MOSIP

DPI Safeguards: Building a Safe and Inclusive Digital Future

How MOSIP Aligns with the Universal DPI Safeguards Framework

About Modular Open Source Identity Platform (MOSIP)

MOSIP was incubated at IIIT-Bangalore as a core component of global Digital Public Infrastructure. The platform enables digital identity-led development and transformation for countries. With over 145 million people registered on MOSIP-based foundational ID systems around the world, our vision is to help build a digital future that is interoperable, inclusive, and based on trust.

MOSIP offers adopters the flexibility to design, build, and own critical software infrastructure for ID. The open source and open standards platform comes with a modular, configurable, and customisable architecture, built on the principles of security and privacy by design. With MOSIP, adopters can imagine digital ID as a foundational building block for governance, enabling greater access to government-to-citizen services.

Funded by the Gates Foundation, NORAD, Pratiksha Trust, and Tata Trust, MOSIP has engaged with 27 countries till date across Asia Pacific, Africa, Latin America, and the Caribbean.

About International Institute of Information Technology Bangalore (IIIT-B)

IIIT-B is a premier educational institute, located in the heart of Electronic City, Bangalore, India. Focused on Post-Graduate IT education and research, it contains state-of-the-art infrastructure, world-class faculty, a vibrant alumni community, cutting-edge research facilities, and close industry collaborations.

The institute's specially-designed courses ensure that students are cognisant of current technologies and practices, thereby equipping them with the tools and knowledge to solve real-world, contemporary problems. Since the founding of the institute in 1999, IIIT-B has enjoyed 100% placement every year, on account of the strong support of the industry and the growing base of talented alumni.

About Artha-India Research Advisors Pvt. Ltd.

Artha-India Research Advisors Pvt. Ltd. is a globally networked policy consulting organisation that partners with governments, multilateral agencies, philanthropies, and the private sector to address systemic challenges that hinder people's aspirations for shared prosperity and opportunity.

Over the coming decades, developing nations will undergo critical transitions as they urbanise, digitise, and formalise their economies—all while striving to deliver jobs and reduce emissions. These transformations will create tremendous opportunities but also present complex, multidimensional policy challenges. Addressing these requires new paradigms and interdisciplinary solutions that are deeply rooted in local context and informed by a nuanced understanding of the political economy of execution.

At Artha, we work alongside leaders to navigate these transitions and the opportunities and disruptions they bring, in order to secure long-term prosperity, social stability and the opportunity for each individual to achieve their full potential. Our approach blends rigorous research with a relentless focus on execution.

Disclaimer and Terms of Use

The analysis in this paper is a collaboration between the International Institute of Information Technology, Bangalore's MOSIP project, and Artha-India Research Advisors Pvt. Ltd.. The copyright of this paper is the sole and exclusive property of MOSIP, who commissioned this research from Artha-India. The work was supported by funding from EkStep Foundation. This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Authors

Arun Gurumurthy, MOSIP
Sasikumar Ganesan, MOSIP
Rohit Ranjan Rai, MOSIP
Sridhar Ganapathy, Artha-India Research Advisors

Attribution

Please cite the work as follows: "Gurumurthy A., Ganesan S., Rai R. R., Ganapathy S.. 2025. DPI Safeguards: Building a Safe and Inclusive Digital Future, How MOSIP Aligns with the Universal DPI Safeguards"

Acknowledgments

We would like to extend our sincere gratitude to Brinda Lashkari and Neha Jain from Artha-India Research Advisors Pvt. Ltd. for their support in our preliminary study to map the UN Safeguards Principles and Processes to MOSIP's practices.

Within the MOSIP team, we thank Ramesh Narayanan for his guidance throughout this exercise, as well as Sivanand Lanka, Vishwanath Vaidyanathan, Chaitanya Kesiraju, Mohanachandran S, Mahesh Binayak, Resham Chugani, Pragya Kumari, and Srija Gadamsetti, for their contributions in identifying and compiling the relevant documentation and features.

We would also like to thank Meghna Das, Tarun Cherian, Mahek Sarkar, and Niharika Sinha from the MOSIP Communications Team for shaping the narrative, and ensuring that the report communicates our findings with clarity and purpose.

This study has been a collective effort, and we appreciate the dedication, care, and expertise of all who contributed to it.

Table of Contents

Executive Summary

01 Background and Approach

02 MOSIP's Journey as a DPG and Foundational ID Provider

03 Mapping the DPI Safeguards to MOSIP

F2 - Do Not Discriminate

F4 - Reinforce transparency and accountability

F6 - Promote autonomy and agency

O2 - Evolve with evidence

O3 - Ensure data privacy by design

O4 - Assure data security by design

O5 - Ensure data protection during use

O6 - Respond to gender, ability, or age

O9 - Build and share open assets

04 Contributions to the Universal DPI Safeguards Framework

1. Key practices from the MOSIP platform submitted to Framework V1.0

2. Suggested feedback to processes and practices in the DPI Safeguardsframework

05 Looking Ahead: MOSIP's Plans and Commitments to Safety and Inclusion

Appendix

Table 1: Alignment of MOSIP to the following principles, processes and practices as a Tech provider

Table 2: Suggested Responsible Authority for key Framework practices

Executive Summary

The Modular Open Source Identity Platform (MOSIP), in collaboration with Artha-India Research Advisors (Artha) , conducted a study to assess how effectively the platform supports countries in aligning their Digital Public Infrastructure (DPI) with the recommendations of the UN Universal DPI Safeguards Framework, released in September 2024.

Both MOSIP and the DPI Safeguards Framework share a commitment to building safe, inclusive, and equitable DPI ecosystems. Our findings highlight strong convergence on foundational principles, including privacy protection, minimal data collection, and user control over personal information, underpinned by transparency, accountability, and active multi-stakeholder participation. To translate these principles into practice, MOSIP integrates capabilities such as differential privacy and zero-knowledge encryption to reinforce data security, while advancing interoperability and decentralisation through its modular open-source architecture and contributions to global standards.

A preliminary mapping exercise shows that, of the 43 recommendations across 9 principles of the Framework for technology providers, MOSIP's platform, processes, and practices align with over 30. In addition, MOSIP has provided inputs drawn from its engineering and technology practices for consideration in strengthening the UN Universal DPI Safeguards Framework.

MOSIP regularly works towards addressing the needs of countries and is committed to upgrading software to comply with global best practices and standards. However, it is important to note that, as a Digital Public Good, its role does not extend to implementation or assurance of these practices in deployed digital ID systems. The implementation, governance, and sustainability of such systems remain the responsibility of governments, system integrators, and other technical partners.

With advances in emerging technologies, MOSIP is exploring areas such as quantum-safe cryptography, general-purpose biometric devices, and decentralised service access to strengthen security and safeguard the inclusion of marginalised populations. The project is also pursuing ongoing efforts to enhance access, inclusion, and scalability.

Through this mapping process, MOSIP has identified certain recommendations from the Safeguards Framework to be taken up for rigorous review and possible implementation in its road map, ensuring that future developments remain aligned with global best practices and standards.

01 Background and Approach

The multi-phase and multi-stakeholder Universal DPI Safeguards initiative, stewarded by the UN Office for Digital and Emerging Technologies (ODET) and the United Nations Development Programme (UNDP), offers a pragmatic framework for countries seeking to implement Digital Public Infrastructure (DPI)[1].

In 2024, the Global Digital Compact (GDC) recognised both the transformative potential of DPI and the necessity of safeguards to ensure its responsible development and implementation. The Universal DPI Safeguards Framework (hereon referred to as the Safeguards Framework) was released with a set of actionable common guidelines for DPI design and implementation that serves public interest and ensures safe and inclusive adoption of DPI. In 2025, the Universal DPI Safeguards Framework will be implemented and evolved by ODET, guided by an iterative improvement process and feedback from global mainstreaming and country implementations.

MOSIP undertook a preliminary study to map the alignment between its ongoing efforts to advance safety and inclusion and the Safeguards Framework. **The purpose of this study was to inform and validate MOSIP's approach, and feed practical insights on the applicability of the Safeguards Framework to DPIs back into the framework evolution process.**

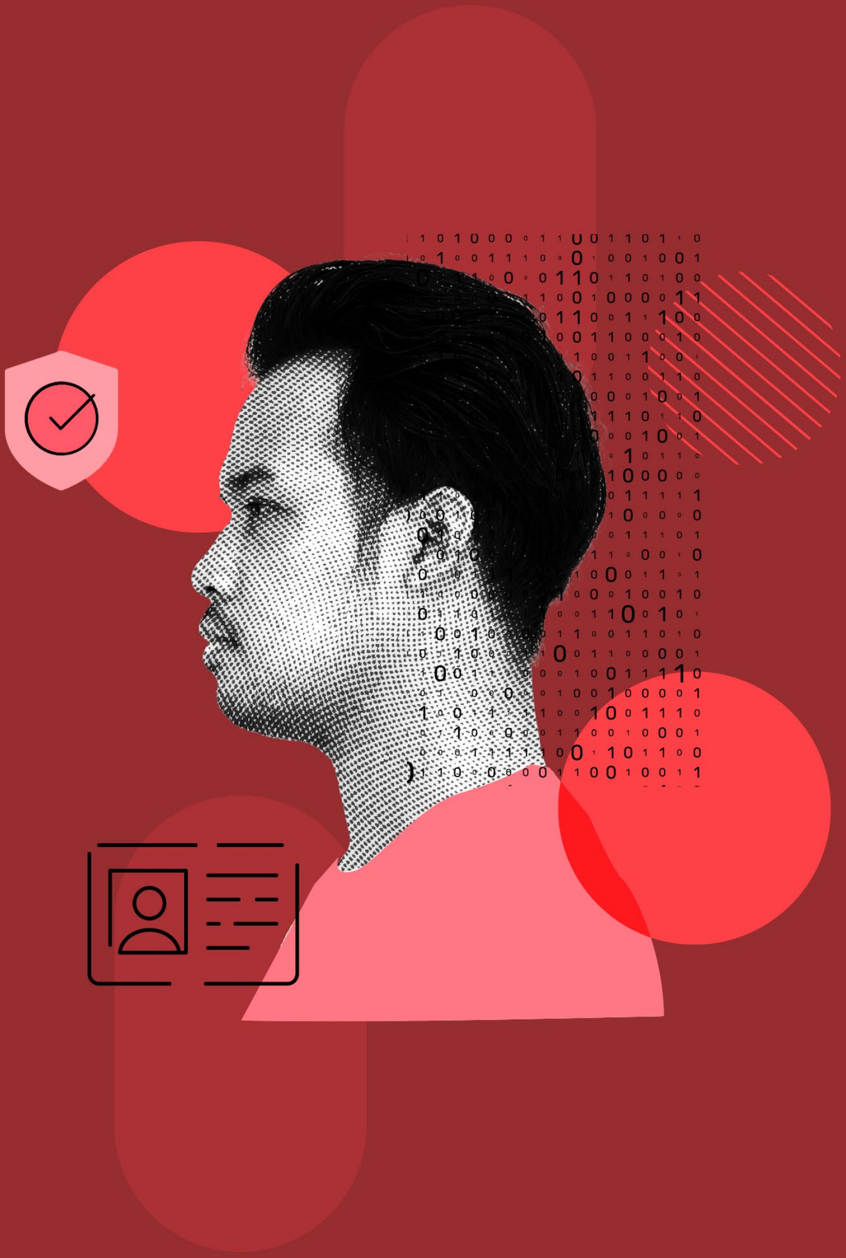
This report focuses on the subset of the Safeguards Framework recommendations (Version 1.0) that are relevant to technology providers, and specifically to MOSIP as a Digital Public Good (DPG). MOSIP's processes, practices, and principles, including software modules, technical standards, features, and engineering and development processes, were assessed through interviews with key personnel of the MOSIP team and review of publicly accessible documentation. The evaluation was based on the described practices available via the MOSIP Docs portal[2]; the underlying code implementing these practices was not assessed. Alignment with the Framework's processes and practices was determined based on the risks addressed and categorised as fully aligned, partially aligned, not aligned, or not applicable.

This document provides an overview of the MOSIP platform's alignment with the principles and processes set out in the Safeguards Framework, together with the project's inputs on its further refinement. These contributions include practices not yet reflected in Version 1.0 of the Safeguards Framework, as well as inputs on how the Safeguards Framework can better empower all stakeholders in the DPI journey of a country.

[1] Digital public infrastructure (DPI) refers to systems that serve as foundational, digital building blocks for public benefit. (Clark et al. 2025.Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1)

[2] https://docs.mosip.io/1.2.0 (accessed in February 2025)

02 MOSIP’s Journey as a DPG and Foundational ID Provider

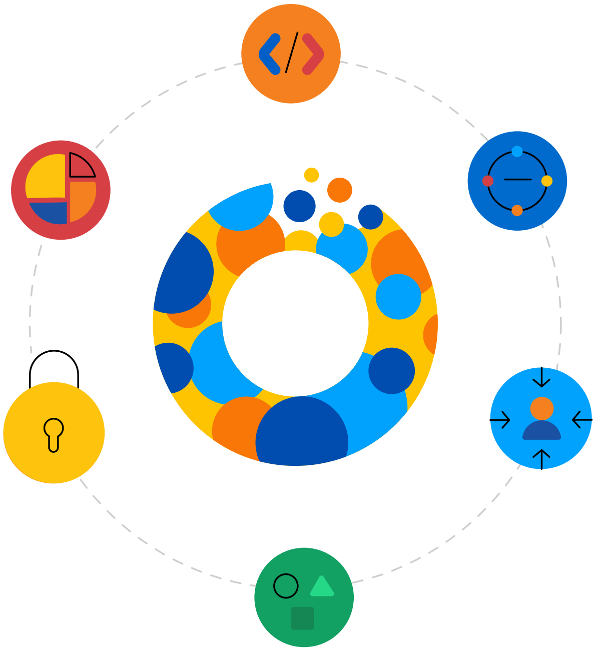


National identity systems can serve as critical enablers for delivering essential services, including financial assistance, healthcare, and social protection, improving access and outcomes for individuals. In recognition of this potential, MOSIP was established in 2018 to support the development, testing, and implementation of foundational ID systems. The MOSIP platform enables governments to adopt a new digital ID system or enhance existing systems while supporting a country's ownership over its digital infrastructure.

MOSIP Offers

- Technology to establish core digital ID infrastructure
- Ongoing tech support through issue resolution and bug fixes
- Training programmes for country officials
- Capacity-building initiatives to enhance stakeholder familiarity with systems, enabling country partners to adapt and modify their ID ecosystems in rapidly evolving digital environments

As a Digital Public Goods Alliance (DPGA) member, MOSIP complies with the Digital Public Goods Standard[3] and follows principles that align with the broader goals of openness, independence, interoperability, modularity, and security. Like all DPG providers, MOSIP develops software, built to comply with best practices and standards, and encourages the implementation and maintenance of these practices in the deployment of the software. However, DPG providers are not directly involved in the customisation or operation of these systems within countries; this responsibility rests either with a systems integrator acting on behalf of the government or with a designated public authority within the government itself. **MOSIP's guiding principles are designed to allow governments to build secure, inclusive and sustainable national ID systems. By ensuring that the governments retain full control over their digital system, MOSIP supports local innovation and long-term system sustainability, without ongoing dependency on the platform itself. These guiding principles are outlined below:**



Open-Source

MOSIP offers trusted and transparent technology. This gives a government greater control over its digital systems.

Modular

MOSIP offers a set of loosely coupled modules interoperating to provide the necessary functionalities of an ID system; this offers greater flexibility and control in the country context.

Vendor-Neutral

Vendor lock-in can limit flexibility and reduce government control over a system. MOSIP's architecture is designed to avoid such constraints, allowing governments to integrate with a broad range of compliant technologies.

Secure & Privacy Preserving:

MOSIP is built on cryptographic encryption and a privacy-by-design architecture to safeguard sensitive personal information. It minimises the storage of such data and ensures that all transfers occur only with explicit user consent.

Human-Centric

The MOSIP team learns from and incorporates on-the-ground resident experiences and realities to make systems more context-specific.

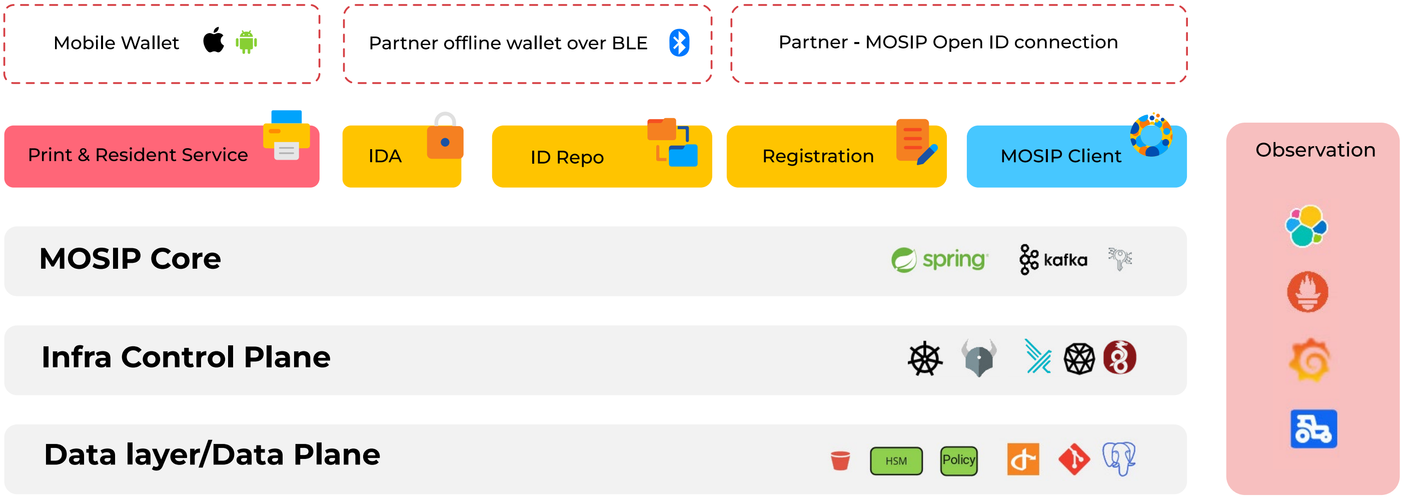
Inclusive

MOSIP's systems attempt to incorporate gender, race, and socioeconomic considerations while incorporating solutions to include users in low connectivity areas.

[3] The Digital Public Goods Standard is a set of specifications and guidelines designed to maximise consensus about whether a digital solution conforms to the definition of a digital public good. According to the UN Secretary General's Roadmap for Digital Cooperation, digital public goods are open-source software, open standards, open data, open AI systems, and open content collections that adhere to privacy and other applicable best practices, do no harm, and are of high relevance for attainment of the United Nations 2030 Sustainable Development Goals (SDGs).

Figure 1: MOSIP Architecture

Source: Compiled by the authors



LEGEND

- 🟨 Core components
- 🟥 Reference components
- 🟦 External component
- □ Partner components with reference implementation
- ⬜ Thirdparty components integrated to MOSIP
- ■ Observation plane

03 Mapping the DPI Safeguards to MOSIP

This study highlights a clear alignment between MOSIP's approach and the objectives of the Safeguards Framework in advancing safe, inclusive, and equitable DPI ecosystems. Both initiatives underscore the importance of safeguarding personal data and ensuring that digital systems are designed to serve the public interest. In line with these principles, MOSIP prioritises user privacy and data protection, at the core of its design and implementation philosophy.

The Universal Digital Public Infrastructure Safeguards Framework

Foundational Principles	Operational Principles
F1: Do no harm	O1: Leveraging market dynamics
F2: Do not discriminate	O2: Evolve with evidence
F3: Do not exclude	O3: Ensure data privacy by design
F4: Reinforce transparency and accountability	O4: Assure data security by design
F5: Uphold the rule of law	O5: Ensure data protection during use
F6: Promote autonomy and agency	O6: Respond to gender, ability or age
F7: Foster community engagement	O7: Practice inclusive governance
F8: Ensure effective remedy and redress	O8: Sustain financial viability
F9: Focus on future sustainability	O9: Build and share open assets

Source: The Universal DPI Safeguards Framework

The Universal DPI Safeguards Framework aims to establish actionable guidelines for implementing DPI that mitigates risks at both individual and societal levels, promotes multi-stakeholder engagement, and emphasises transparency, accountability, and inclusivity in the design and implementation of digital systems. Similarly, MOSIP encourages stakeholder participation to ensure that identity systems are responsive to the needs of diverse communities.

Both MOSIP and the Safeguards Framework advocate for minimal data collection practices and user control over personal information. MOSIP advocates collecting as little data as possible to allow a greater number of individuals to be brought into the digital economy.

MOSIP's commitment towards safety and inclusion is demonstrated through features/modules available in the platform and operational processes and practices that are followed in the development and evolution of the MOSIP platform. A preliminary mapping of these efforts to the Safeguards Framework reveals alignment of MOSIP's efforts to the Framework's recommendations for Technology providers, with 30 recommendations across 9 principles. Additionally, MOSIP's practices that employ differential privacy, zero-knowledge encryption and other techniques are provided as contributions to enrich the Framework.

The next section is a brief synthesis of the MOSIP platform's efforts to advance safety and inclusion and its alignment with the UN Universal DPI Safeguards Framework. For a detailed analysis of each principle, practice, and associated platform feature, please refer to Table 1 in the Appendix.

F2: Do Not Discriminate

Framework: The Safeguards Framework states the need to design and implement alternate processes for users who lack assumed documentation to register for a DPI.

MOSIP Platform: Countries typically require populations to show existing proof of address and identity when registering for a digital ID system. Strict processes designed to prevent fraud, such as mandating official documents like birth certificates, can sometimes exclude vulnerable populations who lack such documentation, especially in remote or underserved areas. To address this, the MOSIP platform allows alternative methods, such as introducers (community leaders) verifying identities of individuals.

MOSIP's systems are designed to support the inclusion of vulnerable populations. For instance, individuals with no documented proof can be included in the system using the introducer concept, where an individual or an organisation can vouch for the authenticity of informal information provided by an undocumented person. The system is sufficiently flexible to allow a family member to introduce their spouse or child. Additionally, MOSIP enables in-home registration for populations facing mobility challenges or belonging to communities with religious or cultural restrictions.[4] Although MOSIP offers these features, the decision to do so is the prerogative of the implementing country.

Critical Trade-Off between Ensuring Security and Achieving Complete Inclusion

It is critical to consider the trade-off between rules and requirements designed to ensure high accountability with the goals for greater inclusion.

A high bar for documentation requirements introduces friction and will result in exclusion (ex: proof of residential address may limit the ability of the homeless population or those living in informal settlements).

While relaxing such requirements may increase inclusivity, it also introduces a potential for fraud. We recommend that the implementers should prioritise inclusion — ensuring that all individuals are registered. Over time, ID systems can be fine-tuned to reduce this tolerance while maintaining coverage, gradually eliminating inaccuracies. The goal is to avoid overly stringent measures and processes that end up excluding individuals, particularly affecting the hard to reach rural or marginalised populations.

[4] See Table 1 (Item No. 30) : Design and implement alternate processes for users who lack assumed documentation.

F4: Reinforce Transparency and Accountability

Framework: The Safeguards Framework outlines the importance of managing access to databases and taking efforts to mitigate the risk of unlawful tampering and deletion of records.

MOSIP Platform: In the MOSIP platform, transparency and accountability are ensured through encrypted record storage and tamper-proof management of datasets. Audit records are generated at every instance of an update happening in the system, making unauthorised changes or deletions detectable. All authorised access to Personally Identifiable Information (PII) is through secure Application Programming Interfaces (APIs) alone, and with the data subject's consent and authorisation. The platform also allows data subjects to track the complete history of authentications and eKYC transactions performed.

F6: Promote Autonomy and Agency

Framework: The Safeguards Framework outlines the necessity of establishing secure data exchange protocols. To achieve this, it recommends updating systems to align with evolving legal requirements, encryption among databases, and implementing features to ensure user control over personal data.

MOSIP Platform: The platform design mandates obtaining of user consent when information is shared for the purpose of verification, typically during delivery of services. While the language of the consent is the prerogative of the implementing country, the design expectation is that consent is sought and captured to initiate data sharing.[5]

Safeguarding user data by providing control to users over their data is crucial. Inji, MOSIP's identity wallet and verifiable credentials tool, provides individuals with control over their data by enabling the decentralisation of ID verification processes.

Through Inji, identity credentials can be securely stored on the user's device or in a cloud wallet as verifiable credentials, rather than in a central database. Users retain granular control over what data they share, with whom, and for how long, using consent-based selective disclosure to reveal only necessary details. Inji employs strong encryption and cryptographic signatures, ensuring credentials are tamper-proof and verifiable even without internet connectivity. Additionally, users can revoke access or allow credentials to expire, preventing unauthorised or prolonged use.

O2: Evolve with Evidence

Framework: The Safeguards Framework emphasises the implementation of rigorous testing protocols to identify and mitigate any assumptions, mistakes, or design flaws in the development phase that could negatively impact users.

MOSIP Platform: MOSIP issues Quality Test Reports and Security Test Reports that contain the bugs and security vulnerabilities identified in various MOSIP modules.[6] These cover both web application and API testing scenarios. MOSIP publishes the reports of the findings, providing a description of the bug, priority level, severity level, the risk of it unfolding, and proposed recommendations to mitigate this risk. Moreover, MOSIP conducts regular vulnerability assessments to ensure that potential risks are identified and mitigated early.

All new or updated versions of the platform also undergo a go/no-go review, enabling the MOSIP team to make informed release decisions, monitor progress, and address any outstanding gaps or issues before deployment.

[5] See Table 1 (Item No. 29): Implement optional features for user control over personal data

[6] See Table 1 (Item No. 24): Implement rigorous testing protocols

O3: Ensure Data Privacy by Design

Framework: The Safeguards Framework prioritises the privacy of the users of DPI systems. It also recommends that DPI providers devise incident management and mitigation strategies and give more control to users by design.

MOSIP Platform: The MOSIP platform provides many alternatives for individuals to verify their identity. Apart from biometric authentication, additional modalities of authentication such as by email, mobile OTP, and demographic authentication.[7]

Data privacy requires sensitive data to be maintained and used safely without personal identifiers being exposed to vulnerabilities. The MOSIP platform by design maintains sensitive identity data in an encrypted form (in rest and in use). The platform's biometric device policy ensures that biometric authentication is secure, interoperable, and privacy centric. There are regular data integrity checks and alerts amongst other design principles and features.[8]

By evolving in line with emerging global data security and privacy best practices, MOSIP endeavours to provide a platform with updated security and privacy preserving features and processes (please refer to O2 Evolve with Evidence). The platform supports user control over their data, and enhances the ease of implementation of user control.[9]

The platform's tokenised ID authentication and verification along with safe authentication options (Yes/No, limited KYC), and through multi factor authentication functions, promotes minimal data being shared while achieving robust identity verification.[10] Through strict encryption protocols, federated database architecture, and anonymisation profile support, the daily interactions of users remain confidential and safe.[11]

The MOSIP platform provides the ability to perform analytics while protecting the privacy of individuals by deploying classifiers. This ensures that government agencies or organisations can get a sense of important statistics to encourage adoption among vulnerable populations, while preventing them from reverse-engineering or identifying any individual based on the data. This is because the classifier assigns a tag to an individual's data based on pre-set criteria and patterns without exposing sensitive personal details.

Data is encrypted and can only be accessed by those who hold the key or permissions to access the data. Such strict encryption restricts access and viewability to identity data. The lack of visibility of data – because of it being encrypted – and the limitations on the access of such data add friction to the possible aggregation of identity data of one individual.[12]

O4: Assure Data Security by Design

Framework: The Safeguards Framework provides several processes and practices for technology providers to strengthen data security such as maintaining standards for physical and database security or using established cyber security frameworks.

MOSIP Platform: The MOSIP platform is designed to facilitate secure data management, data handling, and data sharing processes and practices.

[7] See Table 1 (Item No. 11): Ensure that biometric authentication is not mandatory
[8] See Table 1 (Item No. 12): Address data leakage and unauthorised use with technical safeguards
[9] See Table 1 (Item No. 13): Develop privacy requirements and select mitigation strategies, documenting and iterating the analysis.
[10] See Table 1 (Item No. 14): Ensure unlinkability, unobservability, and zero-knowledge proofs are the default
[11] See Table 1 (Item No. 15): Ensure unobservability of daily user interactions by design
[12] See Table 1 (Item No. 15): Ensure unobservability of daily user interactions by design

Data is encrypted by default. While at rest, while in transit, and while being used. Anonymised profiles of end-users with limited data are created at different stages of the ID life cycle for policymakers and administrators to use data for monitoring, evaluation, and analysis.[13] This reduces exposure risks. Authentication in the platform does not require transmitting actual user data, except when KYC is required by law and policy. Even in this case, no biometric except facial image is transmitted.

The platform adopts a federated architecture to enhance privacy and resilience by distributing data and control, disallowing any aggregation or profiling of individuals. Sensitive data such as demographic and biometric information are distributed across different registries and are accessible only by specific API calls. Tamper-proof audit logs are maintained for accountability.

The platform team at MOSIP also conducts regular web application and API related security testing and issues a security test report.[14] (More about this in the principle 'Evolve with Evidence').

Key Management for Encryption

Secure key management is core for encryption to be effective as a security feature. The Keycloak and Key Manager modules[15] serve as the gateway to secure data authentication, access, and authorisation by safe management of the keys to encrypted data.

Keycloak's role-based access control ensures that only authorised users can access sensitive data (which remains encrypted while they use it), manage registrations, or perform other critical tasks, thus maintaining the system's integrity and security and preventing internal attacks and API misuse.

The Key Manager service provides all the cryptographic operations like encryption/decryption and digital signature/verification.

[13] https://docs.mosip.io/1.2.0/id-lifecycle-management/anonymous-profiling-support
[14] See Table 1 (Item No. 2): Implement a framework for safe data storage and processing
[15] https://docs.mosip.io/1.2.0/modules/keycloak; See Table 1 (Item No. 3): Implement data validation, completeness, and consistency checks.

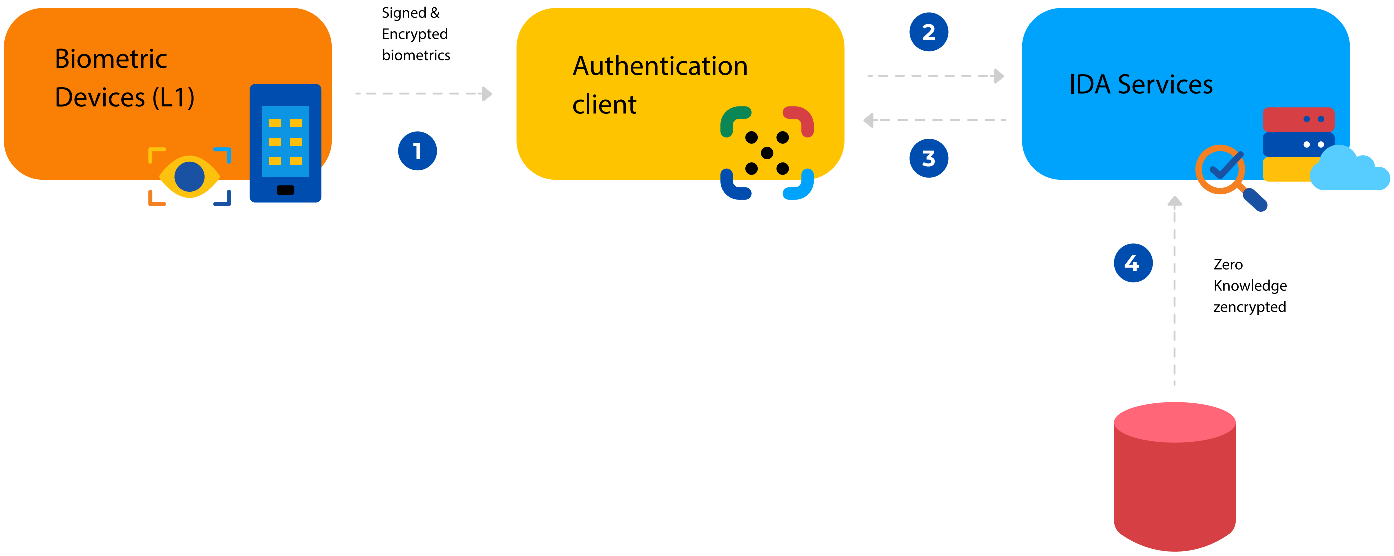
O5: Ensure Data Protection During Use

Framework: Data protection at every stage of the DPI life cycle is crucial and the Framework provides technology providers with guidance to ensure a user's data stays safe during collection, processing, and storage.

MOSIP platform: MOSIP, as a technology provider, aligns with the Safeguards Framework's recommended processes for data protection. MOSIP conducts regular security audits, data encryption and integrity checks on the platform, maintains data in a decentralised manner, maintains a discipline of continuous feature testing, security testing, performance testing, and monitoring.[16] Additionally, internal team building and training for data protection is provided by MOSIP. In MOSIP, data is encrypted at capture and remains encrypted throughout the data use lifecycle.[17] Any operation on data happens only in temporary memory and only upon specific requests through the API gateway. No data leaves the system without notifying the data subject. The administration of the MOSIP-based ID system happens in a zero-knowledge approach, where system administrators do not have access to PII while operating their identity system.

Figure 2: ID Authentication Flow

Source: MOSIP Docs 1.2.0, Data Protection



[16] See Table 1 (Item No. 21): Conduct regular security audits to check encryption protocols
[17] See Table 1 (Item No. 15): Data is protected in flight and rest using strong cryptographic techniques

O6: Respond to Gender, Ability, or Age

Framework: The Safeguards framework highlights the importance of ensuring products are designed with inclusive features that cater to the needs of vulnerable populations.

MOSIP Platform: MOSIP has taken multiple steps to ensure the incorporation of inclusive design features into the platform. In remote regions that face significant internet connectivity issues, MOSIP leverages unstructured supplementary service data (USSD) that allows users to access critical information using feature phones, by bypassing the need for advanced smartphones and internet connectivity.[18] MOSIP partnered with researchers at the Oregon State University to apply their gender-inclusiveness magnifier[19] that enables gender-inclusive design and software development in MOSIP modules, by identifying and fixing any features creating barriers to access to women, and actively engaging in gender sensitive software development.[20]

O9: Build and Share Open Assets

Framework: The Safeguards framework emphasises the importance of interoperability, so that data and information are understood consistently across various systems and even sectors. It also prioritises knowledge sharing and collaboration among governments, industry stakeholders, and civil society to promote the development and adoption of DPI and DPGs.

MOSIP Platform: MOSIP is built on a modular, microservices-based architecture, which enables interoperability across digital identity systems, allowing seamless integration with various applications and services. One example of this is eSignet, which supports multiple authentication methods and allows users to present their identity across usage scenarios while maintaining privacy and security. By leveraging open standards and a modular architecture, MOSIP ensures that identity systems built on its framework can interact with other DPI, facilitating cross-border recognition, e-governance services, and financial inclusion.

MOSIP introduced the MOSIP Partner Programme to help stakeholders connect with MOSIP, and become part of an ecosystem invested in building foundational digital ID systems that are trustworthy, secure, efficient, and interoperable, while being customised to specific needs.[21]

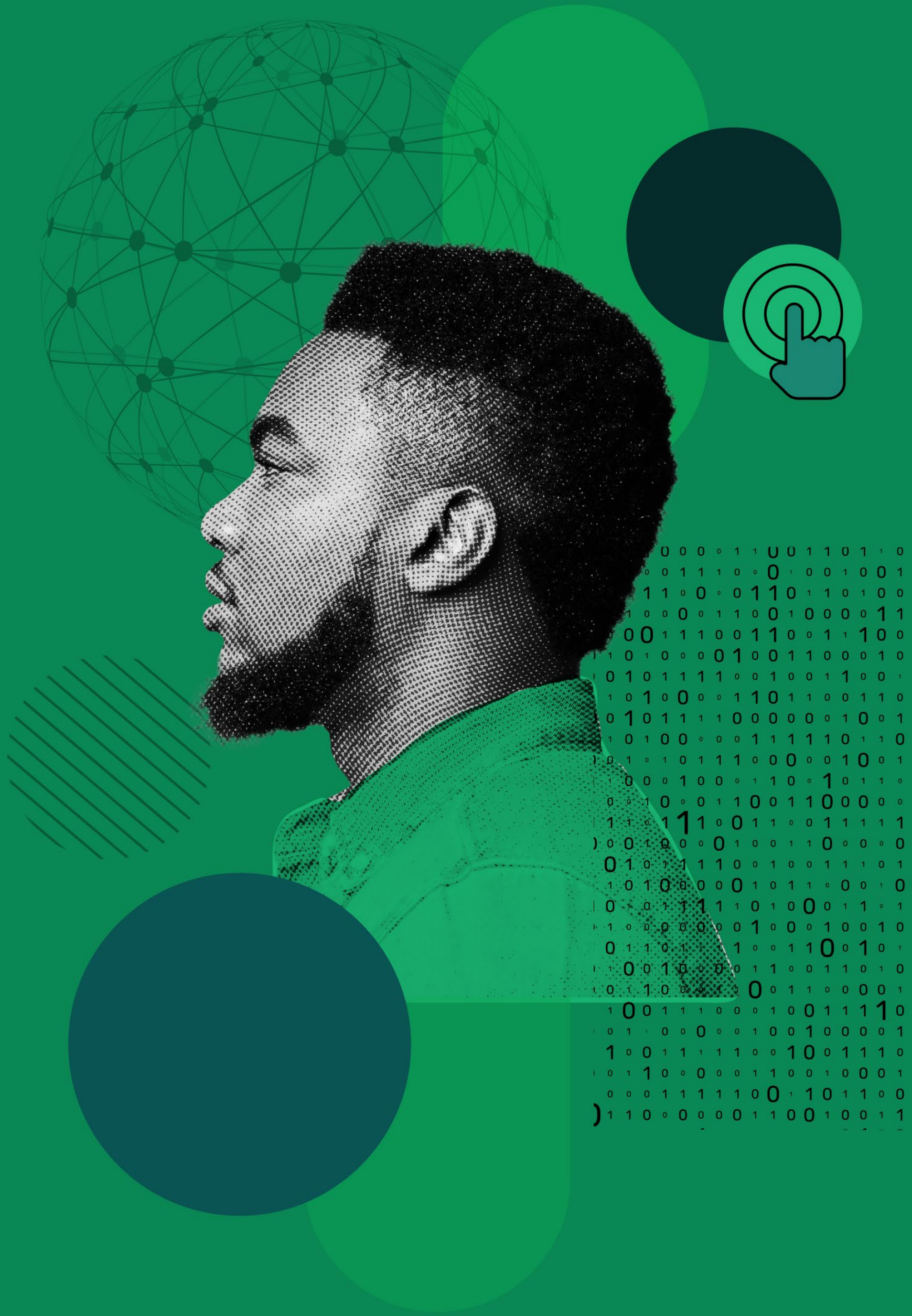
[18] In regions that have a large digital divide, unstructured supplementary service data (USSD) allows users to access critical information by bypassing the need for advanced technology. MOSIP collaborated with the National ID Program, Ethiopia (NIDP) platform called Fayda. The initiative showcases how USSD can be utilised to provide critical Fayda services efficiently even in regions with limited technological resources. MOSIP proposes enabling features such as registration status checks, virtual ID generation, retrieval of lost UINs, language support/selection, and reporting of life events, including registration for maternity care, childbirth, and marriage using USSD based technology.

[19] MOSIP partnered with researchers at Oregon State University (OSU) to leverage the GenderMag methodology developed by the team at OSU. GenderMag, also known as the Gender-Inclusiveness Magnifier, is a usability inspection method to find and fix gender-inclusivity bugs in problem-solving software. It brings in inclusivity in four areas: administration, process, APIs, and in the UI/UX.

[20] See Table 1 (Item No. 18): Establish robust data delinking mechanisms once the purpose of the processing of personal information has been served; Implement strict controls to enforce purpose limitation and restrict secondary data use; Integrate strict data anonymisation protocols into design; Ensure unobservability of daily user interactions by design.

[21] See Table 1 (Item No. 10): Ensure that semantic interoperability is emphasised, so that data and information are understood consistently across various systems.

04 Contributions to the Universal DPI Safeguards Framework



1. Key Practices from the MOSIP Platform, Submitted to Framework V1.0

The Safeguards Framework sets out several key processes and practices for building secure and inclusive digital systems. MOSIP, with its experience in developing safe and inclusive technology that is being tested across 27 countries and used by over 145 million residents globally, has identified a few practices that can enrich the DPI Safeguards Framework and provide practical guidance to technology providers in the DPI ecosystem. Five such practices are outlined below, mapped to the relevant processes in the Framework.

1. Safeguards Process: Ensure secure and auditable data handling

MOSIP's Practice:

a. **Anonymous Profiling Support:** The basic guideline followed to create anonymised profiles is that no dataset should violate the privacy of the person or point to specific individuals without their involvement.

b. **Data Access Control:** Sensitive data in MOSIP is encrypted in the database, making APIs the only entry point for accessing information. Keycloak enforces strict authentication and authorisation policies, preventing internal attacks and API misuse, and ensuring zero-knowledge administration of the system.

c. **Ensuring Quality via Operator Onboarding:** Maintaining quality and accuracy during user registration in foundational identity systems is essential. Operators are individuals stationed at registration centres to register new individuals. 'Operator Onboarding' involves registering trusted and trained operators within the ID system, contingent upon their prior registration and possession of a valid Unique Identification Number. Personnel are prompted to provide their biometrics and finalise the onboarding process. This ensures that the registration client can only be accessed and edited by people registered as operators, adding a layer of security and trust. Through this process, MOSIP-based systems verify that the operator entering data into the ID system is a trained individual, which safeguards the system against fraudulent or flawed data. Onboarding operators with biometrics provides accountability, ensuring that any fraudulent activity is traced back to the personnel involved in the registration process.

2. Safeguards Process: Implement a framework for safe data storage and processing

MOSIP's Practice:

Go/No-Go Call: Before any project or module is approved for release, it must meet defined criteria through a structured Go/No-Go call. The go/no go call ensures that no update/release contains bugs that could compromise safe data storage and processing.

3. Safeguards Process: Use an established cybersecurity framework

MOSIP's Practice:

Support for transparent revocable ID: users can revoke that ID and move to a new ID without any relying party being aware of the change. Internal tokenisation necessary for this is handled by MOSIP.

4. Safeguards Process: Design and implement alternate processes for users who lack assumed documentation

MOSIP's Practice:

At-home registration for vulnerable populations, introducer based enrolment, and biometric exception process.

5. Safeguards Process: Establish robust data delinking mechanisms once the purpose of the processing of personal information has been established

MOSIP's Practice:

The ID Authentication module (IDA) is an independent module and may be hosted by several providers. IDA hosts all the biometric templates and demographic data. Unique additional protection is provided here to make sure that mass decryption of user data is very difficult to achieve. The data can only be decrypted if the user's Unique Identification Number (UIN) is provided.

2. Suggested Feedback to Processes and Practices in the DPI Safeguards framework

The Safeguards Framework V1.0 provides 85 practices covering 32 key processes in the DPI lifecycle for technology providers.

The 'Technology provider' group includes actors such as solution vendors, systems integrators, DPG providers and other stakeholders operating in the DPI ecosystem who are the focal point for technological work on risk identification and mitigation, ranging from advisory to actual maintenance and support of DPI . While DPG providers design technology solutions that embed principles of transparency, accountability, and compliance, the authority to activate and enforce these mechanisms is typically the responsibility of the government, supported by system integrators (SIs) and other technical vendors. As a result, the influence of DPG providers over aspects such as upholding the rule of law, ensuring mechanisms for redress, and continuously updating of compliance practices to align with evolving legal and regulatory requirements is inherently limited. Our suggested modifications are of two types outlined below:

1. The Safeguards Framework V1.0 contains 26 practices tagged to Technology Providers that would be more appropriate for governments and systems integrators. The table provides a listing of the Safeguards process and practices and suggests a suitable Responsible Authority (lead stakeholder) for the practice. A brief rationale for the suggested change is provided below:

Excerpt from Table 2 [See Appendix]

Safeguards Principle	Safeguards Framework Process and Practice	Suggested Responsible Authority	Rationale
Ensure data privacy by design	**Framework Process:** Implement and maintain comprehensive cybersecurity measures. **Framework Practice:** Use network segmentation to isolate critical systems and limit the spread of potential breaches.	Systems Integrator	The platform architecture can safeguard the data, as MOSIP does, by storing biometrics and demographic data separately to minimise spread of potential breaches but cannot control network design in an implementation.
Ensure data privacy by design	**Framework Process:** Establish mechanisms to ensure a right to opt-out whenever appropriate. **Framework Practice:** Collaborate with regulators to ensure that the opt-out mechanisms developed are aligned with legal requirements and that they provide clear, transparent options for users to manage their data preferences effectively.	Government	The DPG provider can ensure that their solutions provide clear, transparent options for users to manage their data preferences. However, the decision to implement this is a policy consideration and rests with the implementing authority.

2. These 26 practices can be reframed to clarify actions pertaining to technology providers in designing, building or developing technical features or modules to support implementation of the operational principles of the Framework. If necessary, the policy/implementation prerogatives of the same principles can be reiterated in the relevant categories

05 Looking Ahead: MOSIP’s Plans and Commitments to Safety and Inclusion

MOSIP is continually adapting to the needs of countries and to advancements in emerging technologies. Current areas of focus include quantum-safe cryptography to future-proof security, general-purpose biometric devices to support individuals without smartphones, and decentralised access to services to strengthen privacy while broadening the use of identity verification. The sections below discuss a few of these ongoing efforts in greater detail.

Access

Offline authentication innovations

The practice of carrying paper-based IDs is normal and practical. While future generations may rely less on paper, it remains essential for many today. For instance, when traveling, a dead phone battery can make digital solutions impractical. Additionally, older generations often find paper easier to use than documents stored in smartphones. Behaviourally, a printed document in a file is straightforward to share and process, especially in formal settings like handing it to a government functionary in any interaction.

Ongoing experimentation focuses on enhancing tools to bridge the gap between paper-based and digital systems by incorporating features like facial recognition into physical documents. This approach aims to maintain the practicality of paper while improving its reliability and usability.

Biometric-based authentication such as facial authentication offers the highest level of assurance as it assures the presence of the individual. Offline authentication, however, presents challenges in maintaining a similarly high level of assurance. For instance, in a cross-border scenario, remote areas often face significant internet connectivity issues. Even when internet access is available, server reliability may be inconsistent. To tackle this challenge, MOSIP proposed a standard CBOR-based QR Code that involves embedding a low-resolution image of the person with a minimal demographic dataset within the QR code. This QR code would be digitally signed by the ID authorities (Issuer) and then printed on a physical card. Subsequently, the signed data within the QR code can be utilised for facial authentication.

Inclusion

Age-based credential attributes

- Dynamic Age Verification in Credentials: Implementing support for age attributes in Verifiable Credentials (VC) to enable real-time age-based validations, such as "is_above_18" or "is_above_65," based on the current date.
- Integration with Wallet and Verified Claims: Ensuring seamless utilisation of age attributes for Wallet-based verifications and claims to enhance user experience and compliance with age-specific requirements.

Scale

MOSIP’s objective to make its platform available in countries with small populations and low resources is being accomplished through planned software optimisations and reducing hardware requirements where feasible.

Recommendations from the Safeguards Framework for further action from MOSIP

Through the mapping process MOSIP has identified certain process inputs which the project has taken up for rigorous review and possible implementation in its road map. Below are some examples of processes identified for action:

- Regularly revisit and refine privacy requirements and mitigation strategies to ensure they remain effective.
- Conduct regular audits to verify compliance with data protection regulations, ensuring that consent workflows and security measures are continually updated to meet evolving legal requirements and industry standards.
- Use established categories such as those from LINDDUN or other privacy threat modelling frameworks to systematically identify where privacy risks may arise within your system.
- Integrate zero-knowledge proof protocols to allow for the verification of transactions or identities without revealing any unnecessary information. (This is separate from zero-knowledge administration).
- Develop customisable data control features such as consent management tools and privacy settings, allowing users to adjust their data sharing preferences easily, like GDPR-compliant consent dashboards: the dashboard does not exist in MOSIP’s current practices.

Appendix

Table 1:

Alignment of MOSIP to the following principles, processes and practices as a Tech provider

	Safeguards Principle	Framework Process and Practice	MOSIP <> Framework Alignment
1	**Assure data security by design**	**Process:** Ensure secure and auditable data handling **Practice:** Adopt a federated and decentralised architecture to enhance privacy and resilience by distributing data and control.	Access to data is limited to pre-defined roles and access by such roles is audited (Role based access controls). Administrators can monitor and control access permissions centrally via Keycloak, providing visibility into who can access what within the system. Data that identifies individuals is maintained in a de-centralised manner, disallowing any aggregation or profiling of individuals. Tamper proof audit logs are maintained for accountability.
2	**Assure data security by design**	**Process:** Implement a framework for safe data storage and processing. **Practice:** Use Role-Based Access Control (RBAC): Set up RBAC to limit data access based on user roles and responsibilities. **Practice:** Schedule regular penetration tests to identify and fix vulnerabilities in data storage and processing system	MOSIP's Internal security practices, integrated in the platform's development lifecycle, include rigorous threat modelling, secure coding practices, comprehensive code reviews, and continuous vulnerability assessments to ensure that potential risks are identified and mitigated early. By embedding these security measures during development MOSIP fosters a proactive security culture that not only minimises vulnerabilities but also supports a robust defence strategy throughout the system's lifecycle. MOSIP also releases Security Test Reports that contain all the security bugs that were identified in various MOSIP modules (a combination of both web application and API related security testing scenarios). Other practices include role-based access control and a Go/No-Go checklist requirements before release.

3	**Assure data security by design**	**Process:** Implement data validation, completeness, and consistency checks **Practice:** Implementation of robust data validation and backup through ensuring data integrity and authenticity through advanced methods. This can be done through: - Regular data backups. - Advanced validation methods. - Completeness and consistency checking. - Use of cryptographic signatures for data authenticity..	All data packets and APIs are digitally signed to ensure authenticity and integrity. This prevents tampering with data during transmission or storage. The platform implements strict access controls via APIs, ensuring that only authorised personnel can access specific data. Rate limiting and API authentication further protect against unauthorised access. Data is stored in a distributed manner across relational databases and object storage, ensuring redundancy and availability.
4	**Assure data security by design**	**Process:** Safeguard user data through heightened user control and accountability **Practice:** Provide multiple platforms for users to understand and manage consent so that those with lower literacy and tech access can do so independently. **Practice:** Train staff and relevant partners to ensure a common understanding of internal data use and sharing policies, but also universal recognitiown of their importance. **Practice:** Provide users flexible access to and ownership of their data after they provide consent, thereby respecting users’ rights to revoke access.	Inji enables secure issuance, digitalisation, storage, exchange and seamless verification of trusted data as verifiable credentials. It enables consent driven data sharing by allowing users to control who they wish to share their identity information with. MOSIP also takes up the role of building awareness on data privacy and security through its country based specialised workshops.

5	**Assure data security by design**	**Process:** Use an established cybersecurity framework **Practice:** Implementations have adequate and effective safeguards against unauthorised access, tampering (alteration or other unauthorised changes to data or credentials), identity theft, misuse of data, cybercrime, and other threats occurring throughout the DPI life cycle.	For any report of lost identity or detection of fraudulent activity, the module can require temporary suspension of authentication activities on a user. This is enabled by the hotlisting feature. The authentication service checks if the identifier used is hotlisted and if so, the authentication process is aborted and fails. The hotlisting service can be used by helpdesk and anti-fraud solutions to list and delist the identifiers that need to be blocked temporarily. Tampering and identity theft: MOSIP by design also does not allow access to any database without relevant credentials: there is no option to make search-based API calls to the database. All relying parties get privacy enabled tokens to prevent profiling across transactions. Permanent ID is never shared. Segregation of biometric & demographic data in storage reduces harms of breaches and chances of data-based profiling.
6	**Assure data security by design**	**Process:** Ensure secure and auditable data handling **Practice:** Utilise tokenisation and data masking, implement granular electronic consent frameworks, enforce end-to-end encryption, and employ digital signatures and verifiable credentials to ensure robust, auditable, and trustworthy data management and transactions.	MOSIP uses zero-knowledge encryption through which unique additional protection is provided to ensure that mass decryption of user data is difficult to achieve. The data can only be decrypted if the user's UIN is provided. All sensitive data in MOSIP systems is encrypted in the database, making APIs the only entry point for accessing information. Keycloak enforces strict authentication and authorisation policies, preventing internal attacks and API misuse (Keycloak acts as the Identity and Authentication Management system, handling user authentication and authorisation for the platform's microservices. It ensures that only authorised users can access specific modules and data) Anonymised profiles are created at different stages of the ID life cycle for data usage, monitoring, evaluation, and analysis. This ensures that the limited dataset does not violate the privacy of the person or point to specific individuals, reducing the risk of exposure.

			In certain contexts, identity verification can be performed anonymously for one-time use. However, when identity verification is tied to transactions requiring identity verification, it becomes necessary to link the user's identity to the transaction. This is done by providing relying parties with a "sticky" token identifier (persisting a user within the particular system for better service delivery), which can serve as a reference ID for the individual in their system. When authentication is successful, the APIs return a token. Depending on the relying party's policies, the token may be random or "sticky."
7	**Build and share open assets**	**Process:** Ensure modularity and reusability across sectors, enabling evolution with society by unbundling DPI into core components (e.g., digital identity, payments, data sharing) **Practice:** Implement standardised APIs and protocols that enable different modules to communicate and integrate with existing systems across sectors.	MOSIP is built on a modular, microservices-based architecture, and most MOSIP modules are designed as robust foundational infrastructure components, making them suitable for integration into various projects across sectors. Some core components of MOSIP can be used independently, and are designed to be deployed to add particular capabilities to existing systems.
8	**Build and share open assets**	**Process:** Ensure modularity and reusability across sectors, enabling evolution with society by unbundling DPI into core components (e.g., digital identity, payments, data sharing) **Practice:** Design DPI modules with cross-sector usability in mind, ensuring that they can be reused in different industries.	Modules built by MOSIP are adopted by multiple DPGs, DPI's and industries. MOSIP publishes all forms libraries in multiple programming languages to reduce adoption barriers. MOSIPs reference implementation, Inji, enables access to essential services— healthcare, financial inclusion, global mobility, and social support. Its features also include the interoperability necessary for seamless and secure credential verification, which can be used across sectors.

9	**Build and share open assets**	**Process:** Ensure that semantic interoperability is emphasised, so that data and information are understood consistently across various systems. **Practice:** Creating shared data dictionaries, ontologies, and common data models to ensure consistent understanding of exchanged information.	MOSIP is built using globally accepted open standards, which facilitates interoperability by ensuring that data formats and protocols are consistent across different systems. This adherence to standards helps in maintaining the meaning of data during exchange. Examples of how the MOSIP platform's schema and MOSIP's device standards are adopted across industry: Secure Biometrics Device Interface Specification: This standard specifies a language-agnostic protocol and corresponding interfaces for biometric devices to support features such as the discovery of devices, capability exposure of the device, and capture of biometrics using the device for all instant capture modalities. This protocol also specifically addresses the trustworthiness of both the device and the captured data, in addition to data security.
10	**Build and share open assets**	**Process:** Ensure that semantic interoperability is emphasised, so that data and information are understood consistently across various systems. **Practice:** Establish cross-organisational collaborations and training programs to equip stakeholders with the necessary skills and knowledge.	The MOSIP Partner Programme (MPP) was initiated to help stakeholders connect with MOSIP, and become part of an ecosystem invested in building foundational digital ID systems that are trustworthy, secure, efficient, and interoperable, while being customised to specific needs. The MPP helps **create, build, and sustain relationships** with stakeholders in an ever-expanding industry of digital technology. It is supported by a robust and systematic framework that opens opportunities for knowledge transfer and community events, including webinars and conferences.

11	**Ensure data privacy by design**	**Process:** Ensure that biometric authentication is not mandatory **Practice:** Design features that offer users alternative authentication methods besides biometrics, such as passwords, tokens, or multi-factor authentication, to ensure user choice and privacy. **Practice: Design** DPI that allows users to opt out of biometric authentication without losing access to essential services, maintaining inclusivity and accessibility.	MOSIP is designed to provide alternative options of identity capture and authentication. The authentication APIs enable MOSIP to offer multifactor authentication: • **Biometric:** Finger, face, iris • **Demographic:** Name, date of birth, age, gender, etc. • **One-Time Password (OTP):** Based on the level of assurance needed for the transaction, the relying party can decide which factors are sufficient for identity verification. • **Password-based authentication.** MOSIP enables and empowers users to opt out from biometric authentication, but the decision to implement such policies rests with the adopter (during implementation).
12	**Ensure data privacy by design**	**Process:** Address data leakage and unauthorised use with technical safeguards. **Practice:** Consider wider scenarios for data leakage. **Practice:** Analyse stakeholder interests and concerns. **Practice:** Implement differential privacy or synthetic data.	MOSIP design assumes the worst might happen; thus, it has built-in mechanisms to prevent and recover from any such data leakage: 1. No access to database without authenticated API calls 2. Encrypted data at rest and in flight 3. Integration with trusted applications only, under specified policies 4. Fraud avoidance: association of authentication only with specific transactions 5. Misuse prevention: users can lock or unlock their authentication 6. Virtual ID and Tokens to prevent identity theft 7. All data sent out of MOSIP will be digitally signed 8. All incoming data will be signed by the respective entity 9. Any data sent to a relying party will be encrypted 10. Protection against internal attacks with every record in DB protected with integrity 11. Centralised key management 12. All APIs are protected with OAUTH 2.0

13	**Ensure data privacy by design**	**Process:** Develop privacy requirements and select mitigation strategies, documenting and iterating the analysis. **Practice:** Create a data flow diagram to map the system's entities and processes, identify privacy threats using established categories, and assess risks. **Practice:** Regularly revisit and refine your privacy requirements and mitigation strategies to ensure they remain effective.	MOSIP's privacy protection measures include data protection, transparency, user control, confidentiality, selective disclosure, user anonymity and intrusion protection. Identifying and protecting essential assets needs a systematic approach that incorporates adequate security controls. This is facilitated by threat modelling the three stages of the MOSIP system. Firstly, MOSIP breaks the system down into subsystems and visualises it using data flow diagrams. Secondly, MOSIP uses STRIDE/DREAD to do threat analysis and risk assessment on the selected assets. Finally, the team suggests effective countermeasures based on the quantified risks.
14	**Ensure data privacy by design**	**Process:** Ensure unlinkability, unobservability, and zero-knowledge proofs are the default. **Practice:** Requests for information can be refused, complied with fully, or partially, with zero-knowledge proofs used to verify information without transferring personal data. **Practice:** Design technical systems to protect user interactions from being correlated across different relying parties, unless the user provides their consent **Practice:** Ensure that DPI operators cannot gain knowledge of user behaviour or interactions without explicit user consent, using techniques like encryption and anonymisation to safeguard privacy.	Unlinkability is established using tokenised ID (PSUT) rather than a permanent ID. Alternatively, the country can choose to use the Yes/No Authentication where the relying party has to collect all the user information with his consent and can send it to MOSIP for verification. The platform returns just Yes/No if the given information is correct. Both measures enable unlinkability and partial knowledge. Alternatively, login using QR code provides a cryptographic key based login with no personally identifiable information.

15	**Ensure data privacy by design**	**Process:** Ensure unobservability of daily user interactions by design **Practice:** Use advanced anonymisation methods, such as differential privacy or data masking **Practice:** Employ decentralised data storage solutions to distribute data across multiple nodes, reducing the likelihood that any single entity can observe or track user interactions. **Practice:** Integrate zero-knowledge proof protocols to allow for the verification of transactions or identities without revealing any unnecessary information.	Data masking and data anonymity are maintained. By default, all data is encrypted. For better reporting and analysis, MOSIP introduced anonymous profile support that provides unlinkable and anonymous reports and data. MOSIP's Inji credential stack, Claim 169, Openid4VP-BLE are projects that aim to help unobservability. MOSIP provides the necessary tools and standards to help countries and residents achieve this. To secure user data, data is protected in flight and rest using strong cryptographic techniques. All operations on decrypted data are done in temporary memory).
16	**Ensure data privacy by design**	**Process:** Provide features to protect users against tracking and profiling **Practice:** A user interacting via DPI with other parties is protected from tracking and profiling by privacy-enhancing technologies like pairwise-pseudonymous identifiers, zero-knowledge proofs and unlinkability.	1. Virtual ID/Handle enables residents to protect their actual ID with a revocable ID. 2. Token ID (PSUT - Partner Specific User Token): The Token identifier/PSUT is a system provided customer reference number for relying parties to uniquely identify the users in their system. The token identifier is an alias meant for the partner/ relying party typically unique (Configured through PMS policy, in case uniqueness is not needed, partner policy can be set to provide a random number) to them. This identifier is included in the response of the authentication transactions. One key differentiator is that the PSUT is not accepted as an identifier for authentication transactions.

17	**Ensure data privacy by design**	**Process:** Implement strict controls to enforce purpose limitation and restrict secondary data use. **Practice:** Design DPI systems to enforce data processing strictly according to the predefined purposes.	The MOSIP platform has only authentication and e-KYC APIs and has no search APIs. As an identity system it controls only the user verification and does not collect nor process any other data.
18	**Ensure data privacy by design**	**Process:** Establish robust data delinking mechanisms once the purpose of the processing of personal information has been served **Practice:** Use automated scripts that routinely delink identifiers from datasets after data processing is complete, as practiced in some Nordic countries' privacy frameworks. **Practice:** Implement temporary session identifiers in online services that expire after the session ends. Pairwise pseudonymous identifiers should be used wherever possible to prevent correlation of user data across interactions.	The MOSIP platform maintains no links and everything is encrypted and secured or anonymised. Multiple handles/virtual id can be used. Virtual ID is pseudonymous and random. The handles are user provided alias names for their UIN. In the database every VID/handle is a new encrypted anonymous record. The ID Authentication module (IDA) is an independent module and may be hosted by several providers. IDA hosts all the biometric templates and demographic data. Unique additional protection is provided here to make sure that mass decryption of user data is very difficult to achieve. The data can only be decrypted if the user's UIN is provided.
19	**Ensure data privacy by design**	**Process:** Integrate strict data anonymisation protocols into design **Practice:** Implement methods where direct identifiers are removed or replaced with pseudonyms.	MOSIP platform maintains no links, and data is encrypted and secured or anonymised.

20	**Ensure data privacy by design**	**Process:** Implement strict controls to enforce purpose limitation and restrict secondary data use. **Practice:** Design tools that require explicit user consent for any data use beyond the initially stated purpose	The MOSIP platform has only authentication and e-KYC APIs and has no search API. As an identity system it controls only the user verification and does not collect nor process any other data. Encryption in IDA is designed to require the user's UIN/VID/handles.
21	**Ensure data protection during use**	**Process:** Conduct regular security audits to check encryption protocols **Practice:** Train the technical teams on the importance of strong encryption practices and the potential risks of outdated or weak encryption methods **Practice:** Document the results of security audits and encryption checks, and make necessary adjustments to improve the system's security posture **Practice:** Implement automated monitoring tools to continuously check for vulnerabilities in encryption implementations and to ensure compliance with the latest security protocols.	The platform is designed on open source code and is openly available on GitHub. The openness of code keeps the MOSIP platform transparent and open to scrutiny. Security Test Report: This report contains all the security bugs that were identified in various MOSIP modules. This is a combination of both web application and API related security testing scenarios. Go/No Go Release Checklist: The Go/No-Go checklist delineates the criteria that must be satisfied for the project/ modules to be approved for release. It enables stakeholders to make informed decisions regarding the status and progress of the release, as well as identify any gaps or missing items.
22	**Ensure data protection during use**	**Process:** Ensure digital preservation of records **Practice:** Create a migration plan for digital records to ensure they remain accessible as technologies evolve.	The MOSIP platform runs on a strict data migration and maintenance discipline. With each version released, the platform permits only data packets that are verified in format and follow the MOSIP data standards through the registry database. Availability of data is permitted only by parties who have the relevant permissions or keys to access the relevant data.

23	**Ensure data protection during use**	**Process:** Implement regular performance metrics tracking with predefined response protocols **Practice:** Develop and monitor key performance metrics related to data protection, such as response times to security incidents, system uptime, and encryption effectiveness. **Practice:** Establish predefined response protocols that detail immediate actions to be taken when performance metrics fall below acceptable thresholds, ensuring quick and effective resolution of issues. **Practice:** Implement automated alerts for anomalies.	Performance Test Report: The MOSIP platform provides details on the performance measurement approach of prioritised scenarios of MOSIP modules and provides detailed reports on the results. This metric is published and is used by the countries to determine the necessary hardware.
24	**Evolve with evidence**	**Process:** Implement rigorous testing protocols **Practice:** Implement rigorous testing protocols to identify and mitigate any assumptions, mistakes, or design flaws in the development phase that could negatively impact users.	The platform has three specialised test rigs for automation testing. • The **UI test rig** ensures thorough validation of web-based application modules, including Admin UI, PMP UI, and Resident UI. • The **Domain-Specific Language (**DSL) test rig facilitates end-to-end testing of MOSIP including functionalities like registration and authentication. • The **API test rig** rigorously tests all MOSIP APIs, covering various corner cases for enhanced reliability. MOSIP also publishes a Security Test Report that outlines the various vulnerabilities in its systems, along with the severity risk and proposed recommendation to mitigate this risk.

25	**Reinforce transparency and accountability**	**Process:** Ensure accountability through records controls **Practice:** Embed records management controls such as automatic metadata capture and retention and disposition controls to manage access and mitigate the risk of unlawful tampering and deletion of records.	The data is encrypted in a way that makes it very difficult to swap or tamper records. There is no plaintext record of identity that can map to a person. All transport level data is encrypted and decrypted within the MOSIP platform code preventing any form of tampering. Audit records are created at every location to create evidence of any change. Source truth is maintained in the packet and every change should have an equivalent source of truth.
26	**Respond to gender, ability or age**	**Process:** Embed vulnerability in product design **Practice:** Perform targeted risk assessments to evaluate how the product might expose vulnerable groups to harm.	Engagements with Aapti and the GenderMag initiative substantiate MOSIP's commitment towards building inclusive technology. Through the GenderMag exercise MOSIP has committed to bring in inclusivity in its administration, process, UI/UX, and API design. Associated Research and Publications: 1. Building Gender-Inclusive Digital Identity Systems 2. Gender Inclusion Toolkit for Digital Identity Systems 3. Systematising Inclusive Design in MOSIP 4. Inclusive UI Design Guidelines
27	**Respond to gender, ability or age**	**Process:** Embed vulnerability in product design **Practice:** Ensure that the product is designed with inclusive features that cater to the needs of vulnerable groups.	Software tends to favour methods statistically preferred by men. Removing gender biases is important to ensure everyone's ability to fully participate in and benefit from the technology. Recognising this, MOSIP partnered with researchers at Oregon State University (OSU) to leverage the GenderMag methodology developed by the team at OSU. GenderMag, also known as the Gender-Inclusiveness Magnifier, is a usability inspection method to find and fix gender-inclusivity bugs in problem-solving software. Moreover, GenderMag is an initiative by MOSIP for inclusion-led design of technology. MOSIP plans on bringing in inclusivity in four areas: Administration - through designing solutions that reduce digital barriers, for eg Database Administration, Data Sharding, Rancher Process - through designing inclusive solutions for example by offline verification APIs supporting inclusive services though for example - USSD , eSignet, Token Seeder And the UI/UX - to reduce the digital entry barrier.

28	**Promote autonomy and agency**	**Process:** Implement a standardised consent workflow and ensure compliance with regulations. **Practice:** Develop and follow standardised protocols for data requests and transfers to ensure consistency and interoperability among different data providers and users **Practice:** Conduct regular audits to verify compliance with data protection regulations, ensuring that consent workflows and security measures are continually updated to meet evolving legal requirements and industry standards. **Practice:** Implement automated monitoring tools to continuously check for vulnerabilities in encryption implementations and to ensure compliance with the latest security protocols.	Acquiring consent for every interaction of the resident with the MOSIP platform (Registration Client, Preregistration, Authentication, Resident Service, eSignet) is built into the platform. The content of the consent is beyond the scope of MOSIP Platform as it is configured by the respective client. The eSignet consent design is roughly in line with cloud providers, with the Inji mobile app making consent more reliable and efficient. MOSIP's internal process and its roadmap planning continues to review this work.
29	**Promote autonomy and agency**	**Process:** Implement optional features for user control over personal data **Practice:** Develop customisable data control features such as consent management tools and privacy settings, allowing users to adjust their data sharing preferences easily, similar to GDPR-compliant consent dashboards.	Every place the resident interacts with MOSIP - Registration Client, Preregistration, Authentication, Resident Service, eSignet. The content of the consent is beyond the scope of MOSIP Platform as it is configured by the respective client. The dashboard does not exist as of today.

30	**Do not discriminate**	**Framework Process:** Design and implement alternate processes for users who lack assumed documentation. **Framework Practice:** Ensure the system accommodates users with limited legal capacity, ensuring no one is excluded.	MOSIP supports the enrolment of children through a modified biometric capture process. For infants, only face biometrics can be captured since fingerprints and iris scans may not be feasible or reliable for very young individuals.

Table 2:

Suggested Responsible Authority for key Framework practices

	Safeguards Principle	Safeguards Framework Process and Practice	Suggested Responsible Authority	Rationale
1	**Assure data security by design**	**Framework Process:** Implement a framework for safe data storage and processing. **Framework Practice:** Use Role-Based Access Control (RBAC): Set up RBAC to limit data access based on user roles and responsibilities.	Government/ SI	Partially applicable. MOSIP does not engage in data processing activities in implementations. They provide features for counties to set up RBAC, but the customised deployment which is used in conjunction with other digital government systems needs to do the same for the implementation.
2	**Assure data security by design**	**Framework Process:** Implement data validation, completeness, and consistency checks. **Framework Practice:** Implementation of robust data validation and backup through ensuring data integrity and authenticity through advanced methods. This can be done through: regular data backups, advanced validation methods, completeness and consistency checking, and/or use of cryptographic signatures for data authenticity.	Government/ SI	Partially applicable. The use of cryptographic algorithms and ensuring data consistency is a part of a DPG provider's scope. However, regular data backups and advanced validation methods are post-implementation practices that are not in its scope.

3	**Assure data security by design**	**Framework Process:** Safeguard user data through heightened user control and accountability. **Framework Practice:** Provide multiple platforms for users to understand and manage consent so that those with lower literacy and tech access can do so independently.	Government/ SI	Partially applicable. DPG providers are responsible for designing and incorporating solutions that ensure users can understand and manage consent. However, the content and constraints of this consent are beyond its scope as it is a policy consideration.
4	**Ensure data privacy by design**	**Framework Process:** Address data leakage and unauthorised use with technical safeguards. **Framework Practice:** Establish liability regimes for data leakage scenarios.	Government	The framework process of addressing data leakages and unauthorised use with technical safeguards falls under a DPG provider's scope. However, establishing liability regimes for data leakage scenarios is out of its scope as it is a policy and post-implementation consideration.
5	**Ensure data privacy by design**	**Framework Process:** Emphasise transparency and user empowerment in managing data. **Framework Practice:** Communicate privacy practices and policies to users, ensuring they are easily accessible and understandable.	Government/ SI	Partially applicable. Crafting privacy policies that are accessible and understandable are within the DPG provider's scope. Moreover, a DPG provider can provide visibility of these practices on its platform. However, ensuring this communication to users falls outside its scope.
6	**Assure data security by design**	**Framework Process:** Safeguard user data through heightened user control and accountability. **Framework Practice:** Provide users flexible access to and ownership of their data after they provide consent, thereby respecting users' rights to revoke access.	Government/ SI	Designing the technology to allow users to revoke access falls within the scope of a DPG provider. However, implementing the right to revoke access is a policy consideration and out of a DPG provider's scope.

7	**Assure data security by design**	**Framework Process:** Safeguard user data through heightened user control and accountability. **Framework Practice:** Help users navigate "legalese" by prioritising key elements of consent, including what is collected, explicit purpose(s), duration, parties with access, and channels to change and/or revoke consent.	Government/SI	The DPG provider can design the technology in a way that ensures users' consent is required to collect, process, store, and/or revoke access to data. However, the content of this consent and implementation to support users is the responsibility of the adopting nation.
8	**Assure data security by design**	**Framework Process:** Safeguard user data through heightened user control and accountability. **Framework Practice:** Train staff and relevant partners to ensure a common understanding of internal data use and sharing policies, but also universal recognition of their importance.	Government	Partially applicable. MOSIP's country training is tailored to suit the unique needs of each country. These sessions focus on the hands-on implementation, customisation, and integration of the MOSIP platform within the local context. However, training to highlight the importance of data use and sharing policies falls outside its scope.
9	**Ensure data privacy by design**	**Framework Process:** Emphasise transparency and user empowerment in managing data. **Framework Practice:** Conduct regular audits and reviews of data handling practices and privacy measures to ensure they remain compliant with evolving regulations.	Government	Reviewing data handling practices is a post-implementation consideration that is outside the scope of a DPG provider. Moreover, ensuring that practices are compliant with evolving local regulations is not its responsibility. A DPG provider typically has a set of its own privacy considerations that it aims to uphold. It can routinely update systems based on its own set of policies.

10	**Ensure data privacy by design**	**Framework Process:** Establish mechanisms to ensure a right to opt-out whenever appropriate. **Framework Practice:** Integrate opt-out features into the design of DPI systems, ensuring they are user-friendly and accessible, based on best practices identified from leading global privacy standards.	Government	Partially applicable. A DPG provider can incorporate features that enable opt-out for users. However, ensuring it is offered is a policy consideration and the responsibility of the adopting country.
11	**Ensure data privacy by design**	**Framework Process:** Establish mechanisms to ensure a right to opt-out whenever appropriate. **Framework Practice:** Ensure that opting out does not hinder access to essential services, and that personal data is protected from being used for secondary purposes, even when anonymised, to maintain user trust and compliance with privacy regulations.	Government	The decision to ensure that opting out does not hinder access to essential services is a policy consideration.
12	**Ensure data privacy by design**	**Framework Process:** Establish mechanisms to ensure a right to opt-out whenever appropriate. **Framework Practice:** Collaborate with regulators to ensure that the opt-out mechanisms developed are aligned with legal requirements and that they provide clear, transparent options for users to manage their data preferences effectively.	Government	The DPG provider can ensure that their solutions provide clear, transparent options for users to manage their data preferences. However, the decision to implement this is a policy consideration and rests with the adopting nation/the implementor.

13	**Ensure data privacy by design**	**Framework Process:** Implement strict controls to enforce purpose limitation and restrict secondary data use. **Framework Practice:** Design tools that require explicit user consent for any data use beyond the initially stated purpose.	Government	A DPG provider typically only has APIs for authentication and e-KYC. It does not have the ability to collect or process data. However, the systems can be designed in a way that ensures that without the user' UIN/VID/handles decryption is not possible.
14	**Ensure data privacy by design**	**Framework Process:** Integrate strict data anonymisation protocols into design. **Framework Practice:** Design forms and digital interfaces that collect only essential information.	Government	This is out of the scope of a DPG provider as the adopting nation decides the ID schema and UI schema which then determine the information collected.
15	**Ensure data privacy by design**	**Framework Process:** Integrate strict data anonymisation protocols into design. **Framework Practice:** Pseudonymised data might still be re-identifiable and should not be treated as anonymised without further scrutiny. It still requires access management, controlled processing environments, transaction protocols and a liability regime for misuse.	Government	Controlling the individuals and entities that have access to the data is out of the scope of a DPG provider and is the responsibility of the adopting country.

16	**Ensure data privacy by design**	**Framework Process:** Integrate strict data anonymisation protocols into design. **Framework Practice:** Periodically review data collection practices and storage to identify and eliminate unnecessary data, similar to practices in the California Consumer Privacy Act (CCPA).	Government	DPG providers typically collect data that they use for the creation of the identity. However, this evidence is stored independently which allows adopters to delete the evidence after a certain period. The practice to periodically eliminate unnecessary data, however, is the responsibility [decision lays in their hands] of the adopting country. Articulation of the practice would benefit from specifying which features/elements of the CCPA are recommended.
17	**Ensure data privacy by design**	**Framework Process:** Implement and maintain comprehensive cybersecurity measures. **Framework Practice:** Use network segmentation to isolate critical systems and limit the spread of potential breaches.	SI	The platform architecture can safeguard the data, as MOSIP does, by storing biometrics and demographic data separately to minimise spread of potential breaches but cannot control network design in an implementation.
18	**Ensure data privacy by design**	**Framework Process:** Establish secure data exchange protocols. **Framework Practice:** Apply strong encryption and access controls to safeguard data within CCRs.	SI	DPG providers ensure that the data they collect is encrypted and subsequently secure from data breaches. However, limiting access controls within CCRs is a consideration for the implementor as it is an issue with the underlying hardware.
19	**Ensure data privacy by design**	**Framework Process:** Establish secure data exchange protocols. **Framework Practice:** Adhere to data protection regulations and standards to maintain user privacy and trust.	SI	The DPG provider needs to ensure that the design of the system upholds and adheres to data protection regulations and standards. However, adherence is out of scope for a DPG provider.

20	**Ensure data privacy by design**	**Framework Process:** Establish secure data exchange protocols. **Framework Practice:** Regularly review and update compliance practices to align with evolving legal requirements.	Government/ SI	The DPG provider typically works with multiple countries and has a set of principles they consistently update and follow. However, ensuring compliance with evolving local legal requirements is out of its scope.
21	**Promote autonomy and agency**	**Framework Process:** Implement optional features for user control over personal data. **Framework Practice:** Incorporate functionalities like data export and deletion requests, giving users full control over their personal information.	Government	This is out of the scope of a DPG provider as data export and deletion requests are a policy consideration.
22	**Reinforce transparency and accountability**	**Framework Process:** Implement comprehensive reporting and accessibility protocols. **Framework Practice:** Develop detailed and frequent reports on system performance, usage statistics, and incident responses.	Government/ SI	Reporting can be built into the software by the DPG provider; however, ensuring its implementation is out of its scope.
23	**Reinforce transparency and accountability**	**Framework Process:** Implement comprehensive reporting and accessibility protocols **Framework Practice:** Create accessible platforms for public retrieval of these reports, ensuring clarity for non-technical audiences.	Government/ SI	Creating constant reports and ensuring clarity for non-technical audiences is a policy consideration and the responsibility of the adopting nation, not the DPG provider.

24	**Promote autonomy and agency**	**Framework Process:** Implement optional features for user control over personal data. **Framework Practice:** Regularly update reports and documentation to reflect system changes and maintain accuracy.	Government/ SI	This is a post-implementation practice and thus, not in the scope of the DPG provider.
25	**Respond to gender, ability or age**	**Framework Process:** Ensure that DPI are linguistically appropriate for the whole population. **Framework Practice:** Build DPI systems with interfaces that support multiple languages, allowing users to select their preferred language upon accessing the platform.	Government	The DPG provider builds the ability to configure multiple languages. However, the option to offer platform services in multiple languages is out of its scope and up to the adopting country.
26	**Respond to gender, ability or age**	**Framework Process:** Ensure that DPI are linguistically appropriate for the whole population. **Framework Practice:** Ensure that technical support services, such as help desks, chatbots, and customer service hotlines, are available in the primary languages spoken by users.	Government	The DPG provider can design systems in a way that offers these services in multiple languages. However, the option to offer this is a policy consideration and out of a DPG provider's scope.

iiit-b
ज्ञानमुत्तमम्

MOSIP