Centre for Digital
Public Infrastructure

Version 1

Key Legal Clauses

to include in DPI implementation Agreements for Countries

AUTHORS

Kamya Chandra | Tanushka Vaid | with co-creation from the DPI legal, tech & policy ecosystems

Foreword

Digital Public Infrastructure (DPI) refers to population-scale verifiable identities, interoperable payments systems, and consented data-sharing networks which form the foundation of digital economies.

While building DPI, it is important to ensure that legal principles and best practices are integrated at every stage of the procurement cycle, such as during needs assessment, technical scoping and specifications, rollout strategy, bidding, evaluation, and contracting.

When countries craft legal contracts between country departments, private vendors and open-source product owners (where applicable), they often risk including loopholes which can be exploited by vendors for commercial interests.

This document outlines key clauses that can guard against vendor lock-in, ensure data sovereignty and ensure adherence to global best practices. These clauses must not be read in isolation: it is important for each legal contract to be supported with a technical specifications document ("Scope") that can provide the nuanced implementation information without which legal protections will be unenforceable in practice.

One example of this is a legal clause which states that data must be downloadable and portable in standardised formats, must be supported by a technical document that outlines which formats must be adhered to in order to be interoperable with the country's current infrastructure.

These clauses have been leveraged for implementations of verifiable credential wallets as data sharing infrastructure, but could be extensible to other foundational DPI (such as verifiable ID systems, payments infrastructure, real time data exchange layers, etc.).

These clauses apply to two types of DPI (software) implementors:

TSPs	**Technology Service Providers:** Entities that bid for country DPI implementations by offering to deploy a ready-made open source product in partnership with the Open Source Product Owners.

ISVs	**Independent Software Vendors**: Entities that bid for country DPI implementations by offering an existing customised proprietary product built on top of open source code that obviates a country's need to re-deploy a local instance.

Global DPI Implementations in Trinidad and Tobago (T&T), Brazil and Peru have incorporated these clauses into their legal agreements with global consulting firms for building verifiable credential wallets for personal data-sharing.

These clauses can be incorporated into different types of legal arrangements based on the country's context and decision. In T&T, the Country entered into agreement with the open-source product owner who in turn had a back-to-back agreement with the Service Provider. Both agreements incorporated these clauses for the signatory parties. In Brazil, these clauses were incorporated into the country's own standard legal templates to strengthen legal safeguards and ensure best practices. In Peru, these clauses formed a tri-lateral agreement between the Country, Open-Source product owner and Service Provider to include all parties into a shared framework.

Their experience serves as a powerful reminder that countries can start to proactively safeguard themselves against some of the common pitfalls of DPI implementations (including vendor lock in, lack of access to source code, handing over personal data, data breaches) through well-designed, robust legal agreements.

We hope this guiding document can help other countries in their challenging but rewarding journey of institutionalising population-scale digital transformation.

Note:

XX. Sentences in black are the legal clauses to consider.

> Sentences in lavender are explanations for the legal clauses provided.

SECTION I

Definitions for reference

"Country Partner"	refers to the country that intends to deploy digital public infrastructure within its jurisdiction.
"Implementation Partner"	refers to Independent Software Vendors, Service Providers, system integrators, program managers or any entity that bids for country DPI implementations.
"DPG Partner"	refers to the Open Source product owner in cases where they are involved in implementations.
"Solution"	refers to the technology product which is the subject matter of this Agreement.
"Pilot"	refers to the DPI implementation in the relevant country carried out by the Service Provider or ISV which is the basis for this engagement.
"Technical Scope"	refers to the supporting technical document with details of the Solution(s) that are being implemented on the basis of which Service Provider or ISV will submit the bids.

SECTION II. A.

Responsibilities of the Implementation Partner

01 The Implementation Partner shall implement and deploy the Solution in accordance with the Technical Scope document.

> *This links the Legal Contract with the complementary Technical Scope document to provide implementation specifications to be adhered to while executing the rights and obligations outlined herein.*

02 The Implementation Partner shall interact with the Country Partner to ensure that the rollout reflects the relevant legal, social and customary nuances as may be relevant to the effective design, implementation and deployment of the Solution.

> *The Implementation Partner must conduct programmatic activities such as stakeholder mapping, private-sector consultations, local awareness campaigns to ensure that the DPI fits seamlessly into society.*

03 The Implementation Partner shall use its own employees to directly provide these services and shall not engage any other consultants and/ or service providers for this purpose without the prior written consent of the Country Partner. The Implementation Partner shall be solely responsible for adhering to the obligations mentioned herein and shall not delegate any obligations towards the Country Partner to be borne by any other entity.

> *The Implementation Partner should not be able to sub-contract the deployment to other third parties without the country's prior knowledge and consent.*

04 The Implementation Partner shall be obliged to prepare and maintain such documentation of the Solution as in the Country Partner's reasonable opinion is necessary and sufficient.

> *Adequate documentation is crucial to ensure the country is able to independently operate and maintain the infrastructure post completion of the contract. Details of what the documentation must include should be outlined in the Technical Scope document based on the Country Partner's needs and must not be open to negotiation post bid-completion.*

05 The Implementation Partner, upon request from the Country Partner, may offer additional functionalities for the implementation of the Solution. Such additional functionalities along with the details of portable and proprietary components must be clarified between the Country Partner and the Implementation Partner in writing and added to the Technical Scope Document.

> *When implementors offer proprietary aspects on top of the core open source product, they must clarify in writing which aspects are portable to other vendors and which are proprietary (potentially resulting in vendor lock-in) so that the country can make an informed decision.*

06 Upon completion of the implementation of the Solution or upon termination of this Agreement, the Implementation Partner shall ensure that requisite transition measures, enumerated in the Technical Scope Document, are implemented prior to final handover.

> *Technology transfer arrangements such as IP ownership, source-code delivery or escrow, and perpetual licenses to use software, are some of the mechanisms to ensure continuity of service even when vendors are switched.*

07 The aforementioned transition shall include training and knowledge transfer imparted to the Country Partner in order to ensure that there are no disruptions to the baseline functionalities or end user's access to the Solution.

> *The implementation partner must train the country officials to operate and maintain the solution in the long term so that the country is not dependent on the private provider indefinitely. This training must begin upon commencement of the implementation to provide country officials with adequate time to learn the systems. Training clauses actionable only post contract-completion can lead to inadequate support that prolongs vendor dependency.*

08 In the event that the Implementation Partner wishes to ensure continued engagement with the Country Partner post expiration of this Agreement, the Implementation Partner shall provide clear and transparent pricing models prior to commencement of implementation of the Pilot, including but not limited to one-time license fees, annual maintenance fees, managed service offerings, and optional add-on services.

> *Prior to commencement of the Pilot or DPI implementation, the implementor must clarify the pricing model in writing to prevent cost shocks or unexpected expenditures once implementation is underway.*

09 The Implementation Partner shall, wherever applicable, incorporate the UN DPI Safeguards as outlined in Annex 2 to be mutually agreed upon by all Parties.

> *The Country Partner and Implementation Partner must jointly decide the safeguards relevant and highlight these in the Technical Scope document prior to commencement of implementation.*

Note:

In addition to these clauses, best practices for government cloud migration should be stated in a Government Cloud Policy, data classification policies, and supporting technical documents.

SECTION II. B.

Responsibilities of the DPG Partner (where applicable)

Where open-source product owner i.e. "DPG Partner" is also supporting the implementation, they must agree to provide the required support to the Implementation Partners. This helps ensure that contributions back to the source code can be merged on time, and that delays in core product upgrades or documentation do not delay country execution.

01 The DPG Partner shall provide the codebase, interfaces, documentation and conduct relevant knowledge transfer for the Solution for the purpose of the Pilot.

> *Where open-source product owners are involved in the implementation, they may undertake training sessions, whether formal or informal, for Implementation Partners and Country Partners to understand and deploy their code.*

02 The DPG Partner shall, to the extent reasonably possible, attempt to merge all contributions made by the Service Provider to the source code.

> *When contributions are merged back, it prevents the code from being 'forked' separately for the country, and helps mature the product for subsequent implementations as well.*

03 The DPG Partner shall bear its own respective personnel and other costs associated with its responsibilities towards the fulfilment of the Pilot.

> *Open-source product owners may have back-to-back agreements with Implementation Partners or contracts for 'Engineering Partner' support that account for their time and contribution towards the country implementation, however those clauses may not include the country and form the basis of a separate agreement.*

SECTION III.

Data Governance

In countries where robust Data Protection laws and Cybersecurity laws exist, it should be directly referenced in legal contracts. However, in LMICs where legal frameworks are still nascent, Country Partners must assess whether data protection legislations are consistent with international best practices. Where there are serious deficiencies, it is essential to have project level safeguards agreed upon which will provide responsibilities on data controllers, data subject rights, grievance redressal, and recourse against disproportionate data collection and use. This will need to be coupled with technical standards for data protection and cybersecurity in the Technical Scope document.

01 The Implementation Partner shall comply with commonly recognised principles of data protection in relation to the collection, storage and processing of personal data. This shall include, but not be limited to, obligations in relation to purpose specification, data minimisation, retention restrictions, data deletion post completion and use limitation as applicable.

> *For ensuring data security and privacy, it is important that key principles of minimalism, confidentiality, retention and processing restrictions are stringently applied so that there is no scope for misuse. Details of applicable data protection laws must be included in the legal contract and supporting technical standards and specifications must be included in the Technical Scope document.*

02 Notwithstanding any rights that may exist pursuant to Trade Secrets Act or similar provisions, the Implementation Partner shall ensure that all data related to, and emerging from, the implementation is downloadable and portable in an open standardised format upon demand of the Country Partner.

> *This empowers countries with the ability to shift to another private vendor by guaranteeing that the data from previous implementations is available on demand in readable, downloadable and exportable formats (the exact formats must be specified in the Technical Scope document).*

03 Ownership: All data generated from the implementation for the Country Partner shall be owned exclusively by the Country Partner.

> *The country must remain, in all cases, the sole owner of all data generated by and through the implementation, including statistics and metrics of deployments, to prevent reuse or publication without the Country Partner's consent.*

04 The Implementation Partner shall only access data necessary for implementation and support, with the permission and/or supervision of any relevant authorities indicated by the Country Partner. The Implementation Partner shall not retain, sell, or otherwise use the data outside the scope of the services provided under this Agreement.

> *The Implementation Partner must confirm in writing to only use data necessary for the implementation of the DPI as permissioned by the country and be explicitly forbidden from using it for any commercial activity or third-party purposes.*

SECTION IV.

Term and Termination

01 Upon expiry or earlier termination of this agreement as set out in this Clause 4, the Implementation Partner will hand over and transition all the assets and services related to the Solution to the Country Partner or any other Implementation Partner that the Country Partner may identify. This shall include all assets that it has in its possession as of the date of termination regardless of its state of completion, including but not limited to - all source code and documentation in relation to the Solution, administrative access over all the aspects of the Solution that can be so transitioned. The Implementation Partner shall, from the date on which such handover and transition is complete, have no obligation or commitment whatsoever towards the Solution.

> *The Implementation Partner must be legally required to hand over all implementation related assets to the country or the country's chosen vendor upon the Country Partner's request for termination. By including this provision countries ensure continuity of previous efforts even upon dissolution of the contract.*

SECTION V.

Intellectual Property

[These clauses apply exclusively to Service Provider implementations. ISV implementations may require modification to address proprietary components developed beyond the core open-source product.]

01 The Service Provider shall, in the course of developing the Solution, ensure that it does not use any proprietary code or incorporate into such Solution any intellectual property whose continued use is subject to any licence or assignment from any third party. However, the Service Provider shall continue to retain all ownership of any pre-existing intellectual property, including any proprietary software tools. In the event such pre-existing intellectual property is used in the implementation of the Solution, the Service Provider shall grant to the Country Partner a perpetual, non-exclusive, non-transferable right to utilise such IP as a part of the Solution. Notwithstanding anything herein, the Service Provider shall ensure that the Solution once implemented is capable of functioning independent of the use of any proprietary IP including software tools.

> *While the SP can use proprietary tools to help them implement the product, the SP must ensure that all IP crucial to the continued operation and maintenance of the infrastructure lies solely with the country. This distinction is essential for preventing unintended vendor lock-in.*

02 The Service Provider shall ensure that all its employees have executed appropriate intellectual property assignment agreements that will ensure that any code developed under and in the course of providing the Services, including but not limited to customisations and enhancements, shall be capable of being released as open source code or handed over to the Country Partner. The suitable modality for releasing such code shall be agreed upon in writing by the Service Provider and Country Partner.

> *The IP developed during the customisations provided to the country must be handed over to the country or released as open source code so that it cannot be locked-in to the vendor.*

03 Notwithstanding anything contained herein or in any standard open source license terms, the Service Provider shall not modify, create derivative works or fork the open source code for any purposes except with the written permission from the DPG Partner. Such permission shall be granted based on the purpose specified in the permission and the Service Provider shall not use the modified code for any purposes other than those mentioned in the written permission.

> *If the code is forked, the country will not be able to benefit from the upgrades made to the core open source code and the DPG will not be able to benefit from the contributions made back to the code by the service provider based on the implementation experience.*

Conclusion

Implementing digital public infrastructure and negotiating with large private technology firms can be daunting, particularly when the infrastructure in question is critical to the functioning of digital economies. With this paper, it is our endeavour to outline some of the key provisions that may be included in legal contracts to safeguard the rights and interests of countries.

The incorporation of these clauses in DPI deployments in Trinidad and Tobago, Brazil, and Peru are proof that implementations and Implementing Partners can adhere to best practices when outlined explicitly.

For further support, the pro bono Centre for Digital Public Infrastructure is always present to guide countries on the road to secure, scalable and inclusive DPI implementations.