MSC
MicroSave Consulting

Leveraging data sharing systems to improve public service delivery in LMICs

White paper

November 2025

Launched during the Global DPI Summit 2025 at Cape Town.

Table of contents

Foreword

Access to data is a key driver of digital development, especially in low- and middle-income countries. Governments can design effective policy interventions, deliver services that target the right beneficiaries, and monitor their efforts when they can securely share and use data across institutions. Achieving these outcomes requires a shared commitment to collaboration and data interoperability within the public sector, as well as safeguards to ensure that data is shared with the data owner's consent securely.

This white paper examines how data sharing systems, as part of a country's digital public infrastructure (DPI) approach, can help achieve public sector data interoperability. This paper aims to (i) build a shared understanding of the different models and approaches to data sharing, (ii) highlight the benefits of data sharing in the public service delivery context through country-specific case studies, and (iii) offer guidance to stakeholders on the enablers, challenges, and future pathways for scaling data sharing.

This paper does not cover other impact pathways, such as personalized delivery of services by the private sector and verifiable credentials that data sharing can enable. Nor does it elaborate on the taxonomy of trusted data sharing systems. These themes will be explored in subsequent publications as part of MSC's ongoing work on DPI.

The research and country experiences captured here are intended to help the broader ecosystem understand the current global data sharing landscape. We hope this paper supports governments, development partners, the private sector, and funders as they shape strategies that advance data sharing and, in turn, lead to effective and inclusive public service delivery.

Mitul Thapliyal

Managing Partner, MSC (MicroSave Consulting)

Message from Co-Develop

When we think about infrastructure, we tend to think about roads, electricity grids, and telephone networks; the physical plumbing that powers economies and connects people. But in an increasingly digital world, we need infrastructure to match it. And at the heart of that digital public infrastructure (DPI) is something often overlooked: the ability for systems to talk to each other.

In most low- and middle-income countries today, data remains locked in silos. A health ministry cannot easily verify a citizen's identity. A social protection agency cannot confirm who has already received benefits. A farmer seeking a subsidy must submit the same documents to multiple offices. This fragmentation is not only inefficient, but it also excludes the very people these systems are meant to serve.

Data sharing systems are the digital plumbing that can change this. When governments can securely exchange trusted data across institutions, they can reach the right people with the right services at the right time. They can pay health workers more efficiently. They can provide subsidies to farmers more quickly. They can ensure vulnerable populations are not left behind. This is what we mean by infrastructure thinking: building reusable, interoperable foundations that everyone can build upon, rather than creating redundancies.

At Co-Develop, we believe that safe and inclusive digital public infrastructure is essential to building fairer societies. Our mission, supporting 50 countries in adopting DPI over the next five years, is grounded in a simple conviction: unless we see people in villages and towns saying, "I am benefiting from this," we are not succeeding.

This white paper brings together these insights and more. It examines how data sharing systems can transform public service delivery when designed with inclusion, trust, and interoperability at their core. It offers practical guidance for governments, funders, researchers, and technologists working to build these foundations.

We offer this research in the spirit of co-development and the belief that lasting progress emerges through partnership. We hope that it contributes not just to dialogue, but to action: helping countries build digital systems that uphold human dignity and expand opportunity for all.

CV Madhukar

CEO, Co-Develop

Acknowledgments

This white paper was authored by Anshul Pachouri, Shivangi Malhotra, Aastha Nath, and Shubam Kumar.

Several colleagues from MSC (MicroSave Consulting) contributed their inputs to this white paper, including Mitul Thapliyal, Kunjbihari Daga, Debarshi Chakraborty, Abhishek Raj, Anirooddha Mukherjee, Vikram Pratap Sharma, Diganta Nayak, Mansi Sharma, Allina Tiwari, Deepakshi Bhardwaj, and Felicien Lokossou. Editorial and design support from Rahul Ganguly, Kamiya Satija, Dinesh Singh and other team members is also duly acknowledged.

The authors also wish to thank Dr. Kanwaljit Singh and Tanner Lewis (Gates Foundation), Julia Clark (World Bank), Robert Opp (UNDP), Dr. Pramod Verma (Centre for Digital Public Infrastructure – CDPI), C.V. Madhukar (Co-Develop), Priya Vohra (Digital Impact Alliance – DIAL), Dawit M. Dame and Yodahe Zemichael (Ethiopia National ID Program – NIDP), Christopher Kantinti (National Identification and Registration Authority- Uganda), Stella Alibateese (National Information Technology Authority- Uganda), Mphatso Augustine Sambo (National Registration Bureau, Malawi), Emily Pagador (PhilSys Registry Office, Philippines), Mouhamed Mahi Saikh Sy and Ndeye Maguette Gueye Ndiaye (Agence de la Couverture Maladie Universelle, Senegal), Nanjira Sambuli (Carnegie), Tim Wood (Co-Develop), Pamod Amarakoon (DHIS2 Sri Lanka), Felix Ochoro (Tony Blair Institute, Zambia), Yoon-seok Ko (National Information Society Agency, South Korea), Brijesh Kumar(Tony Blair Institute, Sierra Leone), Gail Hodges, Mark Haine, Elizabeth Garber (OpenID Foundation – OIDF and SIDIHub), Prof. S Rajagopalan, Arun Kumar Gurumurthy, and Nagarajan Santhanam (MOSIP / IIIT-B / OpenG2P), and Manish Srivastava (eGov Foundation) for their valuable inputs.

Executive summary

Data sharing is one of the three key pillars of digital public infrastructure, alongside digital identity and digital payments. While the use and effects of digital IDs and payment systems are more evident to their users, data sharing systems generally operate behind the scenes to enable governments, private sector entities, and individuals to share data seamlessly.

Data sharing plays a crucial role in the digital development of low-and middle-income countries, especially in the delivery of public services. However, data often remains siloed across different government institutions, which limits the extent to which it can potentially inform decision-making. Interoperable data sharing systems can bridge these silos to allow institutions to securely access and reuse information from other institutions to improve public governance and service delivery.

This white paper highlights how emerging models and data sharing approaches can improve access to and experience of public services for individuals and businesses. It proposes a broad conceptualization of data sharing as an umbrella term that includes data exchange, data access, and consent-based personal data sharing. The paper defines data sharing systems as the combination of technology solutions, policies, governance frameworks, and institutional arrangements that enable data sharing among stakeholders, including governments, private sector entities, and individuals.

This paper proposes a typology of data sharing systems based on various dimensions, including diverse participation structures, user categories, governance, and financial models. It then builds on this understanding to explore how data sharing systems enable interoperability in the public sector and the importance of incorporating trust into these systems by design. This paper recognizes data protection as a crucial element of trust and examines the mutually reinforcing interplay between data protection and data sharing systems. Data sharing systems operationalize privacy principles by embedding technical controls, while data protection frameworks require these systems to incorporate consent requirements and enforce individuals' data protection rights.

After it establishes the core nuances and approaches of data sharing systems, the white paper states their tangible benefits in improving public services in LMICs. It then presents country-based case studies of national data sharing systems from four geographies: Brazil, Cambodia, Mauritius, and Uganda. Each country's data sharing system varies based on maturity and adoption levels, technology choices, user categories, use cases, and efficiency gains.

Brazil's Conecta.gov.br is a cross-sectoral platform that uses API gateways to allow government entities to exchange data for public services. Cambodia's CamDX, built on Estonia's X-Road model, provides a decentralized data exchange that connects public and private institutions to enable e-KYC and business registration, among other use cases. Mauritius' InfoHighway enables secure government-to-government data exchange through the country's government intranet, facilitating public service delivery across various sectors. Uganda's UGhub, based on the WSO2 architecture, enables the government to deliver public services by onboarding multiple stakeholders, including the private sector.

The white paper then briefly explores open data ecosystems for AI innovation as an emerging focus for governments to improve public services through data sharing.

This white paper builds on the insights from country case studies and the overall data sharing landscape to present the key challenges and enablers that affect the development and scaling of data sharing systems. The adoption of data sharing systems by countries is slowed by inadequate technical

infrastructure, low digitization rates, fragmented governance and policy frameworks, organizational capacity constraints, and a lack of sustained funding. While these challenges hinder the growth of data sharing systems, several enabling factors can contribute to their successful development and use.

Establishing nodal authorities to govern data sharing can ensure policy coherence and show strong political will. Adopting and regularly updating regulatory frameworks, including data protection regulations, government interoperability frameworks, and national data strategies, clarifies stakeholder roles and responsibilities.

Anchoring the technical foundations of data sharing systems in international open standards and modular architecture can accelerate their adoption. Integrating national digital identity with national data sharing systems can simplify verification processes for service delivery. Finally, increasing stakeholder awareness through training, partnerships, and advocacy can improve institutional understanding of data sharing systems.

The white paper concludes with a call to action for coordinated efforts by governments, funders and donor institutions, research and academic institutions, and other ecosystem partners to improve the strategic adoption of data sharing systems.

Governments should harmonize governance frameworks, develop national data strategies and interoperability standards, and identify high-impact use cases for data sharing across sectors. Funders and donor institutions should align to provide coordinated funding, support readiness assessments to understand the country context, and allocate resources for cross-learning initiatives. Research and academic institutes should study data sharing governance models to inform policy decisions and conduct impact assessments of data sharing systems. Other ecosystem partners, including the private sector and civil society, should collaborate to conduct hackathons and challenges to identify new use cases of data sharing.

The white paper concludes with an emphasis that data sharing systems today are not merely technical tools. They have evolved to become a crucial component of digital governance. Embedding data sharing systems in robust institutional frameworks can make public services more accessible, efficient, and transparent. By adopting these systems, LMICs can chart a path toward more inclusive development, where citizens benefit from data that is used securely, efficiently, transparently, and in the public interest.

1 Understanding data sharing

The growth of internet access and smartphone penetration has rapidly increased data creation from digital interactions and online transactions globally. The term “data” has different meanings in different contexts. It can include structured data that fits into a schema, that is, a defined format. For example, customer databases maintained by companies or citizen databases that governments maintain. Data can also be unstructured, that is, data that does not fit into an organized and defined format. Data can refer to personal information, such as health or tax records, and non-personal data, such as geospatial data, traffic data, and weather data. Data can also be classified as open data or protected data. Open data refers to data that is made publicly available for anyone to access, use, and share, often provided by governments or organizations. On the other hand, protected data is subject to legal or regulatory restrictions on access and use.

This large volume of data can generate significant value for business decisions and public governance. However, private and public sector entities struggle to unlock the socioeconomic value of data due to its siloed storage and management across different information systems. Data sharing between different digital information systems can address this challenge. Hence, data sharing is crucial in digital development, especially in low- and middle-income countries.

However, the term “data sharing” has different interpretations depending on the context. Data sharing is an umbrella term that includes data exchange, access, and consent-based personal data sharing. This white paper broadly uses the term “data sharing” to refer to all these types of systems.

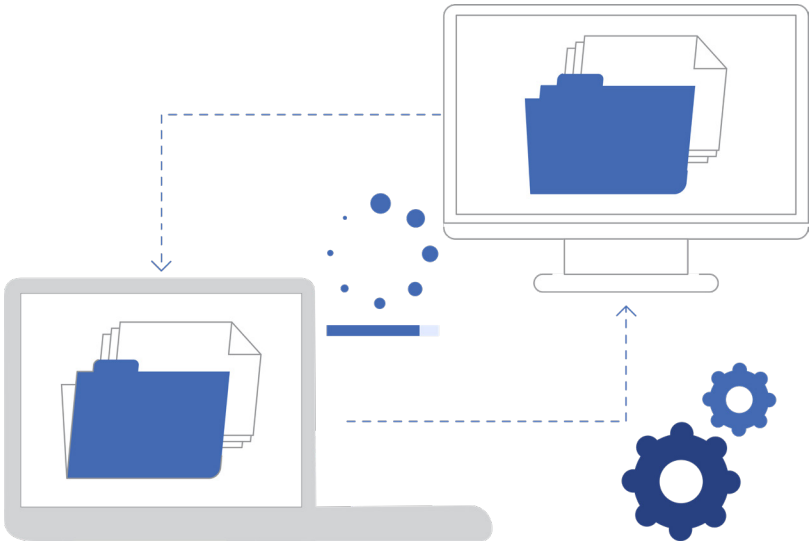
Data exchange, data access, and consent-based personal data sharing are different modalities of data sharing.

Data exchange implies entity-to-entity data sharing, where each participant can both provide and receive data. For example, a federal tax authority shares data with and receives data from its regional counterparts.

Data access more accurately represents making data available for public use. For example, open government data portals enable public access to government data for reuse by businesses, academia, and individuals.

Consent-based personal data sharing and management allows individuals to exercise control over sharing their personal information. For example, a platform may allow individuals to selectively share personal information, such as education documents or government-issued IDs, with entities that seek to verify this information.

Figure 1: Distinction between data exchange, data access, and consent-based personal data sharing



Data sharing is recognized as one of the three core components of digital public infrastructure (DPI) in countries, along with digital identity and digital payments. While digital IDs and payment systems are more evident to users, data sharing often operates in the background to improve coordination between different entities.

A DPI approach to build data sharing systems

The World Bank defines DPI as an approach to digitalization, focused on creating foundational, digital building blocks designed for public benefit. DPI systems generally adhere to the key principles of reusability, interoperability, accountability, and country ownership. In the context of data sharing systems, these principles can be applied in the following manner:

Reusability: Data sharing systems should be designed to serve multiple sectors, such as health, education, agriculture, and social protection, rather than being built for a single use case. Creating modular components can prevent a patchwork of expensive, duplicate solutions.

Accountability: Accountability can be created by embedding privacy-by-design and security-by-design principles in system architecture to ensure that data sharing is secure, transparent, and legally compliant.

Country ownership: Governments should define the vision, policies, architectures, and regulatory governance of national data sharing systems to ensure adaptability to country contexts.

Interoperability: Systems, datasets, and institutions must be able to exchange and interpret data seamlessly across platforms and sectors. Interoperable platforms can help centralize data governance and federate data sharing and management.

Figure 2: DPI approach for data sharing

1.1. Interoperability through trusted data sharing

Crucially, impactful real-world adoption of any data sharing system requires building trust in the design. Here, a data sharing system refers to the technology solutions, policies, governance frameworks, and institutional arrangements that enable data sharing among stakeholders, including governments, private sector entities, and individuals.

Digital trust generally refers to individuals' expectations that digital technologies and services, and the organizations providing them, will protect all stakeholders' interests and uphold societal expectations and values.

A combination of suitable laws and policies, institutional arrangements, and technical architecture is required to build trust in data sharing systems.

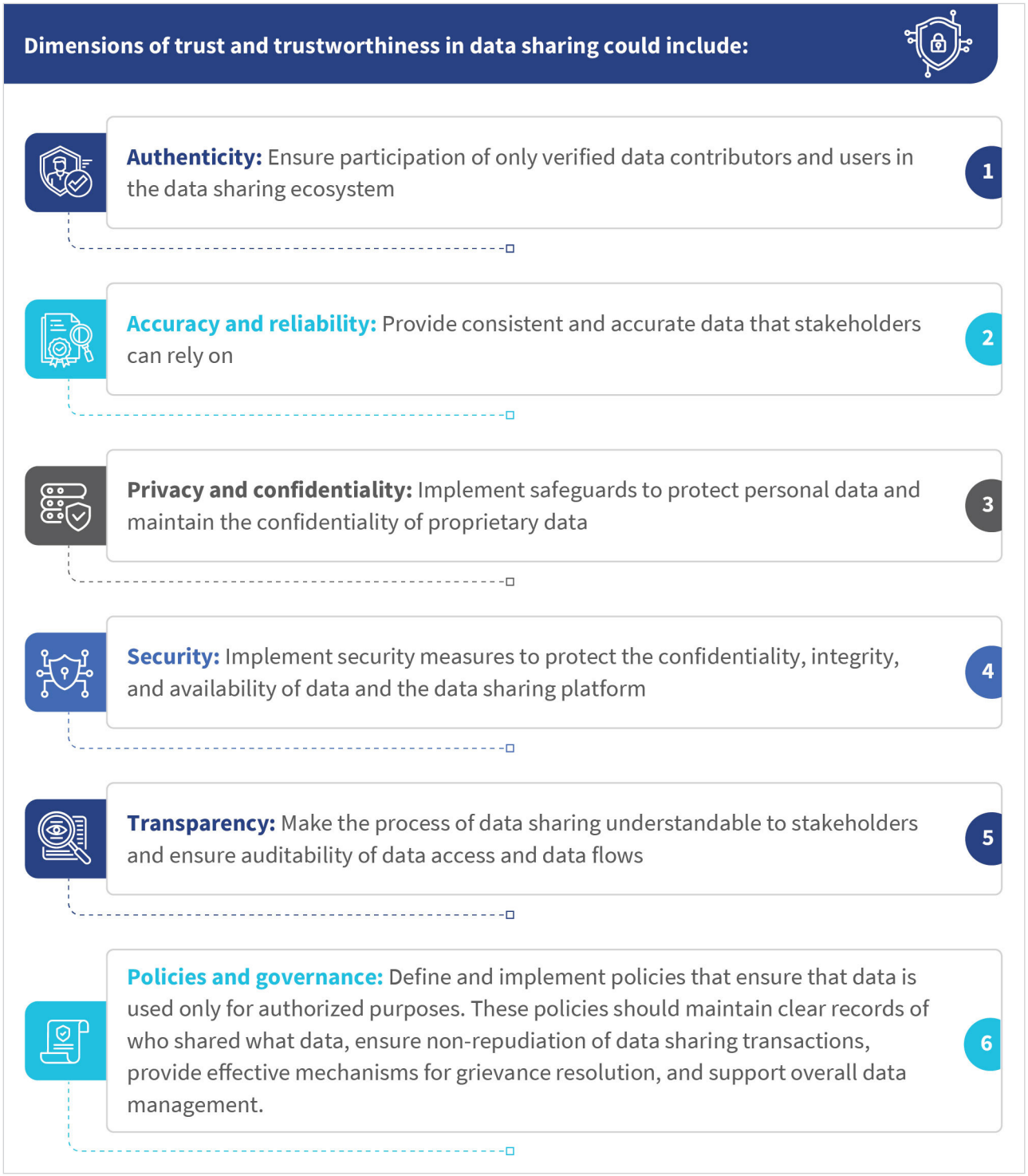


Figure 3: Ensuring trust and trustworthiness in data sharing

A data sharing system that incorporates these dimensions of trust can improve public governance in several ways. The primary benefit is improved data interoperability across different entities.

Interoperability refers to the ability of different units, such as databases, applications, or programs, to communicate, execute programs, or transfer data among each other.

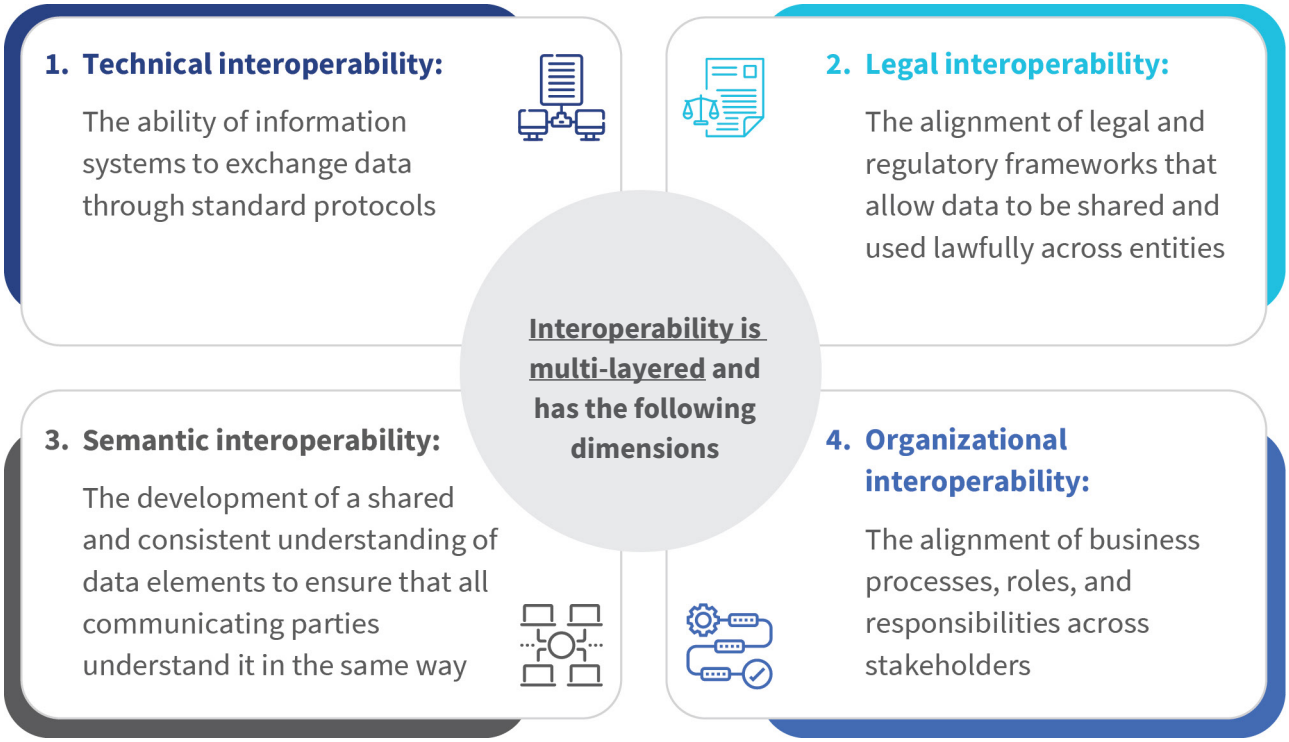


Figure 4: Dimensions of interoperability

Interoperability enables entities to use information seamlessly across different databases and information systems. Implementing interoperability through trusted data sharing systems can provide direct benefits, such as operational and administrative efficiencies alongside ecosystem innovations.

Interoperability also indicates how mature the digital transformation of governments is. While several countries have adopted interoperability frameworks and invested significantly to digitize government platforms, most are disconnected without sufficient automation of the data exchange process. This disconnected network of digital government platforms often contributes to a poor experience of digital public governance.

Enabled by trusted data sharing, interoperability allows public sector entities to operationalize the "once-only principle." This principle ensures that citizens only provide their data to government entities once. The once-only principle states that any data, documentation, or information a citizen has already shared with a public entity must be reused and shared with other public entities to deliver digital public services. This ensures that data from different government entities is consistent, accurate, and reliable. This is vital for government entities to make informed decisions, enhance operational efficiency, and promote stakeholder trust.

1.2. Typology of data sharing

Given their multidimensional nature, data sharing systems can be viewed through multiple lenses. Different typologies can be identified based on the objective of governments and other stakeholders who seek data interoperability through data sharing systems. For instance, data sharing may be undertaken voluntarily or under a legal obligation. Participation structures in data sharing systems could be one-to-one, one-to-many, many-to-one, or many-to-many. Users of data sharing systems may use them for a fee or at no cost. The table below explains this typology in detail.

Governance models	 **Voluntary participation**	Entities can voluntarily share data under a common standard or an agreement. For instance, the Trusted Exchange Framework and Common Agreement (TEFCA) in the US is an example of voluntary data sharing in the healthcare sector. Organizations that wish to join TEFCA and exchange health information with each other must register their networks as qualified health information networks.
	 **Legal mandate**	Data sharing may be mandated under the law in a few cases, especially in the public sector. For example, it may be legally mandated in the public sector. In Brazil, public administration entities are required to ensure mechanisms for data interoperability and reduce the costs of access to data. Similarly, in Cambodia, all public sector bodies automatically become members of the Cambodia Data Exchange (CamDX) under the law. In the financial sector as well, banking institutions may be legally mandated to share data. For instance, the UK has a legal mandate for the nine largest banks to adopt open banking.
Financial models	 **No-cost model of data sharing**	Many data sharing systems seek to facilitate information exchange for socioeconomic development and effective policymaking. Data sharing to achieve such objectives may adopt a no-cost model. For example, India's Tax Information Exchange System (TINXSYS) facilitates state tax departments in exchanging interstate trade data.
	 **Fee-based model of data sharing**	In some instances, data sharing systems may provide access to data for a fee. Each instance of data sharing may require users to pay a fee. For example, Account aggregators (AAs) in India usually charge a fee to financial information users. Prominent AAs, such as Anumati and Finvu, have publicly listed their pricing details for every instance of fetching and providing the data.
Data classification	 **Personal data**	Some data sharing systems facilitate the sharing of personal data, which directly identifies an individual. For example, platforms, such as Irembo in Rwanda, collect and process personal data to provide users with services related to immigration, health, and document notarization, among other services.
	 **Non-personal data**	In other data sharing systems, the focus is on sharing or exchanging non-personal data. For example, data sharing systems for climate mitigation often involve sharing non-personal data, such as satellite imagery and carbon emission data. For instance, the Odisha Forest Stack in India seeks to enable carbon credit generation. In Indonesia, the National Registry System for Climate Change facilitates the monitoring of climate mitigation actions taken in the country.

User categories		
	Government-to-government (G2G)	Some data sharing systems focus on enabling data sharing among different government ministries, departments, and agencies to improve public governance. G2G data sharing systems could be operationalized through data exchange protocols or common platforms that various government entities use to share data. For example, Brazil's Conecta.gov.br facilitates government-to-government data exchange and does not allow citizens to use it directly.
	Government-to-business (G2B)	Government-to-business (G2B) data sharing systems establish a direct interface between governments and businesses. Such systems usually seek to improve revenue collection for the government and facilitate the private sector's ease of doing business. For example, Chile's Registro de Empresas y Sociedades portal simplifies business registration and other enterprise processes through interoperability features that connect the business registry and tax agency websites.
	Government-to-citizen (G2C)	Government-to-citizen (G2C) data sharing systems establish a direct interface between governments and citizens. Such systems usually seek to simplify citizen access to public services. For example, Uganda's UGHub is a data sharing system to simplify citizens' access to government services across sectors, such as education, healthcare, and utilities.
	Business-to-business (B2B)	Some data sharing systems facilitate information exchange between businesses, which usually enables ease of doing business and operational efficiencies. Singapore's SGTraDex is an example of data sharing in the trade sector. The platform allows businesses to share supply chain-related data through a common data highway.
	Citizen-to-government (C2G)	Data sharing systems, such as DigiLocker in India, enable citizens to share their data with government entities and avail themselves of different services by providing verified documents.
	Consumer-to-business (C2B)	Some data sharing systems allow users to store their personal data in digital wallets and grant controlled access to businesses for personalized offers or services. For instance, the Solid personal online data store (Pod) allows individuals to choose which applications use their data to prevent user lock-in to specific platforms.

Participation models	**One-to-one data sharing**	When data sharing systems facilitate unilateral data sharing between a single sender and recipient, the participation structure qualifies as one-to-one data sharing. A national tax authority that shares information with its regional office could be an example of one-to-one data sharing.
	One-to-many data sharing	A one-to-many participation structure in data sharing implies that a single entity has the right to aggregate and share data. However, multiple recipients can be involved. Government open data portals are typical examples of this type of data sharing. For instance, in the U.K., Find open data initiative publishes data from government sources to help the ecosystem build better products and services.
	Many-to-one data sharing	In a many-to-one participation structure for data sharing, multiple data contributors send data to a single hub or data custodian. For example, Nigeria's National Data Repository is a platform that hosts aggregated data from healthcare institutions to track active HIV cases, their testing, and treatment.
	Many-to-many data sharing	Multiple entities can send and receive data in a many-to-many participation structure for data sharing. A data consumer can also commonly be a data contributor. In the case of G2G data sharing systems, government ministries, departments, and agencies may also have a legal mandate to participate in a data sharing system. For example, Brazil's Conecta and Uganda's UGhub are data sharing systems with a many-to-many participation structure.
Sector scope	**Cross-sectoral**	Some data sharing systems are cross-sectoral and designed to facilitate data sharing across healthcare, banking, education, land governance, and law enforcement, among others. Examples of cross-sectoral data sharing systems include Brazil's Conecta and Cambodia's CamDX. Each of these systems facilitates data sharing across multiple sectors.
	Sector-specific	Data sharing systems can also focus on one sector and be designed to solve a specific challenge in it. For example, Singapore's OpenCerts is a data sharing platform that allows educational institutions and employers to issue tamper-proof certificates and verify their authenticity.

Table 1: Typology of data sharing systems

This typology represents a spectrum of approaches to design and deploy data sharing systems. A specific data sharing system could fall anywhere along this spectrum. For example, a data sharing system may operate entirely on a no-cost or fee-based financial model. A data sharing system can also allow some data exchange transactions to occur at no cost, while other transactions would require a fee.

Similarly, a data sharing system may exclusively be designed to share personal data or non-personal data. Depending on the system's use cases, some may involve sharing personal data while others involve non-personal data.

1.3. Interplay between data protection and data sharing systems

Platforms such as DigiLocker in India, Conecta.gov.br in Brazil, and Mauritius' InfoHighway enable different entities to obtain personal data, such as identity information about citizens, to facilitate service delivery. Because such platforms involve sharing personal data, embedding privacy safeguards by design is critical.

The relationship between data protection and data sharing systems is mutually reinforcing and increasingly central to digital governance. Well-designed data sharing systems can advance data protection goals. Simultaneously, evolving data protection regulations can shape how data sharing systems operate.

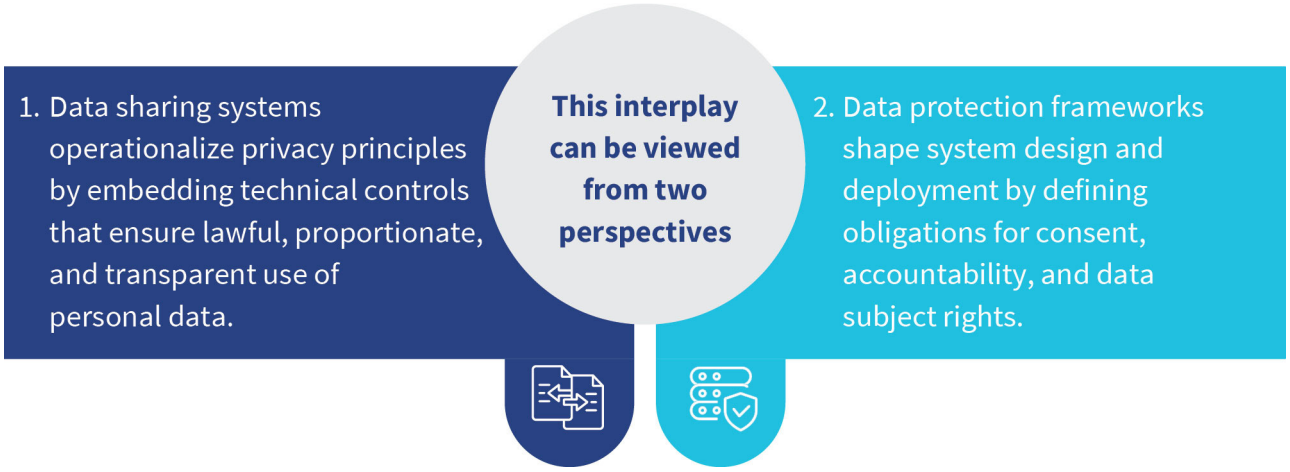


Figure 5: Mutual interplay of data sharing and data protection

1.3.1. Data sharing systems operationalize data protection principles by design

The 1980 OECD guidelines on the protection of privacy and transborder flows of personal data are foundational to modern data protection laws worldwide. The guidelines outline core privacy principles, which include provisions to limit the collection and use of personal data, ensure data quality, specify purposes for data use, transparency and accountability, and uphold individuals' rights.

Modern data sharing systems translate many of these principles into practice. By design, they limit unnecessary collection by allowing authorized entities access only to the data needed for a specific purpose. This reduces duplication of efforts and reinforces the principles of data minimization and purpose limitation.

Interoperability frameworks in countries, such as India and Brazil, are the technical foundation for data sharing systems. These frameworks specify standards for data formats, exchange protocols, and custodial responsibilities. They indirectly uphold the OECD principles of data quality, accountability, and security safeguards.

Moreover, some data sharing systems also indirectly operationalize modern privacy rights, such as the right to data portability, which allows individuals to transfer their personal data between service providers. Although originally conceived to ensure competitive markets, such rights enhance fairness and user control within the public sector.

The design and deployment of data sharing systems requires frameworks and technical specifications that inherently overlap with privacy obligations. Embedding these controls early ensures that interoperability strengthens, rather than weakens, individuals' data-protection rights.

1.3.2. Data protection frameworks shape system design and deployment

Just as data sharing systems can strengthen privacy by design, data protection regulations shape how such systems operate. Most data protection laws impose direct obligations on data controllers, that is, entities that decide how personal data is used. Indirect obligations usually lie with data processors, that is, third-party entities that act on the instructions of data controllers.

These obligations require compliance with data protection principles, identification of a lawful basis to process personal data, and implementation of technical and organizational safeguards against data breaches.

Generally, data protection laws provide several lawful bases on which entities can process personal data. One such lawful basis is an individual's consent. Others can include processing personal data for public interest to fulfil contractual obligations and legitimate interests, such as the prevention or investigation of crimes.

Where consent is the lawful basis to process personal data, data protection laws require that consent should be explicit, specific, free, unambiguous, and informed. Technical interventions need to be implemented to achieve valid consent. These include designing mechanisms to gather user consent, manage the consent lifecycle, log and audit consent, and enable consent revocation by individuals. Organizational practices and procedures also play a role to ensure accountability around consent management and user rights.

Considering this, the nature of consent may vary based on a data sharing system's use cases. Consent may be captured through a consent agreement, through third-party intermediaries, such as consent managers, or explicitly from the individual at the start of a data sharing transaction. The scope of the consent may extend to active processing of personal data or just its storage. The consent may be valid for a single instance of data sharing or be reusable for recurring services.

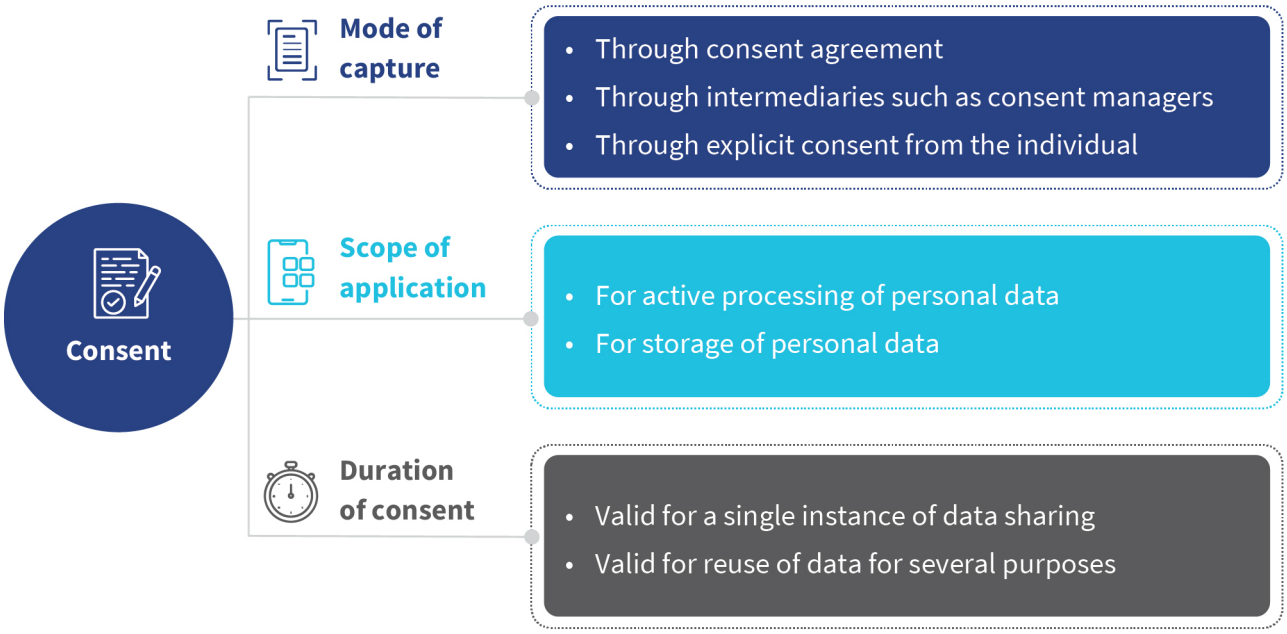


Figure 6: Nuances of consent in data sharing

Data protection laws worldwide, including Europe's General Data Protection Regulation, India's Digital Personal Data Protection Act (DPDPA), and Brazil's LGPD, recognize consent as a primary lawful basis to process personal data.

However, requesting consent can be impractical in many public sector use cases, and data protection laws in several jurisdictions also recognize this practical nuance. For instance, India's DPDPA permits the government to reuse existing digital personal data to issue subsidies, benefits, and services, among others, without obtaining fresh consent from individuals. Similarly, the data protection laws in Brazil and Nigeria allow government authorities to process personal data to perform their legal or public-interest duties. In these scenarios, government authorities do not necessarily have to obtain an individual's consent.

Therefore, in each jurisdiction, implementing agencies must determine when individuals' consent is necessary and when data may be processed on other legal grounds without explicit consent. Data sharing systems should include suitable protocols and technical solutions for both scenarios.

Regardless of the lawful basis, data protection laws grant individuals rights to request access to and correct personal data. Some data sharing systems already provide citizen dashboards that display what data is held and by which public authorities, thus enabling the right of access.

Data protection regulations also create legal obligations for security, transparency, and accountability throughout the data processing lifecycle. Aligning system architecture and operational protocols with these obligations allows governments to deliver efficient, trusted services without compromising privacy or public confidence.

Finally, it is essential to highlight that strong data protection underpins public trust in data sharing systems. With this trust, governments can use data to enhance public service delivery in LMICs.

2 Role of data sharing systems in improving public service delivery

Public service delivery in LMICs often faces structural challenges, such as fragmented information systems, limited administrative capacity, and weak coordination among government agencies. These gaps delay the delivery of public services and create challenges in the effective delivery of services to individuals and businesses. Many people in LMICs, especially the poor and other vulnerable groups, rely on public services and government support for their sustenance. Hence, any change in the efficiency of the public service delivery process can have wider socioeconomic ramifications.

LMICs have increased the development and adoption of national, regional, sectoral, and cross-sectoral data sharing systems to enable the delivery of public services to individuals and businesses and address these structural challenges. For example, African nations, such as Uganda, Namibia, Tanzania, and Morocco, have either developed or are developing cross-sectoral data sharing systems. These systems facilitate interoperability between government ministries, departments, and agencies.

In the Asia-Pacific region, India has implemented both sectoral and cross-sectoral data sharing systems. It includes “Account Aggregators” in the financial sector and cross-sectoral data sharing systems, such as DigiLocker. In Malaysia, the MyGDX platform connects various government agencies to enhance online services. Bhutan is implementing a system to operationalize health information exchange across four health information banks. CamDX has adopted the X-road model to enable public service delivery in Cambodia. Brazil’s Conecta.gov.br is operational in Latin America, while Colombia has also been working to launch an interoperability platform.

These data sharing systems have various use cases. They facilitate revenue collection through taxes, enable business registration, and provide subsidies to low-income households, among other benefits. Data sharing systems across jurisdictions offer benefits for existing public service workflows, as highlighted below.

2.1. Administrative efficiency

Data sharing systems that directly interface with citizens or business entities, such as G2C, G2B, or C2G systems, can eliminate the need for individuals to physically visit government offices. These systems reduce their reliance on assistance from public officials. A cross-sectoral e-services platform built on interoperable data sharing systems saves governments the time and effort required to create separate platforms to enable each service.

Government administrative overhead can be reduced even when data sharing systems operate as a data exchange layer between government entities, without any direct platform interface for individuals or businesses. Data sharing systems save the beneficiaries of public services by implementing the "once-only" principle, which eliminates the need to provide the same documents and information multiple times. Similarly, the duplication of efforts is reduced for the government. Once a government entity has undertaken due diligence to obtain specific information from a service beneficiary, the same information can be shared across ministries, departments, and agencies. These entities can check eligibility for other services, enroll a beneficiary into a new service, or provide social benefits.

Besides procedural efficiencies, interoperable data sharing systems can result in substantial time and cost savings for governments undergoing digital transformation. The automation of service delivery and auditability of transactions through data sharing systems can also reduce leakages of funds or other corrupt practices.

In Brazil, Conecta.gov.br claims to have saved approximately USD 2 billion through faster processing and fewer errors. Similarly, in Cambodia, the implementation of the CamDX system claims to have reduced the processing time to obtain new business licenses or certificates to eight working days.

2.2. Delivering citizen-centric and adaptive public services

Interoperability in the public sector enhances governments' ability to access, interpret, and reuse data at scale by integrating various information systems. Data sharing systems can help to ensure that public services are citizen-centered in the long term. Citizen-centric service delivery is also core to the World Bank's approach to GovTech, which emphasizes the importance of targeting, tracking, and delivering services to citizens and businesses.

Citizen-centric public services refer to the ability of governments to identify the right public services or social benefits that a beneficiary is eligible for based on life events.

	Information Shared	Record/s created	Benefits unlocked	Real world analogues
Birth	• Birth details	• Digital birth registration • Verifiable birth certificates • Immunization records	• Integrated health and nutrition services	• OpenCRVS
School education	• Birth record • Identity proof • Personal health record	• Verifiable school records and transcripts	• Migration assistance • Integrated learning management systems • Adolescent health services • Food security	• DigiLocker
Higher education	• Identity proof • School records and transcripts	• Verifiable college degree and transcripts	• Access to higher education • Employment services • International travel services	• OpenCerts
Employment and business	• Identity proof • Educational records and transcripts • Tax records • Business details	• Employment records • Business registration and licenses • Insurance records	• Taxation services • Digital credit • Government benefits (For example, agricultural services, MSME support)	• Open Banking • UGhub
Family services	• Identity proof	• Certificate of marriage registration • Child's health record	• International travel services • Financial services and insurance • Family health services	• DigiLocker
Old age services	• Identity proof • Personal health record • Insurance records	• Pension records	• Geriatric healthcare and nutrition services • Insurance cover • Emergency assist services	• *Jeevan Pramaan* • X-Road
Death	• Identity proof • Personal health record • Insurance records • Pension records	• Death registration	• Pension and benefits adjustments	• X-Road

Figure 7: Life-event-based delivery of public services unlocked by interoperable data-sharing systems

For example, in Denmark, the Borger.dk citizen portal provides a single platform for citizens to access public services across various life events, which include education, family services, and retirement. Similarly, in Singapore, the APEX platform enables public administrators to use data from various government agencies to determine an individual's eligibility for services.

2.3. Improving the inclusion of vulnerable groups

Vulnerable populations, especially in LMICs, often face barriers to access, affordability, and the ability to navigate digital environments to access public services.

The UN e-government survey proposes an integrated framework of data, design, and delivery for e-government interventions to leave no one behind (LNOB). The survey highlights that the lack of reliable and timely access to disaggregated data for the public sector directly contributes to the exclusion of vulnerable communities.

While solutions for exclusion require various interventions, the development and adoption of data sharing systems can help improve government data access. For instance, G2G data sharing systems that enable real-time data exchange allow government entities to access data from each other about vulnerable groups and their enrollment in various public services. These systems can help enroll individuals automatically in other public services for which they are eligible.

2.4. Improving data governance and transparency

Data sharing systems can improve data governance and transparency. The design of data sharing systems inevitably requires defining data formatting, storage, and exchange protocols. This standardizes how different government departments manage data and can also improve public officials' general understanding of best practices in data governance and management.

Data sharing systems also improve accountability as they maintain data access logs and make any data misuse traceable and subject to legal or administrative review. The interoperability of data records and the standardization of data transfer processes can improve the government and citizens' understanding of public service performance. For instance, in Denmark, the Mit Overblik platform provides citizens with a personal overview of what information different public authorities hold on them, the status of benefits they have applied for, and any ongoing disputes with public authorities.

Finally, data sharing systems can also lead to innovations that drive the delivery of customized services to individuals. For instance, in the financial sector, consent-based personal data sharing underpins open banking innovations in various countries.

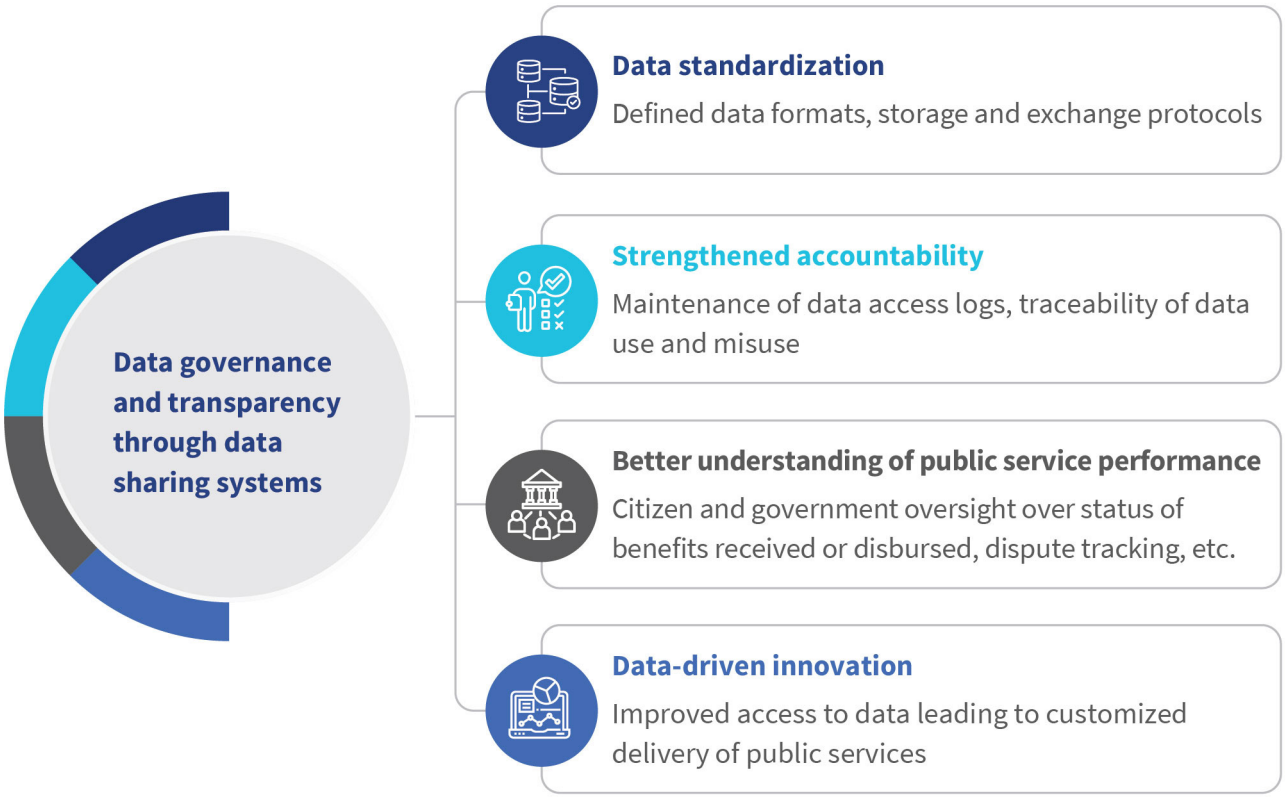


Figure 8: Role of data sharing systems in improving data governance and transparency

While the benefits of data sharing have been established above, its real-world application becomes clear when we examine how data sharing systems have been adopted across geographies. The following section discusses the varied approaches different countries have taken to develop data sharing systems through case studies.

3 Case studies of data sharing systems for public service delivery

Data sharing is central to the targeted and effective delivery of public services. This section examines the approaches of four data sharing systems for public services, which include Brazil's Conecta.gov.br, Cambodia's CamDX, Uganda's UGhub, and Mauritius InfoHighway. The case studies provide an overview of the selected data sharing system's genesis, context, technology, types of users, data protection and consent management, use cases, adoption, and effects.

The table below provides a high-level comparative snapshot of the selected data sharing platforms:

	Brazil: Conecta gov.br	Cambodia: CamDX	Mauritius: InfoHighway	Uganda: UGhub
Launch year and nodal body	2020 The Ministry of Management and Innovation in Public Services	2020 The Ministry of Economy and Finance	2016 The Ministry of Information Technology, Communication, and Innovation	2021 (operationalized) The National Information Technology Authority

	Brazil: Conecta gov.br	Cambodia: CamDX	Mauritius: InfoHighway	Uganda: UGhub
Technology architecture	API based	X-Road	Service-oriented architecture (SOA)	WSO2 enterprise service bus (ESB)
User type	Government, which includes federal and state entities	Government and private sector	Government, which includes ministries, departments, and district councils	Government, private sector, and citizens
Use cases	• Social program enrollment • Tax clearance for business license • Travel pass for low-income citizens with disabilities	• Business registration • Travel application processing, immigration, and issuance of e-visa • Tax registration • Issuance of tourism licenses	• Issuance of a license for boat operators • Financial aid for low-income individuals or households • Central KYC in banks	• Passport application • Work permits • Vehicle registration
Status of data protection law	Brazil's General Data Protection Law (LGPD), enacted in 2018	• Sub-decree no. 252 (2021) on protection of personal identification data • Sub-decree no. 164 (2021) on data exchange between the public and private sectors	Data Protection Act, enacted in 2018	• Data Protection and Privacy Act, enacted in 2019 • Data Protection and Privacy Regulations, enacted in 2021
Adoption and effect	• Number of users: 180 federal government entities and 27 states • Effect: Cost savings of USD 1.8 billion since 2020	• Number of users: 74 state and non-state institutions • Effect: More than 97 million transactions since inception, reduced turnaround time of 8 days to register a business	• Number of users: 33 data publishers • Effect: 628 e-services enabled, 23 years of work time saved, and 600,000 citizens validated for negative income tax	• Number of users: 68 government entities and 78 private sector entities • Effect: More than 100 million transactions as of May 2024

Table 2: Comparative overview of national data sharing systems in selected LMICs

3.1. Conecta.gov.br: Brazil

Conecta.gov.br, launched in 2020 under Brazil's digital government strategy, seeks to simplify public service, reduce fraud, and enable more security and savings in public governance. It is built by the Ministry of Management and Innovation in Public Services as a national interoperable platform that enables real-time, secure, and automated data sharing between government entities. Before its launch, Brazil's government agencies and departments often relied on disparate, paper-based, or isolated digital databases incompatible with each other. Due to this, citizens and businesses had to submit the same information across different government entities repeatedly. Conecta.gov.br addressed this problem by placing the onus of data sharing on public institutions.

A strong legal framework supported the development and implementation of Conecta.gov.br. The law on simplifying public services and the law on digital government empower citizens with the right not to resubmit information already held by the government based on the "once-only" principle.

Types of users

The user base of Conecta.gov.br includes federal and state government entities. As of 2025, more than 190 federal entities and 20 state governments have joined the platform. Conecta.gov.br enables state-level entities to access federal databases. For instance, state tax offices use the platform to access the National Register of Legal Persons (CNPJ) and tax clearance data, which streamlines taxpayer validation for business registration or compliance checks.

The platform is also being scaled up to include municipal governments, which would ensure seamless data exchange across all three levels of public administration and improve public service delivery.

Use cases

Conecta.gov.br enables interoperability in more than 1,000 public services across various sectors, such as social protection, health, education, taxation, employment, and land registration. Some examples of services directly enabled by access to federal databases include:

1. Passport issuance enabled by access to identity and address data;
2. Social program enrollment enabled by access to the federal government's single unified registry for low-income families (CadÚnico services);
3. Tax clearance for business licenses enabled by access to the national register of legal persons (CNPJ) and citizen base registry (CPF).

Another interesting use case is the Interstate Free Pass issued by the National Land Transport Agency (ANTT) for low-income citizens with disabilities. The onboarding of the National Transportation Authority to Conecta.gov.br has automated the process to check individuals' eligibility by accessing the citizen base registry, disability certification data, and family income data.

Technology

The Conecta.gov.br platform is based on a secure application programming interface (API)-driven infrastructure that facilitates automatic and secure information sharing between government entities. It acts as a centralized hub for data sharing. It features fully digitized and centralized onboarding, management, monitoring of participating government agencies, as well as submission, evaluation, and granting of data access requests. Central to this platform is the government API catalog, which consolidates available APIs that enable government agencies to easily access and use verified data sources for public service delivery.

Conecta.gov.br's API manager complements the API catalog. This functionality allows API providers such as Receita Federal do Brasil (Federal Revenue Service), Ministério da Saúde (Ministry of Health), Ministério do Desenvolvimento e Assistência Social, Família e Combate à Fome (Ministry of Social Development and Assistance, Family and Fight against Hunger) to implement access control, grant or revoke permissions, and generate reports on data consumption.

Serpro and Dataprev, the public sector technology providers, support the platform's scalability by handling a large volume of daily transactions. This API-based technology approach has enabled more than 200 federal agencies and state governments to use more than 75 APIs for public service delivery.

Data protection

In Brazil, Decree 10.046 (2020) sets the legal guidelines for data sharing among public institutions. The decree characterizes data sharing between public sector entities as "broad," "restricted," and "specific" to ensure access control based on the confidentiality of the data.

Conecta.gov.br's operations are also subject to Brazil's data protection law (LGPD), which lists 10 data access and processing principles. These include purpose limitation, data minimization, and obtaining explicit and informed consent from the data subject. The LGPD also gives individuals (data subjects) rights over their data, such as the ability to access, modify, delete, anonymize, and port their data or to withdraw their consent at any time. Article 7 of the LGPD permits the public administration to process personal data without consent where needed to implement public policies.

While an individual's consent may not be required for data sharing between government entities through Conecta.gov.br, the API Management System is designed to control and monitor data access. This integration of legal principles directly into the platform's technical design is a critical element for trust.

Adoption and effect

Conecta.gov.br transforms the public experience as it automates data retrieval for more than 1,000 public services across various sectors. This makes the individuals and businesses the platform's direct beneficiaries, even though they do not directly interact with it. Therefore, the platform's success should be measured by its dual adoption focus to secure top-down institutional buy-in from government entities and deliver tangible benefits to the public.

The Conecta.gov.br platform has grown remarkably over a short period of time. Its adoption and impact have increased since its launch. Within its first year of operation, approximately 300 integrations were completed, which indicates a steady early adoption by government entities. As of September 2025, the platform has processed more than 2.4 billion transactions since its inception.

The reported economic impact of the platform has been substantial. As of 2025, the platform claims to have generated cumulative savings of BRL 12.98 billion (approximately USD 2.50 billion) for the government and citizens. These savings result from the platform's ability to reduce redundant paperwork, administrative overhead, citizen efforts, and increased efficiency. The quantifiable adoption and economic return metrics provide a compelling case for governments to invest in data sharing DPI. The platform's proven ability to deliver such a significant return on investment is a powerful lesson for other LMICs that seek to modernize their public services.

3.2. CamDX: Cambodia

The absence of data interoperability and mechanisms to check data consistency and verify it in real-time from credible sources forces citizens and businesses to provide the same information to government entities repeatedly. CamDX was developed in 2020 to improve access to verified government data sources without undermining the security and ownership of data.

The Cambodia Data eXchange (CamDX) is a unified yet decentralized data exchange layer that connects different public and private information systems. It enables the provision of services while ensuring confidentiality, integrity, and interoperability of data and the data exchange process between different entities. CamDX works alongside an authentication system known as CamDigiKey that allows users to access various public services as an e-KYC solution and authentication service through a single-sign-on (SSO) system.

National policies, such as the "Digital Society of Cambodia 2021-2035" and the "Digital Government Policy of Cambodia 2022-2025," support CamDX's enablement.

Types of users

CamDX is designed to be an inclusive data sharing ecosystem for the public and private sectors. As per sub-decree 164, public sector entities are automatically enrolled onto CamDX, while private sector entities can apply for membership. As of October 2025, CamDX had 74 total members, out of which 47 are from the private sector and 27 from government entities. Though both categories can access CamDX services, the automatically enrolled members receive services free of charge within the public sector. In contrast, private sector members are subject to a service fee for e-KYC authentication and data use.

Key members of CamDX in the public sector include the Ministry of Economy and Finance, the Ministry of Interior, the Ministry of Commerce, and the National Bank of Cambodia. The platform has also expanded its use in the financial sector by including banks and non-bank financial institutions as its members. Banks, such as PPC, ABA, and Vattanac Bank, have also become recent users.

Use cases

CamDX's primary use case is the online business registration (OBR) platform. This OBR service was one of the first to be enabled using CamDX, allowing users to apply for business registration, pay a fee, and track the status of their application online, from anywhere at any time. The OBR functionality has simplified the process for businesses to obtain business certificates and clearances.

Applicants can register on the government portal through the CamDigiKey application or create a new account if they lack one to access the OBR system. The account creation request is authenticated against the population registry maintained by the Ministry of Interior, facilitated through the CamDX. Once verified, the applicant completes the registration form, pays the applicable fee, and, upon approval, can download the necessary business permits and licenses. The platform also supports the Global Travel Assessment System (GTAS), a service that links airlines and the immigration department to enhance security and facilitate travel processing through e-Visa.

Another important use case of CamDX is electronic know-your-business (e-KYB) and electronic know-your-customer (e-KYC) for the financial services sector. e-KYB enables financial institutions to verify an enterprise's identity, legal status, and compliance by cross-checking business registration, tax data, and enterprise declarations with the Ministry of Commerce, General Department of Taxation, and Ministry of Labor. Similarly, e-KYC is used by banks, insurers, and microfinance institutions (MFIs) to verify a customer's identity instantly. It uses the CamDigiKey authentication system to securely cross-check identity data with the Ministry of Interior's Population Registry, which reduces fraud and processing time for account opening. This variety of use cases shows how sector-neutral interoperable infrastructure can be used to deliver high-value services across multiple sectors.

Technology

CamDX is inspired and modeled after Estonia's X-Road system. The platform operates as a distributed system without a central database, which performs only data exchange among members.

Each participating organization, whether public or private, installs a security server that manages all data exchange. These servers form a peer-to-peer overlay network secured by a national public key infrastructure (PKI). All data exchanges are encrypted, digitally signed, and time-stamped, which ensures confidentiality, integrity, and availability. Notably, CamDX itself does not store the content of data. Instead, it only logs metadata about transactions for audit and monitoring purposes.

Data protection

Two key regulations govern data sharing and personal data protection in Cambodia. Sub-Decree No. 164 (2021) regulates data exchange between the public and private sectors, which ensures the process is secure, transparent, and accountable. Sub-Decree No. 252 (2021) governs the management, use, and protection of personal identification data owned by the Ministry of Interior.

CamDigiKey is governed by Sub-Decree No.207 (2021). As per Article 18 of Sub-Decree No. 207, every data usage from CamDigiKey requires the consent of the CamDigiKey account owner. The CamDigiKey

account owners have the right to know how their identification and personal data are being used. The once-only principle (TOOP), on which the platform operates, ensures that data is collected from citizens and businesses only once, which adheres to data minimization and collection limitation principles of data protection.

While Cambodia does not currently have a comprehensive data protection law in force governing the operation of CamDX, it has initiated the drafting of the Law on Personal Data Protection (LPDP).

Adoption and effect

CamDX has grown steadily since its launch in 2020. As of October 2025, the online business registration platform had approved more than 50,000 business registrations. The total number of data exchange transactions on CamDX has surpassed 97 million since its inception till October 2025.

While citizens are not direct users of the CamDX platform, they are the ultimate beneficiaries of the enhanced services, such as a streamlined online business registration process and the e-KYC solution through CamDigiKey.

The effect of CamDX is evident in the efficiency gains it has produced for citizens and businesses. CamDX claims to improve the ease of business by reducing the months-long process to register a business to an average of just eight working days.

The platform was also acknowledged internationally and awarded the "open source adaptation of the year" in 2022. The functionalities of CamDX, which enable data consistency and real-time verification, have also provided citizens with convenient access to various public and private services.

3.3. InfoHighway: Mauritius

Mauritius' InfoHighway is a government-to-government data sharing system that allows government agencies to share data seamlessly. It was operationalized in 2016 and operates under the Ministry of Information Technology, Communication, and Innovation (MITCI).

The platform was developed to address data sharing concerns faced by government agencies. Before the deployment of InfoHighway, data was often lost in transit between government departments, shared with the wrong recipient, shared freely without any monitoring or supervision, or not made available on time. All of these inefficiencies directly impacted citizens' access to public services in the country. The Government of Mauritius addressed this challenge with InfoHighway, a single, scalable, e-services platform for citizens. The initiative also sought to improve the consumption of published data among government agencies and operational efficiency.

Types of users

Users of InfoHighway are primarily government ministries, agencies, and departments (MDAs). They can be categorized either as publishers or subscribers of data. A publisher is an agency that makes specific data sets available to subscribers in read-only format. Publishers are required to be on the Government

Intranet System (GINS) to share data. Subscribers, on the other hand, are agencies that require information from other government institutions. They can request information from publishers based on a set of search criteria.

InfoHighway has a defined process to onboard users, overseen by MITCI. The publisher and subscriber entities are onboarded through an application form after a consensus about the data to be shared between them. MITCI reviews these requests and assigns them to the InfoHighway team based on priority. Once requisite information is obtained from subscribers and publishers, network configuration is approved, connectivity is tested, and services are confirmed to work as expected, the onboarding request is closed. This entire process is completed within 14 days, and the subscriber starts to receive data from the publisher.

As of October 2025, 33 data publishers are on InfoHighway. These include federal MDAs, such as the Civil Status Division, the Ministry of Social Security, the Ministry of Social Integration, the Corporate Business Registration Department, the Mauritius Revenue Authority, the National Transport Authority, and the Ministry of Education, five municipalities, and seven district councils.

Use cases

Since 2016, InfoHighway has enabled 628 e-services across various sectors, which include education, social security, transportation, policing, immigration, and taxation and revenue.

Two notable use cases of InfoHighway include the validation of applicant identity to issue a skipper's license by the Mauritius Tourism Authority and verification of citizen identity at source during the negative income tax process. In Mauritius, a commercial or private vessel operator in open waters, such as a boat, must obtain a skipper's license. The InfoHighway system's data sharing makes verification of the eligibility and identity of an applicant for a skipper's license more efficient. Similarly, the platform enables efficient validation of citizen identity, directly from the civil status division database, to issue a negative income tax (NIT). The NIT is a system where eligible Mauritian citizens receive financial support from the Government instead of paying taxes.

InfoHighway also enabled real-time data sharing and contact tracing during the COVID-19 pandemic. In 2022, the Bank of Mauritius, the Registrar of Civil Status, and the Mauritius Police Force signed memoranda of understanding to enable information sharing through InfoHighway to establish a central KYC system.

Technology

Mauritius InfoHighway is hosted at the Government Online Centre, a centralized data center that delivers government services to citizens, businesses, government officials, and overseas non-citizens. All InfoHighway servers are hosted on the Government Intranet System (GINS) and are not connected to the Internet. Multiple layers of security are enforced at the data center, government intranet layer, and at the InfoHighway network layer.

InfoHighway uses service-oriented architecture and the publish-and-subscribe model for information sharing between government agencies. Data is published by an authorized government agency, the

publisher, and the same can be accessed by other government agencies that are subscribers. The e-Government interoperability framework prescribes the policies to be mandatorily adhered to when interconnecting different government information systems. A subscriber agency can access data made available by a publisher through three methods:

1. InfoHighway portal: Subscribers can access InfoHighway through a web browser with a username and password to view publisher data. This is typically useful for manual searches and to view datasets.
2. Web service: The module is directly integrated into subscriber applications, where subscribers can make live queries for data access. The InfoPush module uses a push mechanism to transfer data from publisher to subscriber.
3. Extraction: The InfoExtract and InfoSync modules help subscribers extract data based on date or other relevant criteria for high-volume data transfers. The extracted data is shared with subscribers through the secure file transfer protocol (sFTP).

The InfoHighway platform seeks transparency through real-time monitoring by incorporating specially designed interactive tools for data publishers. One such tool is the InfoWatch dashboard, which displays live traffic and other essential statistics at runtime to data publishers.

Data protection

InfoHighway is designed to improve data protection compliance in the public sector's information-sharing process. In January 2018, the Data Protection Act came into force in Mauritius. The law requires the processing of personal data for explicit and specified purposes.

The platform ensures that data usage is restricted to specified purposes, only the rightful data custodians can publish the data, and subscribers are not permitted to forward data to undeclared entities. It also clarifies who provides and consumes data.

While InfoHighway has generally improved data access and management in Mauritius' public sector, it is important to note that the Data Protection Act creates an exemption for any exchange of information on a need-to-know basis between ministries, government departments, and public sector agencies. Therefore, the Data Protection Act in Mauritius does not apply to this type of data sharing among public sector entities. However, data publishers and subscribers still have to comply with many obligations under the law, such as registration with the data protection office and destruction of any personal data after the purpose for retention has been fulfilled.

Besides the Data Protection Act, information exchange between publishers and subscribers is governed by other laws, such as the Cybersecurity and Cybercrime Act 2021, the Electronic Transactions Act, and the Information and Communication Technologies Act.

Adoption and effect

As of October 2025, InfoHighway has responded to about 816 million queries since the platform went live in August 2016. The platform has onboarded 33 data publishers and enables the provision of 628 e-services. The platform also stands out as one of the first G2G national data sharing systems to be operationalized in Africa.

InfoHighway also claims to have led to direct efficiency gains in terms of time and cost savings for both the public sector and residents. Since January 2017, the platform claims to have saved 23.86 years of working time by reducing the delays caused by communication between people and by providing e-services. There is also a notable effect for specific use cases. InfoHighway has enabled online validation of more than 600,000 citizens in a single day to check the eligibility of citizens for negative income tax.

The enabling policy environment played an important role in the early adoption of InfoHighway. For instance, strategic national policies, such as the government's Digital Government Transformation Strategy 2018-2022 and the Digital Mauritius 2030 Strategic Plan, emphasize the importance of enabling digital-by-default services, which operationalize the once-only principle by reusing data for the transformation of government services, and developing government initiatives to promote one-stop shops for e-services.

3.4. UGhub: Uganda

Traditionally, ministries, departments, and agencies (MDAs) in Uganda struggled with redundant data entry, weak governance, multiple security endpoints, and difficulty when they sought to scale or upgrade applications. As more public services moved online, the Government of Uganda recognized that efficient data sharing could improve public service delivery. Subsequently, the National Information Technology Authority–Uganda (NITA-U), under the Ministry of ICT and National Guidance, was assigned to build the digital foundations for e-services delivery.

In response, the NITA-U operationalized UGhub, a national data sharing platform in 2021, to enable seamless and real-time data sharing across government systems to deliver public services. UGhub has two components:

a. A data exchange layer among government databases that operate on the backend;

b. A citizen-facing interface, which enables the delivery of different public services.

UGhub also seeks to enhance data-driven decision-making through dashboards that provide information on transactions conducted by various entities on the platform. The NITA-U also plans to launch a dedicated e-citizen portal and mobile application for UGhub.

Types of users

UGhub's users include ecosystem players, such as government, citizens, and private entities, which include banks, FinTechs, and insurance firms, which rely on data sharing to improve service delivery across Uganda. Through UGhub, MDAs can securely access verified data from other agencies rather than repeatedly request it from citizens. For instance, when a ministry needs to validate a citizen's identity information for specific use cases, it can do so through the NIRA's national ID records with UGhub's secure API layer. Citizens access various digital services from MDAs through UGhub.

Use cases

The UGhub platform facilitates cross-sectoral data sharing across education, healthcare, banking, utilities, and other sectors. This also includes services, such as e-KYC (electronic Know Your Customer), driver permits, identity issuance, passport applications, work permits, and vehicle registrations.

Technology

UGhub is built on the WSO2 technology stack, centered around WSO2's enterprise service bus (ESB), which integrates various systems and services onto one centralized platform. It combines data from various sources into its middleware and transfers it to various public and private sector service providers to inform them of their service provision. The platform consists of three major layers:

1. **Database layer:** Governments and private sector entities first capture citizens' data in their databases. This layer then fetches the raw data through APIs and integrates it. Once retrieved, this data is promptly shared with the middle layer for thorough verification and authentication.
2. **Middle layer:** This layer is the national integration platform, which manages authentication, authorization, API management, data transformation, and performance monitoring.
3. **Application layer:** This layer acts as the interface through which citizens and government administrators interact with the underlying systems, with data received through the middle layer for various functional and analytical purposes.

Data protection

UGhub is governed by Uganda's Data Protection and Privacy Act, 2019, and the Data Protection and Privacy Regulations, 2021. These laws set rules on how to collect, use, and share personal data. It also requires the data to be processed for clear, lawful purposes. UGhub ensures data is used only for approved purposes. These measures protect personal information and maintain trust in Uganda's digital services.

Adoption and effect

As of October 2025, the platform has onboarded 68 government entities and 78 private sector entities. Between January 2022 and May 2024, more than 100 million transactions have been carried out on UGhub by the National Identification and Registration Authority (NIRA), Uganda Revenue Authority (URA), the National Information Technology Authority - Uganda(NITA-U), the Ministry of Public Services (MoPS), and other entities.

UGhub claims to have reduced wait times for passport applications, work permits, and vehicle registrations from several days to a few hours. Before UGhub was deployed, people relied on fixers and intermediaries at offices, such as courts, police stations, and passport or ID centers, to avail of services. The platform reduced the need for these physical interactions. It cut out intermediaries and made public service delivery quicker and more dependable.

4 Building open data ecosystems to drive AI innovations in public service delivery

Across the world, governments and institutions are beginning to use open data as a foundation for AI-based innovation. Dedicated data access platforms make structured and machine-readable datasets accessible. These datasets enable innovators, researchers, and businesses to develop AI solutions in various domains, such as health, mobility, and resource management. For example, the European Union uses open data initiatives to democratize AI access and ensure its benefits are distributed equitably.

Meanwhile, in other countries, such as Colombia, Brazil, Ghana, and the Philippines, governments have established open data portals to publish information held by different government departments. Not all open data portals are established to explicitly enable AI innovation. However, these can nonetheless lower barriers to data access across various sectors. This also demonstrates that governments now understand how data sharing systems have expanded beyond their role to enable interoperability among government information systems.

Governments increasingly recognize the importance of building data access platforms that focus on open data for AI. Such platforms incentivize the public and private sectors to innovate for citizen-focused services. However, the success of these platforms depends on the AI readiness of the data.

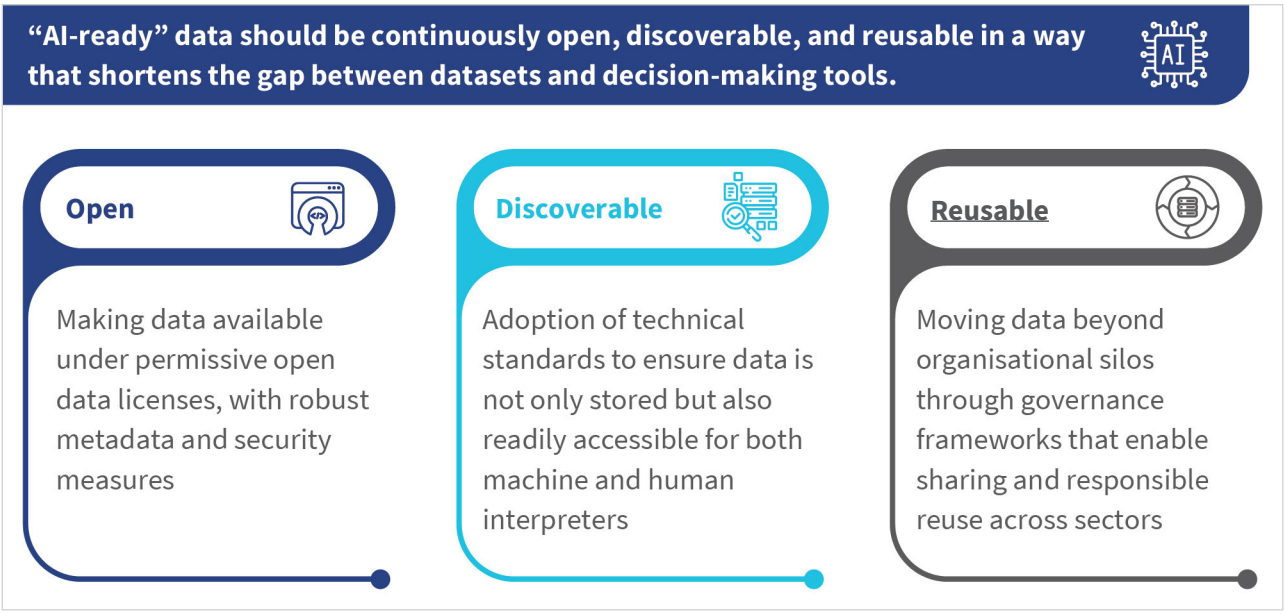


Figure 9: AI-readiness of data

Governments and other stakeholders must evaluate, validate, structure, govern, and share data in ways that support responsible use. In practice, these must build structures based on existing open data and FAIR (Findable, Accessible, Interoperable, Reusable) standards to ensure datasets are of high quality and easily discoverable by people and AI tools. Governments empower local innovators and foreign experts to build AI solutions when they publish data under clear licenses and standards. These AI solutions are built in conformity with privacy and ethical norms for social benefit and enable new AI-driven services, such as predictive analytics or chatbots. "AI-ready" open data that is accessible and well-structured can help extract faster, deeper insights and automate tasks in public services.

The availability of government datasets can catalyze new possibilities for analysis, transparency, and innovation. AI developers can then combine public data, such as linking mobility, weather, and health statistics, to predict disease outbreaks.

Therefore, access to open data will unlock the potential of data-hungry AI applications in the government and the private sector.

Platforms across the world combine open data access with AI toolkits, sandboxes, and use-case libraries. Here are some examples:

AI Hub (South Korea): South Korea launched its AI Hub, a platform designed to accelerate AI innovation with open government data. The platform provides datasets, APIs, and infrastructure to private-sector developers and researchers. Anyone in Korea can download or use data from the platform. The National Information Society Agency (NIA) operates the AI hub and is tasked with the improvement of access to data for AI research and development. The NIA plays a multifaceted role as it provides training data, establishes AI infrastructure and technology standards, and promotes AI-based services in the public sector.

AIKosh (India): AIKosh is a government-led data sharing platform that provides developers and public agencies with datasets, models, and tools to enable AI innovation. It was launched in March 2025 under India's Ministry of Electronics and IT (MeitY) and is part of the IndiaAI Mission. AIKosh is a unified portal of datasets drawn from central or state ministries and private entities. Its objective is to democratize AI access as it provides India-specific data and sandbox features for data analytics and visualization. It has data across various domains, which include agriculture, health, language, and governance.

The platform also provides information on and access to computing toolkits, along with tutorials. AIKosh seeks to support India's digital public infrastructure (DPI) approach by promoting open and responsible use of AI resources for public service innovation.

TGDeX (India): The Government of Telangana in India launched the Telangana Data Exchange (TGDeX) in July 2025 to build AI innovation for public services. TGDeX is a state-driven digital public infrastructure (DPI) that combines the features of an open data portal, a sandbox, and a use case library for AI innovation to improve public services across health, mobility, and food supply, among other areas. The platform seeks to solve challenges that prevent the development and adoption of AI-based solutions to improve public services. These challenges include a lack of curated datasets, limited access to computing, and siloed coordination among government departments.

The platform intends to resolve these issues through AI-ready datasets, pre-trained AI models, a library of use cases, and a sandbox integrated development environment (IDE). As of October 2025, TGDeX hosts 511 data banks, 360 AI models, and 10 use cases that span 21 sectors, such as health, agriculture, urban mobility, and citizen services. The use case collection on TGDeX highlights how access to AI-ready datasets and models from the platform can be used to solve some of these issues in these sectors. The Government of Telangana has also launched the Telangana AI Grand Challenge to provide an opportunity to the ecosystem to work on use cases in sectors, such as healthcare, education, transportation, and beyond.

The development of these platforms highlights a shift toward a growing global consensus. Stakeholders now realize how data sharing systems that enable access to open datasets and AI models can promote data-driven innovation across critical sectors. These data sharing systems connect datasets, models, and users on a single platform. They enable the development of AI-based solutions that can potentially improve efficiency, inclusivity, and citizen outcomes.

As governments, especially in LMICs, publish rich datasets and adopt AI tools, benefits such as innovation in health systems, efficiency in transportation, and climate-resilient agriculture will become more evident. Governments and other stakeholders must remain committed to carefully considering privacy, data protection, inclusion, diversity, innovation, and economic growth. These elements can support AI-driven innovation to flourish on a foundation of open data, accelerating improvements in public services across the developing world.

5 Key challenges and enablers in building and scaling data sharing systems

Governments and other stakeholders need more than technological solutions to build and increase adoption of data sharing systems in low- and middle-income countries (LMICs). Governments need to work together across different levels to align policies, standards, and interoperability frameworks. Other factors that contribute to building and scaling data sharing systems include the readiness of the broader ecosystem and the stability of financial support over time.

Many LMICs face challenges when they integrate all of these elements. When it comes to public service delivery, the stakes are even higher. The benefits of well-designed data sharing systems can be significant, but poorly designed ones can lead to multifaceted issues such as exclusion, especially in LMICs where both citizens and businesses rely heavily on public services.

Examining data sharing systems across different countries reveals both the common challenges they face and the key enablers that help these systems succeed and grow.

5.1. Challenges

In many LMICs, governments and other ecosystem players that seek to develop and scale-up data sharing systems meet a common set of challenges. These challenges are related to technical infrastructure, governance and policy, organizational capacity, and financial sustainability.

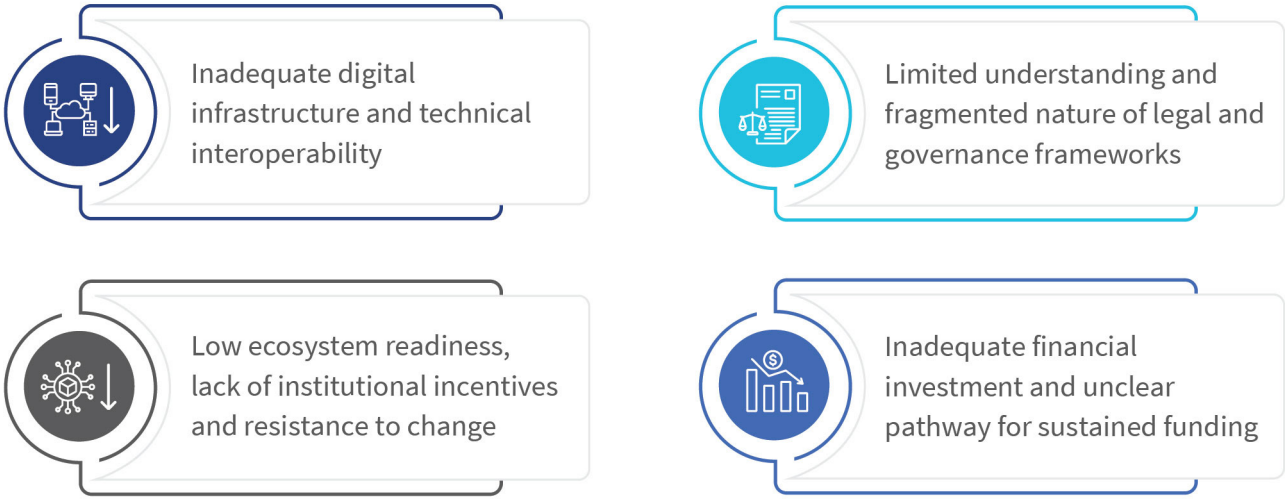


Figure 10: Challenges for LMICs in scaling data sharing systems

1. Technical and infrastructure challenges

- **Inadequate digital infrastructure and connectivity:** The limited availability of digital and ICT infrastructure impacts the development of data sharing systems and the potential of their impact on beneficiaries. For instance, a lack of data centers, cloud infrastructure, and computing resources can hurt the ability of the public sector to ensure steady connectivity to data sharing platforms or networks securely. For beneficiaries of public services, such as citizens and businesses, unreliable internet connections or unaffordable devices mean that even well-designed data sharing systems may remain inaccessible.

- **Technical interoperability gaps:** Legacy systems within ministries and departments sometimes use incompatible formats and interfaces. Poor data quality, inconsistent metadata, and a lack of semantic standards impact the efficiency and scalability of data sharing systems. The integration of heterogeneous systems demands mapping between batch and real-time interfaces, reconciling identifiers, and ensuring consistent timestamping of transactions.

- **Limited digitization and low-quality data:** A significant volume of government data remains undigitized, stored in paper-based or outdated systems that are difficult to integrate. Even digitized data is often incomplete, inconsistent, or lacks standard formats, which restricts its usability for sharing or analysis. These quality and digitization gaps limit the effectiveness of data sharing systems, as they require structured and machine-readable data to function.

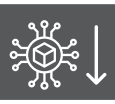
2. Governance and policy challenges

- **Limited understanding of data protection and governance frameworks:** Many LMICs lack national data protection laws and interoperability frameworks that are vital to build a safe and secure data sharing system. Some LMICs have successfully enacted the national data protection law and created a national data strategy and interoperability framework. However, ecosystem players lack adequate understanding when they implement these laws and frameworks.

- **Fragmented or conflicting legal frameworks:** In many LMICs, overlapping or outdated sectoral laws create uncertainty over data ownership, custodianship, and permissible reuse. Conflicting mandates between different levels of governments, regulators, and other agencies lead to a lack

of consensus among different stakeholders. This fragmentation hampers the development of interoperable data sharing systems.

3. Organizational and capacity challenges



- **Limited technical capacity and institutional readiness:** Many public officials in LMICs have minimal exposure to data sharing systems, such as data-exchange platforms, technology architecture, or data-protection principles. Studies have found that data sharing and open-data concepts are often new to public servants, who may not understand their potential returns. This reflects a lack of advanced training and institutional knowledge. A World Bank study finds that "lack of access to infrastructure" and "low technical capacity" severely limit governments' ability to store and share data. Moreover, many institutions struggle to adjust existing administrative processes to new technologies and often maintain parallel paper-based and digital workflows. This duplication undermines the efficiency gains of data sharing systems.

- **Low ecosystem readiness and ineffective coordination:** In LMICs, data often reside in silos maintained on legacy systems, which leads to duplication and reluctance to share. The maturity among ecosystem players, such as ministries, departments, and agencies (MDAs) and private sector entities, varies widely. Meanwhile, coordination mechanisms remain weak. These factors hinder stakeholder buy-in for onboarding MDAs onto data sharing initiatives.

- **Lack of institutional incentives to share data:** Ministries, departments, and agencies (MDAs) have limited motivation to share data, as it often falls outside their formal mandates. In some cases, holding exclusive control over data can strengthen an institution's authority, creating a tendency toward territoriality rather than collaboration. Without clear policies or incentives that reward data sharing, MDAs may prioritize internal control over collective efficiency, which slows the adoption of data sharing systems.

- **Trust deficits and resistance to change:** Stakeholders often fear misuse of data, reputational risk, or loss of control over the information they manage. Citizens, on the other hand, often have privacy concerns. Ministries and departments often resist sharing data due to apprehensions about exposing internal systems or losing institutional autonomy. These trust gaps make it harder for MDAs to collaborate on establishing reliable data sharing systems.

4. Financial sustainability challenges

- **Lack of sustained funding:** Many LMICs face persistent challenges to secure sustained funding to build, maintain, and scale DPI initiatives, which include the data sharing systems. A UN survey notes that Africa faces persistent challenges linked to inadequate investment in e-government development, and similar funding shortfalls are common in other regions. Many of the pilot implementations are donor-funded without clear visibility of financing full-scale implementations.

5.2. Enablers

An examination of how data sharing systems are deployed across different geographies also helps identify the enabling factors for these systems. These enablers can be divided into different categories, such as effective governance, enabling policy and technology framework, the availability and use of national digital ID, sustained efforts to improve stakeholder awareness, and adopting a whole-of-society approach. These elements can create the foundation for interoperable, secure, and inclusive data sharing systems supporting better public service delivery.

Effective governance and leadership: Effective governance is essential to the use of data sharing systems for public service delivery. Clear institutional leadership is critical for coordinated implementation. Governments that designate a nodal authority for data sharing can ensure policy coherence and continuity. For example, Uganda appointed the National Information Technology Authority (NITA-U) as a single institutional anchor to lead the design, build, and scale-up of UGhub.

Enabling policy and regulatory framework: The timely development and adoption of data sharing systems depends on a predictable, enabling policy environment and the availability of data governance and regulatory frameworks. These include data protection laws, e-government interoperability frameworks, and national data strategies. In practice, a sound policy and regulatory framework clarifies the roles of data custodians, publishers, and consumers involved in a data sharing system, protects the rights of individuals, and affixes accountability on all stakeholders.

Technical infrastructure and standards: The creation of scalable data sharing systems in LMICs requires a strong technical foundation anchored in openness and interoperability. The adoption of international open standards, such as OpenAPI and FHIR (Fast Healthcare Interoperability Resources), ensures platform compatibility and reduces dependency on proprietary technologies. Designing systems based on a modular architecture allows components to evolve independently, supporting scale-up and long-term sustainability. These elements form the technical backbone necessary to accelerate the adoption of interoperable, citizen-centric data-sharing systems that enhance public service delivery.

Use of a national digital ID: Though not imperative, the national digital identity can function as a strong enabler to implement and scale up an e-services portal based on an interoperable data sharing system. Residents can verify their identity to access various e-services and avail themselves of different social protection benefits through the national digital ID.

Capacity building and stakeholder awareness: Strong human and institutional capacity is important for successfully implementing data sharing systems. Improved understanding of data sharing systems across different levels of government can be achieved through training, partnerships, and targeted advocacy initiatives. In practice, this means ongoing staff training, boot camps, and ways to identify and empower local champions. Governments can also implement long-term digital skill development programs in collaboration with universities, tech hubs, and the private sector to conduct data sharing and capacity-building sessions. Sustained awareness and capability-building help reduce resistance to change and strengthen stakeholder trust.

Whole-of-society approach to development: The long-term viability of data sharing systems requires a whole-of-society approach. Successful DPI projects often engage the private sector and diversify funding. DPI requires private sector technology vendors, investors, and innovators to thrive. Thus, governments should plan how data sharing systems can also be supported and maintained by the private sector through fair contracting, shared services, or revenue models.

Digital transformation needs to be enabled by clear laws, strong leadership, and skilled institutions. Governments and other stakeholders should establish common technical standards, invest in inclusive infrastructure, and promote collaboration between government, private sector, and civil society to transform how entities securely share data. When these enablers are aligned, they help create a secure and interoperable data ecosystem that improves public service delivery and builds citizen trust.

6 Way forward

If data sharing systems are to be built and scaled, the goals and efforts of all key stakeholders, including governments, academic institutions, ecosystem partners, and funders, should align. Collaborations among these stakeholders can help develop data sharing systems that strategically improve public service delivery in LMICs.

In the data sharing ecosystem, each stakeholder group plays a critical and distinct role. The recommendations outlined below highlight the actions each stakeholder should take to scale data-sharing systems and strengthen public service delivery in LMICs.

Governments

Technical and infrastructure interventions

- Adopt interoperability frameworks and standards
- Define technical requirements for solution providers

Governance and policy interventions

- Adopt and enforce data protection laws
- Harmonize sectoral data frameworks
- Develop a national data strategy
- Prioritize high-impact use cases

Organizational capacity building interventions	• Raise awareness across ministries and local governments to secure data contributor buy-in
Financial sustainability interventions	• Develop a strategy to ensure sustained funding

Governments play a central role as the primary owners and managers of data sharing systems to deliver public services. They are tasked with establishing the foundational building blocks, including regulations and policies, infrastructure, and collaboration mechanisms across institutions.

A key precondition for governments to facilitate data sharing is to adopt or update national data protection laws that establish clear obligations, rights, and enforcement mechanisms for data protection and consent management. The government's adoption of national interoperability frameworks can help maintain common data standards, APIs, service catalogues, and access mechanisms. This is also crucial for the successful adoption of data sharing systems by MDAs across all levels of government.

The government can build trust by enacting clear data protection laws with well-defined mandates. The government can also secure buy-in from data contributors by raising awareness among ministries, regional authorities, and local governments about the efficiency and service delivery improvements that data sharing systems can bring.

A national data strategy should be adopted to complement these efforts. This strategy should define the larger vision for how a country can collect, classify, manage, share, and use data to fulfill its socioeconomic goals. Governments should also harmonize sectoral data governance laws and guidelines so that data flows smoothly across education, health, finance, and other domains and is not held back by conflicting regulations.

Governments can accelerate adoption if they prioritize high-impact use cases, such as social protection, business registration, or tax filing, and scale iteratively. Governments should also actively collaborate with ecosystem partners, such as academia, the private sector, and civil society, to conduct evaluations and impact studies of deployed systems. This would help generate evidence of value and guide scaling strategies.

Further, governments should define technical requirements for solution providers. This could entail mandates that adhere to privacy-by-design and security-by-design principles in all procurements.

Finally, governments should recognize that a "one size fits all" approach does not always work when they develop and adopt national data sharing systems. Each country's infrastructure, needs, institutional maturity, governance structure, and user base differ. Governments should develop a strategy to ensure sustained funding across all phases of development, implementation, and scale-up. This will help maintain the continuity and effectiveness of data sharing systems over time. A phased, customized deployment strategy would allow the government to prioritize high-impact use cases and wider adoption over time.

Funders and donors

Technical and infrastructure interventions	• Support the foundational infrastructure and development of technical standards
Organizational capacity building interventions	• Support readiness assessments, research studies, and learning initiatives
Financial sustainability interventions	• Align efforts with other funders • Target funding based on country context

International development agencies, philanthropic foundations, and multilateral organizations should structure their support strategically. They should align with other funders to provide joint and coordinated funding for national data sharing programs, rather than supporting fragmented initiatives.

Sustained funding is crucial as data sharing systems often require a multi-year commitment for infrastructure, capacity building, and scaling. Funders should also allocate resources to learning initiatives and cross-learning forums, which will enable LMICs to exchange lessons and adopt best practices from other geographies. Finally, funders should support readiness assessments to evaluate the state of infrastructure, institutional maturity, data governance, and ecosystem capabilities. This will ensure that investments are targeted efficiently per the country context.

Research institutes, academia, and think tanks

Technical and infrastructure interventions	• Assess systems and architecture to generate evidence
Governance and policy interventions	• Study governance models to inform policy decisions
Organizational capacity building interventions	• Publish case studies on data sharing systems for cross learning • Conduct impact assessments of data sharing systems

Academic institutions and research groups are key players that can improve the ecosystem-level understanding of how data sharing systems operate. Their research can provide valuable insights into various implementation approaches and their outcomes. They also play a crucial role in ensuring an evolving understanding of how existing data sharing systems impact local ecosystems, what works, what does not, and how these systems can be improved.

Research institutions should also host forums and publish case studies on the successful deployment of data sharing systems, allowing practitioners to learn from cross-jurisdictional experiences. Academia and research institutions can provide independent, evidence-based system maturity and impact assessments. These insights can help governments and funders make informed choices.

Private sector

Technical and infrastructure interventions

- Design interoperable, secure, and open-standard solutions.

Organizational capacity building interventions

- Collaborate to organize innovation challenges and hackathons

Technology vendors and solution providers in the private sector should design interoperable, privacy-by-design, and security-by-design solutions that enable governments to deploy safe and secure data sharing systems quickly. The private sector and other stakeholders should collaborate to run innovation challenges, such as hackathons, to identify use cases in public services through data sharing platforms. These activities may help reveal high-impact use cases and stimulate local talent. The private sector can also help governments reduce the technical skills gaps in data sharing.

When each stakeholder fulfills their role, the path toward interoperable, secure, and trusted data sharing systems becomes achievable. The recommendations in this paper offer a roadmap to guide that journey. The collective ecosystem understanding of data sharing systems can mature when resources are aligned and stakeholders work toward a shared vision, promoting collaboration, consistency, and long-term commitment across all actors involved. This shift can transform data sharing from a technical intervention into a foundational element of better public service delivery across low- and middle-income countries.

Bibliography

1. ABA Bank (Cambodia). “ABA Bank and the Ministry of Economy and Finance — cooperation news.” Accessed October 24, 2025. https://www.ababank.com/aba-news/aba-bank-and-the-ministry-of-economy-and-finance-to-jointly-foster.

2. Agência Gov. “Compartilhamento de Dados Gera Economia de R$ 2,41 Bilhões Entre Janeiro e Outubro de 2024.” Agência Gov, December 2024. Accessed October 24, 2025. https://agenciagov.ebc.com.br/noticias/202412/compartilhamento-de-dados-gera-economia-de-r-2-41-bilhoes-entre-janeiro-e-outubro-de-2024.

3. Agência Nacional de Transportes Terrestres (ANTT). “Passe Livre.” Governo Federal do Brasil. Accessed October 24, 2025. https://www.gov.br/antt/pt-br/assuntos/passageiros/passageiros-rodoviarios/passe-livre.

4. AI Hub (Republic of Korea). “AI Hub.” Accessed October 24, 2025. https://aihub.or.kr.

5. Anumati. “Pricing.” Accessed October 24, 2025. https://www.anumati.co.in/pricing.

6. Bank of Mauritius. “Memoranda of Understanding — media release.” Accessed October 24, 2025. https://www.bom.mu/media/media-releases/bank-mauritius-signs-memoranda-understanding-facilitate-establishment-central-kyc-system.

7. Borger.dk. “Borger.dk (citizen portal).” Accessed October 24, 2025. https://www.borger.dk.

8. Borger.dk. “Life situations — education, family services, retirement.” Accessed October 24, 2025. https://www.borger.dk/hjaelp-og-vejledning/livssituationer.

9. California Health & Human Services (DxF). “Leveraging TEFCA for DxF” (PDF). Accessed October 24, 2025. https://dxf.chhs.ca.gov/wp-content/uploads/2025/05/Leveraging-TEFCA-for-DxF.pdf.

10. CamDX (Cambodia). “CamDX official site.” Accessed October 24, 2025. https://www.camdx.gov.kh.

11. CamDX monitoring. “CamDX monitoring — members/statistics.” Accessed October 24, 2025. https://monitoring.camdx.gov.kh.

12. Central Information Board, Mauritius. eGovernment Interoperability Framework. Accessed October 24, 2025. https://cib.govmu.org/Documents/Maintenance%20Agreement/egiframework.pdf.

13. CIB (Mauritius). “e-Government Interoperability Framework (EGIF) — maintenance agreement.” Accessed October 24, 2025. https://cib.govmu.org/Documents/Maintenance Agreement/egiframework.pdf.

14. Cyber.ee. “Namibia — case studies.” Accessed October 24, 2025. https://cyber.ee/resources/case-studies/namibia.

15. Cybernetica. “Secure Data Exchange.” Cyber.ee. Accessed October 24, 2025. https://cyber.ee/products/secure-data-exchange/.

16. Danish Agency for Digitisation (DIGST). “Mit Overblik (BorgerDK national citizen portal).” Accessed October 24, 2025. https://en.digst.dk/digital-services/borgerdk-national-citizen-portal/mit-overblik.

17. data.gov.gh. “Ghana — about.” Accessed October 24, 2025. https://data.gov.gh/about.

18. data.gov.ph. “Philippines — open data portal.” Accessed October 24, 2025. https://data.gov.ph/index/home.

19. data.gov.uk. “About.” Accessed October 24, 2025. https://www.data.gov.uk/about.

20. dados.gov.br. “Brazil — dados.gov.br (home).” Accessed October 24, 2025. https://dados.gov.br/home.

21. DIAL Global. “Digital public technologies and SDGs” (PDF). Accessed October 24, 2025. https://dial.global/wp-content/uploads/2022/05/Digital_public_technologies_and_SDGs.pdf.

22. DIAL Global. “Effective consent within DPI.” Accessed October 24, 2025. https://dial.global/effective-consent-within-dpi.

23. DIAL Global. “Integrated national data exchange — Uganda case study.” Accessed October 24, 2025. https://dial.global/research/integrated-national-data-exchange-uganda-case-study.

24. DigiQT / Finvu. “Finvu — account aggregator API details.” Accessed October 24, 2025. https://digiqt.com/api-details/india/fintech/account-aggregator-api-finvu.

25. DevelopLocal. “D4D report (2020) — Do not understand its potential returns / hesitant to share data” (PDF). Accessed October 24, 2025. https://www.developlocal.org/wp-content/uploads/2020/07/D4D-report-2020.pdf.

26. Department of Revenue, Government of India. “TINXSYS.” Accessed October 24, 2025. https://dor.gov.in/tinxsys.

27. DLA Piper / Data Protection. “Cambodia — law overview.” Accessed October 24, 2025. https://www.dlapiperdataprotection.com/?t=law&c=KH.

28. Eaves, David, and Krisstina Rao. 2025. “Digital Public Infrastructure: A Framework for Conceptualisation and Measurement.” Working Paper WP 2025-01. UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/sites/bartlett/files/dpi_conceptualisation_and_measurement.pdf.

29. eGov Standards (India). “Interoperability Framework for e-Governance (IFEG) v1.0” (PDF). Accessed October 24, 2025. https://egovstandards.gov.in/sites/default/files/2021-07/Interoperability%20Framework%20For%20e-Governance%20%28IFEG%29%20Ver.1.0.pdf.

30. EUR-Lex (European Union). “Regulation (EU) 2016/679 — General Data Protection Regulation (GDPR).” Accessed October 24, 2025. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

31. European Commission. “Once-Only Principle — system breakthrough (news).” Accessed October 24, 2025. https://commission.europa.eu/news-and-media/news/once-only-principle-system-breakthrough-eus-digital-single-market-2020-11-05_en.

32. European Data Portal / data.europa.eu. “Democratisation of AI through open data — empowering innovation.” Accessed October 24, 2025. https://data.europa.eu/en/news-events/news/democratisation-ai-through-open-data-empowering-innovation.

33. European Data Portal / data.europa.eu. “Leveraging AI — public sector open data (Data Stories).” Accessed October 24, 2025. https://data.europa.eu/en/publications/datastories/leveraging-ai-public-sector-open-data.

34. Gates Foundation. “Digital Public Infrastructure.” Accessed October 29, 2025. https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/digital-public-infrastructure.

35. Gates Foundation. “What Happens to an Economy with Digital Public Infrastructure?” Accessed October 29, 2025. https://www.gatesfoundation.org/ideas/articles/inclusive-economies-digital-public-infrastructure.

36. Governo Eletrônico — ePing (Brazil). “ePing.” Accessed October 24, 2025. https://eping.governoeletronico.gov.br.

37. Governo Federal — Gov.br. “Conecta.gov.br (national interoperability platform).” Accessed October 24, 2025. https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/interoperabilidade/conecta-gov.br.

38. Government of Cambodia — MPTC. “Digital Government Policy of Cambodia 2022–2035” (English PDF). Accessed October 24, 2025. https://asset.cambodia.gov.kh/mptc/media/Cambodia_Digital_Government_Policy_2022_2035_English.pdf.

39. Government of Cambodia — MPTC. “Digital Society of Cambodia 2021–2035 — policy framework” (PDF). Accessed October 24, 2025. https://asset.cambodia.gov.kh/mptc/media/EN-Policy-Framework-of-Digital-Economy-and-Society.pdf.

40. Government of India. Interoperability Framework for e-Governance (IFEG) Version 1.0. July 2021. Accessed October 24, 2025. https://egovstandards.gov.in/sites/default/files/2021-07/Interoperability%20Framework%20For%20e-Governance%20%28IFEG%29%20Ver.1.0.pdf.

41. Government of Mauritius. “Digital Mauritius 2030 — strategic plan (PDF).” Accessed October 24, 2025. https://mdpa.govmu.org/mdpa/wp-content/uploads/2024/04/DigitalMauritius2030.pdf.

42. Government of Mauritius. “Digital Government Transformation Strategy 2018–2022” (PDF). Accessed October 24, 2025. https://govmu.org/EN/infoservices/comm/Documents/Digital%20Government%20Transformation%20Strategy%202018%20-%202022.pdf.

43. Government of Mauritius. “Government Intranet System (GINS).” Accessed October 24, 2025. https://cisd.govmu.org/Pages/gins.aspx.

44. Government of Mauritius. “Government Online Centre — centralized data centre.” Accessed October 24, 2025. https://mitci.govmu.org/mitci/government-online-centre.

45. Government Technology Agency (Singapore). “APEX factsheet” (PDF). Accessed October 24, 2025. https://www.developer.tech.gov.sg/assets/files/apex-factsheet-121222.pdf.

46. GovTech Intel Hub. “Conecta.gov.br — case study.” Accessed October 24, 2025. https://www.govtechintelhub.org/case-study-details/conecta-gov.br:-brazil’s-national-interoperability-platform-for-automated-data-exchange/aJYTG0000000Yxl4AE.

47. Gov.br. “CadÚnico services — API.” Accessed October 24, 2025. https://www.gov.br/conecta/catalogo/apis/cadunico-servicos-dados-familiares.

48. Gov.br. “Citizen base registry (CBC / CPF) — API.” Accessed October 24, 2025. https://www.gov.br/conecta/catalogo/apis/cadastro-base-do-cidadao-cbc-cpf.

49. Gov.br. “Consulta CNPJ — API.” Accessed October 24, 2025. https://www.gov.br/conecta/catalogo/apis/consulta-cnpj.

50. ICTWorks. “Governance — digital public infrastructure success.” Accessed October 24, 2025. https://www.ictworks.org/governance-digital-public-infrastructure-success.

51. ID4Africa. “PS4 Session — Uganda NITA/NIRA” (PDF). Accessed October 24, 2025. https://id4africa.com/2024/ps4/PS4-S2-Uganda-NITA-NIRA-Final.pdf.

52. IndiaAI / AIKosh. “AIKosh.” Accessed October 24, 2025. https://aikosh.indiaai.gov.in/home.

53. InfoHighway (Mauritius). “IH leaflet (v12) — PDF.” Accessed October 24, 2025. https://ih.govmu.org/assets/docs/IH_Leaflet_v12.pdf.

54. InfoHighway (Mauritius). “InfoHighway — application form (public sector)” (PDF). Accessed October 24, 2025. https://ih.govmu.org/assets/docs/InfoHighway_Application_Form_1_-_Public%20Sector_-_v14.1.pdf.

55. InfoHighway (Mauritius). “InfoHighway overview (February 2019)” (PDF). Accessed October 24, 2025. https://ih.govmu.org/assets/docs/InfoHighway_Overview_February_2019.pdf.

56. InfoHighway (Mauritius). “InfoHighway — overview / site (with query string).” Accessed October 24, 2025. https://ih.govmu.org/?_gl=1*m6rtjz*_ga*MTYyOTQxNDQ2Ny4xNzU0NTQ5MDQ1*_ga_JFCCER4YDE*czE3NTkyOTc3MzckbzUkZzAkdDE3NTkyOTc3MzckajYwJGwwJGgw.

57. Irembo. “Support — legal information.” Accessed October 24, 2025. https://irembo.gov.rw/support/legal-information.

58. IT Telangana. “TGDeX — Democratizing AI Innovation through Digital Public Infrastructure — July 2, 2025” (PDF). Accessed October 24, 2025. https://it.telangana.gov.in/wp-content/uploads/2025/07/TGDeX-Democratizing-AI-Innovation-Through-Digital-Public-Infrastructure-2nd-July-2025.pdf.

59. Jamiistack. “Tanzania.” Accessed October 24, 2025. https://www.jamiistack.org.

60. JICA. “Odisha Forest Stack — project detail.” Accessed October 24, 2025. https://www.jica.go.jp/english/about/dx/project/detail/1569311_68029.html.

61. Mazzucato, Mariana, David Eaves, and Beatriz Vasconcellos. 2024. “Digital Public Infrastructure and Public Value: What Is ‘Public’ About DPI?” Working Paper. UCL Institute for Innovation and Public Purpose. https://www.ucl.ac.uk/bartlett/public-purpose/wp2024-05.

62. JICA Open JICAREPORT. “Report PDF (Bhutan).” Accessed October 24, 2025. https://openjicareport.jica.go.jp/pdf/12348769.pdf.

63. MDPA (Mauritius). “Digital Mauritius 2030 — strategic plan (PDF).” Accessed October 24, 2025. https://mdpa.govmu.org/mdpa/wp-content/uploads/2024/04/DigitalMauritius2030.pdf.

64. Ministry of Electronics & IT (MeitY), Government of India. “Digital Personal Data Protection Act (DPDPA)” (PDF). Accessed October 24, 2025. https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf.

65. MITCI (Mauritius). “Government Online Centre — centralized data centre.” Accessed October 24, 2025. https://mitci.govmu.org/mitci/government-online-centre.

66. Minsait (Indra Group). “Interoperability between administration systems” (media room). Accessed October 24, 2025. https://www.minsait.com/es/actualidad/media-room/minsait-facilita-la-interoperabilidad-entre-los-sistemas-de-la-administracion.

67. MyGDX (Malaysia). “MyGDX — landing page / theme.” Accessed October 24, 2025. https://www.mygdx.gov.my/en/landing-page/theme.

68. MySkillsFuture / Singapore. “Digital Certificates (OpenCerts) — FAQ.” Accessed October 24, 2025. https://www.myskillsfuture.gov.sg/content/portal/en/header/faqs/DigitalCertificates.html.

69. National Information Society Agency (NIA), Korea. “NIA — AI infrastructure and technology standards (23000700).” Accessed October 24, 2025. https://eng.nia.or.kr/site/nia_eng/ex/bbs/ListBusiness.do?businessMnCd=23000700.

70. National Information Society Agency (NIA), Korea. “NIA — AI-based services in the public sector (23001000).” Accessed October 24, 2025. https://eng.nia.or.kr/site/nia_eng/ex/bbs/ListBusiness.do?businessMnCd=23001000.

71. National Information Society Agency (NIA), Korea. “NIA — business list (23000900).” Accessed October 24, 2025. https://eng.nia.or.kr/site/nia_eng/ex/bbs/ListBusiness.do?businessMnCd=23000900.

72. National Information Technology Authority — Uganda (demo). “UGHub — integration service.” Accessed October 24, 2025. https://demo.nita.go.ug/nita-u-services/egovernment-services/public-private-digital-systems/integration-service-ughub.

73. National Information Technology Authority Uganda (NITA-U). “Data Protection and Privacy Act, No. 9 of 2019.” December 2019. Accessed October 24, 2025. https://www.nita.go.ug/sites/default/files/2021-12/Data%20Protection%20and%20Privacy%20Act%20No.%209%20of%202019.pdf.

74. NITA-U (Uganda). “Data Protection and Privacy Regulations, 2021” (PDF). Accessed October 24, 2025. https://nita.go.ug/sites/default/files/2022-11/Data_Protection_and_Privacy_Regulations-2021.pdf.

75. NITA-U (Uganda). “UGHub.” Accessed October 24, 2025. https://www.nita.go.ug/ughub.

76. Nigeria Computer Emergency Response Team (ngCERT). “Nigeria Data Protection Act (2023)” (PDF). Accessed October 24, 2025. https://cert.gov.ng/ngcert/resources/Nigeria_Data_Protection_Act_2023.pdf.

77. Nigeria National Data Repository (NDR). “Wallboard.” Accessed October 24, 2025. https://ndr.nascp.gov.ng/public/wallboard.

78. OECD. “G20 compendium on data access and sharing” (PDF). Accessed October 24, 2025. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/09/g20-compendium-on-data-access-and-sharing-across-the-public-sector-and-with-the-private-sector-for-public-interest_13801a1b/df1031a4-en.pdf.

79. OECD.AI. “Government Data Report — practical tool for government data sharing for AI” (PDF). Accessed October 24, 2025. https://wp.oecd.ai/app/uploads/2024/12/Government-Data-Report-A-Practical-Tool-for-Government-Data-Sharing-for-AI.pdf.

80. OECD Legal Instruments. “1980 OECD guidelines (instrument).” Accessed October 24, 2025. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188.

81. OECD OPSI. “CamDX — innovation overview (CamDX-2).” Accessed October 24, 2025. https://oecd-opsi.org/innovations/camdx-2.

82. OECD OPSI. “Centralized digital business license (Chile case).” Accessed October 24, 2025. https://oecd-opsi.org/innovations/centralized-digital-business-license.

83. Open Banking. “Regulatory.” Accessed October 29, 2025. https://www.openbanking.org.uk/regulatory/.

84. Open Development Cambodia. “CamDX presentation (PDF) — Basic CamDX for DG workshop.” Accessed October 24, 2025. https://data.opendevelopmentcambodia.net/en/dataset/18d2f8cb-eae3-4104-8066-774fdfdf-fa6a/resource/71812030-f583-4ff9-a4c1-606ac17c6843/download/presentation-2_basic-camdx-for-dg-workshop-20220331.pdf.

85. Open Development Cambodia. “Decree No. 164 — CamDX laws record.” Accessed October 24, 2025. https://data.opendevelopmentcambodia.net/laws_record/sub-decree-no-164-on-cambodia-data-exchange-through-camdx.

86. Open Development Cambodia. “Sub-Decree No. 164 on Cambodia Data Exchange (CamDX) — resource.” Accessed October 24, 2025. https://data.opendevelopmentcambodia.net/laws_record/sub-decree-no-164-on-cambodia-data-exchange-through-camdx/resource/5f0cdde5-07db-44ec-986a-213a74e72996.

87. PPC Bank (Cambodia). “PPCBank — CamDX.” Accessed October 24, 2025. https://www.ppcbank.com.kh/ppcbank-camdx.

88. Prefeitura de Paracambi / Gov.br. “Governance of data — Conecta-Gov.” Accessed October 24, 2025. https://www.paracambi.rj.leg.br/www.gov.br/governodigital/pt-br/governanca-de-dados/conecta-gov.html.

89. Prefeitura de Vitória da Conquista (Conecta Conquista). “About.” Accessed October 24, 2025. https://conecta-conquista.pmvc.ba.gov.br/sobre.

90. Press Information Bureau, Government of India. “Press release (PRID=1753713).” Accessed October 24, 2025. https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=1753713.

91. Press Information Bureau, Government of India. “Press Release (PRID=2108961).” Accessed October 24, 2025. https://www.pib.gov.in/PressReleasePage.aspx?PRID=2108961.

92. Presidency of the Republic of Brazil. “Decree D9094 (2017) — law on simplifying public services.” Accessed October 24, 2025. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9094.htm.

93. Presidency of the Republic of Brazil. “Decree No. D10046 (2019).” Accessed October 24, 2025. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm.

94. Presidency of the Republic of Brazil. “Law L14129 (2021) — law on digital government.” Accessed October 24, 2025. https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm.

95. Procédure d’adhésion à X-ROAD BJ. Cotonou: Autorité X-Road BJ, n.d. Accessed October 24, 2025. https://www.xroad.bj/publications/documents/procedure-dadhesion-a-xroad-bj

96. Registration Services (Cambodia). “Home — registration services (OBR system).” Accessed October 24, 2025. https://registrationservices.gov.kh/home-en.

97. Registration Services (Cambodia). “Unofficial translation — CamDigiKey sub-decree” (PDF). Accessed October 24, 2025. https://registrationservices.gov.kh/media/2023/09/20230901-Unofficial-translation-Cam-DigiKey-sub-decree.pdf.

98. ScienceDirect. “Article: right to data portability” (journal article page). Accessed October 24, 2025. https://www.sciencedirect.com/science/article/pii/S0267364917303333.

99. SGTraDex. “SGTraDex.” Accessed October 24, 2025. https://sgtradex.com/index.php.

100. Solid Project. “Solid.” Accessed October 29, 2025. https://solidproject.org/.

101. SRN Kementerian Lingkungan Hidup (Indonesia). “National Registry System for Climate Change.” Accessed October 24, 2025. https://srn.kemenlh.go.id/index.php?r=home%2Findex.

102. TGDeX (Telangana). “About us.” Accessed October 24, 2025. https://tgdex.telangana.gov.in/about-us.

103. TGDeX (Telangana). “Potential application — use case collection.” Accessed October 24, 2025. https://tgdex.telangana.gov.in/potential-application.

104. Tourism Authority of Mauritius. “Skipper’s licence.” Accessed October 24, 2025. https://www.tourismauthority.mu/skippers-licence.

105. UNCTAD. “Law on Personal Data Protection — non-official document.” Accessed October 24, 2025. https://unctad.org/system/files/non-official-document/ige7_ecde_p2_Nimul_en.pdf.

106. United Nations / DESA. “UN E-Government Survey 2022.” Accessed October 24, 2025. https://desapublications.un.org/publications/un-e-government-survey-2022.

107. United Nations Department of Economic and Social Affairs (UNDESA). E-Government Survey 2022: The Future of Digital Government. September 2022. Accessed October 24, 2025. https://desapublications.un.org/sites/default/files/publications/2022-09/Web%20version%20E-Government%202022.pdf.

108. Vattanac Bank. “Vattanac Bank joins CamDX — news.” Accessed October 24, 2025. https://www.vattanacbank.com/news/vattanac-bank-joins-camdx-to-enhance-digital-security-and-innovation.

109. World Bank. “Consent-based personal data sharing” (PDF). Accessed October 24, 2025. https://documents1.worldbank.org/curated/en/099425002082230437/pdf/P1705050aeb8e704f088260f228802b73b8.pdf.

110. World Bank. “Digital Public Infrastructure and Development: A World Bank Group Approach” (PDF). Accessed October 29, 2025. https://documents1.worldbank.org/curated/en/099031025172027713/pdf/P505739-84c5073b-9d40-4b83-a211-98b2263e87dd.pdf

111. World Bank. “Interoperability in the public sector” (PDF). Accessed October 24, 2025. https://documents1.worldbank.org/curated/en/099550101092318102/pdf/P1694820242a9c041083900346bab0910eb.pdf.

112. World Bank. “Service Upgrade — The GovTech Approach to Citizen-Centered Services” (PDF). Accessed October 24, 2025. https://thedocs.worldbank.org/en/doc/c7837e4efad1f6d6a1d97d20f2e1fb15-0350062022/original/Service-Upgrade-The-GovTech-Approach-to-Citizen-Centered-Services.pdf.

113. World Bank (ID4D). “Interoperability.” Accessed October 24, 2025. https://id4d.worldbank.org/guide/interoperability.

114. World Bank Blogs (Open Data). “From open data to AI-ready data — building the foundations for re…” Accessed October 24, 2025. https://blogs.worldbank.org/en/opendata/from-open-data-to-ai-ready-data--building-the-foundations-for-re.

115. World Bank Blogs (Open Data). “Toward bridging the data divide.” Accessed October 24, 2025. https://blogs.worldbank.org/en/opendata/toward-bridging-data-divide.

116. World Bank Group. “Interoperability Frameworks.” Identification for Development (ID4D) Guide. Accessed October 28, 2025. https://id4d.worldbank.org/guide/interoperability-frameworks.

117. World Bank Open Knowledge. “Digital Public Infrastructure: Transforming Service Delivery Across Sectors” Accessed October 24, 2025. https://openknowledge.worldbank.org/server/api/core/bitstreams/582c0d73-d367-423c-831d-0640814a7349/content.

118. World Bank Open Knowledge. “GovTech Maturity Index 2022.” Accessed October 24, 2025. https://openknowledge.worldbank.org/server/api/core/bitstreams/5e157ee3-e97a-5e42-bfc0-f1416f3de4de/content.

119. World Economic Forum. “Digital trust.” Accessed October 24, 2025. https://initiatives.weforum.org/digital-trust/home.

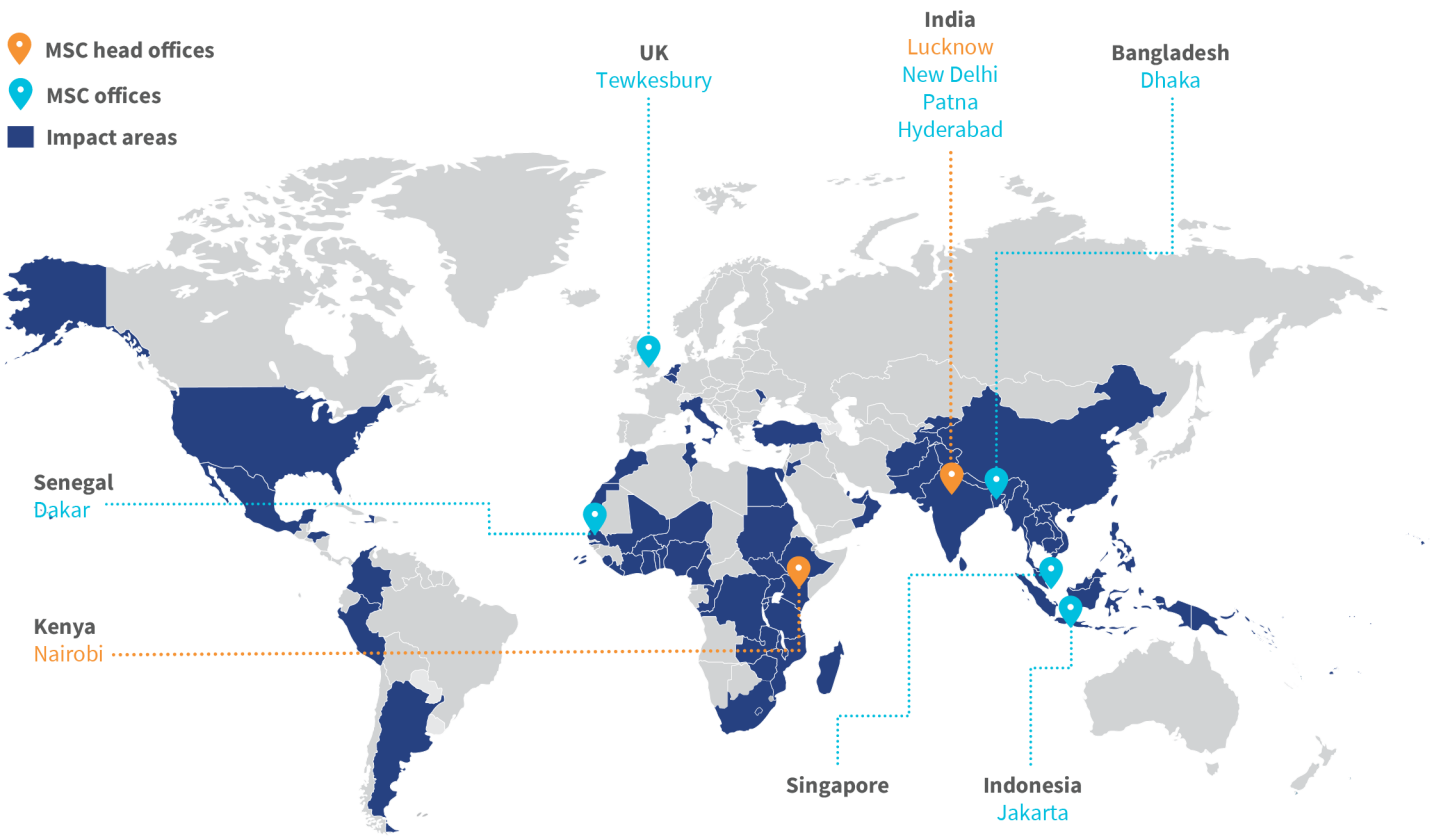
120. WSO2. “Building a digital government in Uganda — conference library (May 2024).” Accessed October 24, 2025. https://wso2.com/library/conference/2024/05/building-a-digital-government-in-uganda.

121. WSO2. “WSO2Con2024 — slides (Building a digital government in Uganda)” (PDF). Accessed October 24, 2025. https://wso2.com/wso2_resources/wso2con2024-slides/building-a-digital-government-in-uganda.pdf.

122. X-Road Global. “CamDX is Cambodia’s national data exchange solution (X-Road case study).” Accessed October 24, 2025. https://x-road.global/xroad-case-studies-library/2024/10/21/camdx-is-cambodias-national-data-exchange-solution-and-its-based-on-x-road.

123. X-Road Global. “Launching citizen-oriented digital services in Colombia (case studies).” Accessed October 24, 2025. https://x-road.global/xroad-case-studies-library/2024/10/21/launching-citizen-oriented-digital-services-in-colombia.

MSC
MicroSave Consulting



Asia head office

28/35, Ground Floor, Princeton Business Park, 16 Ashok Marg,
Lucknow, Uttar Pradesh, India 226001
Tel : +91-522-228-8783 | Fax : +91-522-406-3773

Africa head office

Landmark Plaza, 5th Floor, Argwings Kodhek Road
P.O. Box 76436, Yaya 00508, Nairobi, Kenya
Tel: +254-20-272-4801/272-4806

Email: info@microsave.net | Website: www.microsave.net