Monitoring:** Regular review of risk assessments to reflect changes in data processing.
- **Audit Readiness:** Maintain documentation to demonstrate compliance with DPG Standard Indicators 7 and 9(a).
- **Change Management:** Ensure privacy and security implications are assessed during product updates.

Digital
Public
Goods
Alliance