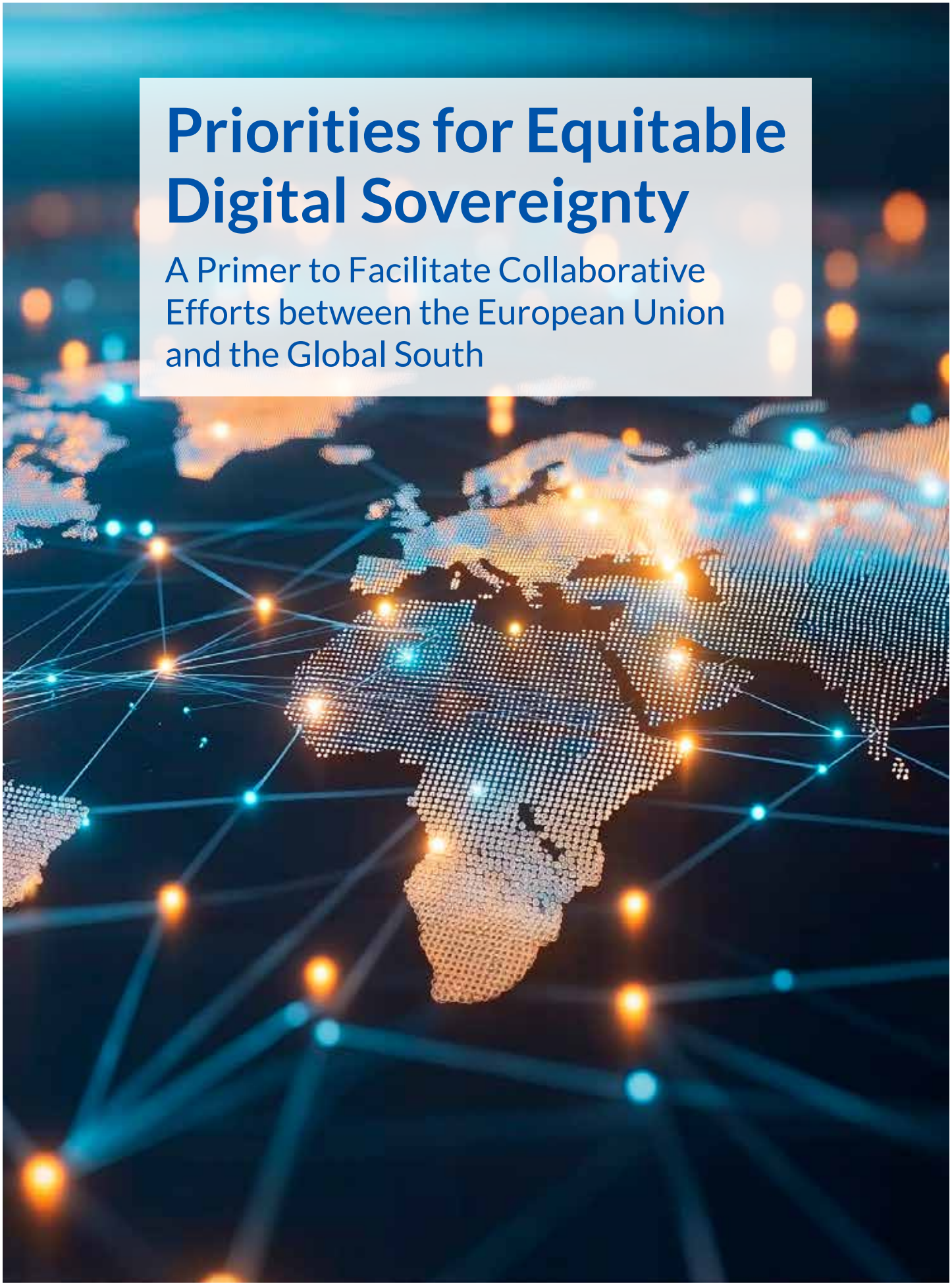
Priorities for Equitable Digital Sovereignty

A Primer to Facilitate Collaborative Efforts between the European Union and the Global South



BertelsmannStiftung

Imprint

© Bertelsmann Stiftung, Gütersloh
August 2026

Publisher
Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
www.bertelsmann-stiftung.de

Responsible
Murali Nair

Authors
Nighat, Astha Kapoor and Kunal Raj Barua
Aapti Institute

Grafic design
Nicole Meyerholz, Bielefeld

Image credits
© Zaifa Art Mart – stock.adobe.com/KI-generiert

Priorities for Equitable Digital Sovereignty

A Primer to Facilitate Collaborative Efforts between the European Union and the Global South

Nighat, Astha Kapoor and Kunal Raj Barua

BertelsmannStiftung

Table of Contents

Priorities for Equitable Digital Sovereignty 5

Intent and direction of this paper 6

1 | What is Digital Sovereignty? 7

2 | Differing Notions of Sovereignty 8
- 2.1 | Overview of Digital Sovereignty 8
- 2.2 | China's Approach to Digital Sovereignty 9
- 2.3 | Digital Sovereignty in the Age of Artificial Intelligence 9

3 | Why are we thinking about digital sovereignty now? 11
- 3.1 | Structural Dependency on Oligopolistic Tech Power 11
- 3.2 | Geopolitical Weaponization of Digital Interdependence 11
- 3.3 | Threats to Internal Sovereignty and Social Cohesion 11
- 3.4 | The Challenge for the Global South 12

4 | Different Models of Digital Sovereignty 13
- 4.1 | European Perspective on Digital Sovereignty 14
- 4.2 | Global South Perspective on Digital Sovereignty 14
- 4.3 | Similarities Between Both Regions 15

5 | Need for Equitable EU-GS Collaboration on Digital Sovereignty 16

6 | Driving Factors for Equitable EU-GS Collaborations[2] 18
- 6.1 | Sharing Best Practices 18
- 6.2 | Bridge-building and Norm-setting 18
- 6.3 | Value-based Convergence 18
- 6.4 | Infrastructure Partnerships 18
- 6.5 | Talent Partnerships 19

7 | Possible Nodes of Collaboration 20
- Example 1 | The EU-Brazil Data Corridor: Value-based Convergence in Practice 21
- Example 2 | Digital Public Infrastructure: Peer Learning & Future Interoperability 21

8 | Three-Year Roadmap for Collaboration 22
- 8.1 | Situating the Roadmap within the ETRS Framework 23

Annexure A | Potential Nodes for Collaboration 24

Priorities for Equitable Digital Sovereignty[1]

Key Insights

- In a rapidly evolving technological landscape, where resources are concentrated in the USA and China, sovereignty for most nations lies in the ability to govern technology within their borders and make deliberate trade-offs to maintain leverage over heavily dependent supply chains.[1]

- The European Union (EU) model is a defense-first idea focused on protecting its market and democratic values from external dependencies. In contrast, the Global South (GS) model is closer to a more developmental idea aimed at preventing digital colonialism and securing a place in the global value chain.

- Despite their different approaches, both the EU and GS appear united to find alternatives to the US-China duopoly and their quest for a 'third path' in the global digital order.

- Meaningful partnerships require identifying and targeting specific leverage points across the digital stack, instead of broad declarations. There is a need for shared agenda-setting, co-investment in infrastructure, and reciprocal talent partnerships that empower communities, not just states.

1 This policy primer is based on developments in the digital sovereignty discourse and its surrounding geopolitical circumstances till February 2026 only.

Intent and direction of this paper

This policy brief is intended as a **primer to frame and inform an ongoing conversation**, not as a definitive solution to the challenges it discusses. The question of identifying equitable priorities between the European Union and countries across the Global South, particularly in rapidly evolving domains such as technology governance and digital cooperation, is complex and continually evolving. Its purpose is to **surface key considerations, highlight areas of alignment and tension, and contribute to creating a more level playing field for dialogue and engagement**.

Policy priorities, geopolitical relationships, technological capabilities, and institutional arrangements change frequently. The insights presented here should therefore be read as **contextual observations at a particular moment in time**, rather than fixed conclusions. We acknowledge that developments in this space may quickly reshape the underlying assumptions and therefore want this to be a starting point for identifying collaborative avenues to strengthen global dialogue.

This brief also **does not attempt to capture the full complexity of the broader ecosystem**. The EU–Global South relationship spans a wide range of political, economic, technological, and developmental considerations. While this paper draws attention to several important themes, it represents only one entry point into a much larger and more nuanced landscape.

Importantly, this document forms an initial phase of a broader project. The work presented here is primarily exploratory in nature. Subsequent phases of the project will move toward more dynamic, collaborative, and context-specific engagement, including deeper consultation with stakeholders and the co-development of approaches that respond to the priorities identified in this primer.

Taken together, this document should be understood as **a starting point for discussion and collaboration**, rather than a final statement of position or policy recommendation.

1 | What is Digital Sovereignty?

Digital sovereignty can be broadly understood as the exercise of agency and power by a political or social entity, such as a nation-state, a community, or an individual, to shape the digital infrastructure, data, services, and protocols that underpin modern life. It moves beyond the traditional, purely legalistic notion of sovereignty as territorial control, encompassing both the normative right to govern and the material capacity for self-sufficient action in the digital realm.

The essence of digital sovereignty can be traced back to debates starting in the 1990s over cyberspace sovereignty, which questioned whether the emergent, borderless internet could be subjected to the authority of territorial nation-states. However, the term is regaining popularity with the increasing politicisation of technology. Scholars argue that the issue is no longer a non-territorial challenge limited to the virtual realm; instead, digital sovereignty has become a larger concept, capturing the digital transformation of societies — one that tries to reflect the search for autonomy and self-sufficiency by nations across the globe.

This paper seeks to unpack this complex landscape. First, it examines the many notions of digital sovereignty. Second, it explores why this idea is becoming an inescapable priority for nations around the globe. Third, it contrasts the models emerging from the European Union (EU) and the Global South (GS), documenting their goals, tools, and originating tensions. Finally, through this comparative lens, it seeks to identify points of commonality or intersection between the EU and GS for strategic alignments that could enable a meaningful and equitable collaboration.

2 | Differing Notions of Sovereignty

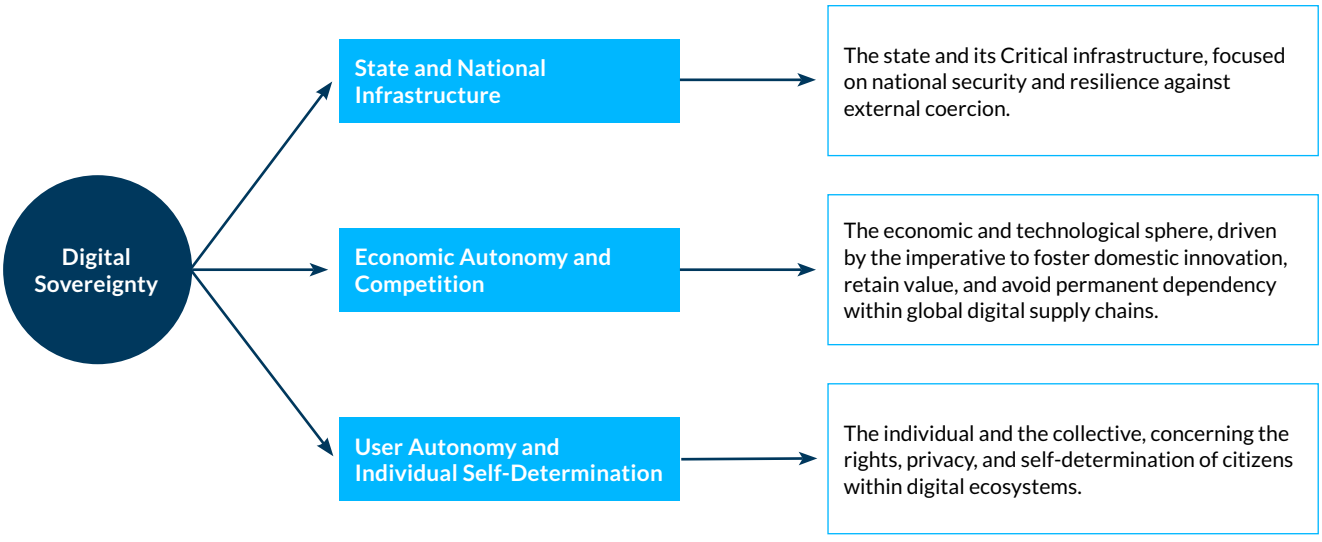
2.1 | Overview of Digital Sovereignty

Given the lack of a uniform or operational definition, digital sovereignty takes on many meanings and is often even used interchangeably with terms such as data sovereignty. It becomes critical to understand the core differences between these terms before embarking on a global mission for equitable collaboration.

At its broadest, digital sovereignty refers to a nation's project to assert control over its digital ecosystem, encompassing infrastructure, platforms, and standards to reduce foreign dependency and surveillance. This pursuit gained urgent political traction following the mass surveillance revelations by Edward Snowden and WikiLeaks, which exposed fundamental vulnerabilities in the global digital order.

One of the most common strategic responses to these vulnerabilities has been the pursuit of data sovereignty. This narrower concept focuses specifically on subjecting data, particularly data that is of critical importance to national security, to national laws and regulations. Its tools are predominantly legal and regulatory, such as data protection laws, data localization mandates, and rules governing cross-border data flows. In short, while digital sovereignty asks, "Who controls the technological system?" data sovereignty asks, "Who has the legal right to control, access, and derive value from the data within it?"

Figure 1 | **Interconnected Spheres of Digital Sovereignty**



Source: Pohle, J. and Thiel, T. (2020). Digital sovereignty. Internet Policy Review, 9(4)

Thus, data sovereignty often functions as a critical component or first step within the larger, more ambitious pursuit of digital sovereignty. A state may enact data localization to protect citizen privacy, but achieving holistic digital sovereignty requires moving beyond regulation to build or control the underlying cloud infrastructure, develop indigenous platforms, and foster a competitive domestic tech industry.

While there are many notions of digital sovereignty, a key framework (Figure 1) has conceptualised core layers of digital sovereignty across three interrelated spheres:

1. **The state and national infrastructure sphere:** control over physical and logical networks.

2. **The economic autonomy and competition sphere:** governance of data flows, economic value, and innovation.

3. **The user autonomy and individual self-determination sphere:** jurisdiction, normative values, and governance of online information.

The central dilemma of our time is that asserting sovereignty in one sphere, such as mandating data control for national security, can directly challenge it in another by potentially stifling economic competition or enabling surveillance that undermines citizen rights. It is within this complex, multi-layered context that nations are now navigating their digital futures.

2.2 | China's Approach to Digital Sovereignty

China is one of the few nations that has mastered effectively navigating between these tensions. It offers the clearest illustration of a state-centric model. It has a long history of leveraging information control as a tool for its political strategy. They exhibit comprehensive control over all three spheres — infrastructure (the Great Firewall), economic (state-backed champions like Huawei), and user autonomy (extensive filtering of information). China has been able to achieve this version of technology autarky due to extensive state investment and a relatively lax regulatory environment in the early 2000s, which enabled an entrepreneurial boom and eventually allowed indigenous technology to thrive. To keep its vision of digital sovereignty alive, in a constantly evolving world, the state has issued multiple laws and policies across all levels, in addition to initiatives like the Digital Silk Road.

2.3 | Digital Sovereignty in the Age of Artificial Intelligence

Digital sovereignty is a malleable political concept prone to reinterpretation with major technological shifts. This holds in the face of the massive technological shift brought about by the global adoption of artificial intelligence (AI). Self-sufficiency in deploying AI models requires tremendous amounts of resources to cater to each layer of the AI stack, from semiconductors to data. A large part of this capacity is concentrated in China and the US, controlling over 90% of the global AI data-centre needs. In reality, most countries cannot sustain core AI infrastructure themselves, nor can they afford or adapt this technology entirely. This creates a catch-22 situation, which inevitably increases the very dependencies digital sovereignty seeks to reduce.

Consequently, the pursuit of AI sovereignty necessitates a fundamental redefinition of the term itself, moving from an ideal of absolute independence to one of strategic agency within interdependence. As scholars argue, effective sovereignty in this context is less about dominating every layer of the stack and more about a state's capacity to govern how AI systems operate within its territory and to adapt the technology to align with national priorities. This translates into a series of deliberate, future-oriented trade-offs. A nation might, for instance, attract foreign investment in compute infrastructure while enforcing strict local regulations on AI deployment.

This section illustrates that digital sovereignty is a fluid concept that continues to evolve in response to major technological revolutions. The shift from the internet era to the age of AI has fundamentally altered what sovereignty means and how it is pursued. While China's model of comprehensive state control and technological isolation represented a plausible vision in earlier phases of digital development, the structural realities of AI render such ambitions unattainable for many. This evolution underscores the central argument of this paper: sovereignty today is less about building walls and more about cultivating leverage.

3 | Why are we thinking about digital sovereignty now?

The convergence of structural dependency, geopolitical tensions, and threats to internal sovereignty has made digital sovereignty an urgent priority for nations worldwide. Several interconnected drivers explain this heightened focus.

3.1 | Structural Dependency on Oligopolistic Tech Power

Decades of concentrated innovation have created dependencies where nations find their economic and administrative functions reliant on a narrow set of external technologies and platforms. The global digital economy is dominated by a tight oligopoly of U.S. hyperscalers like Amazon Web Services, Microsoft Azure, and Google Cloud. Collectively, they control an estimated 63% of the global cloud infrastructure that forms the foundational layer for modern economies. This concentration is not incidental but stems from capital investment that creates insurmountable barriers to entry. As a result, in regions like the EU, up to 90% of critical infrastructure is owned by non-EU and primarily American entities.

This reliance turns commercial relationships into potential vulnerabilities, as control over critical services could be used as a geopolitical instrument. This risk emerged in the case of Microsoft's compliance-driven suspension of services to India's Nayara Energy. This incident demonstrated how essential operational capabilities can be unilaterally disrupted from afar, reframing foreign digital infrastructure as a direct security concern.

3.2 | Geopolitical Weaponization of Digital Interdependence

Digital infrastructure has now become a major arena for geopolitical power struggles, where tech dominance is leveraged to contest national sovereignty. Brazil's recent push to expand domestic data centre capacity, in pursuit of digital sovereignty, illustrates this complexity. While the government offers tax incentives for local infrastructure, most new facilities will likely be owned by US hyperscalers like AWS or Google. Data stored in Brazil is potentially subject to the US CLOUD Act, which compels American companies to hand over data upon request by US authorities, regardless of physical location, meaning that hosting data locally does not necessarily deliver sovereignty.

3.3 | Threats to Internal Sovereignty and Social Cohesion

Cyber-attacks, disinformation campaigns, and other malicious uses of social media to destabilise a society represent a direct threat to a nation's internal sovereignty. For example, Brazil suspended the operations of social media platform X (formerly Twitter) due to non-compliance with its judicial orders, particularly stressing the value of sovereignty, democracy, and compliance with Brazilian laws. The weaponisation of digital platforms to undermine national institutions and social cohesion has added to this urgency, resulting in state intervention seeking to reassert control.

3.4 | The Challenge for the Global South

The convergence of structural dependency, geopolitical tensions, and threats to internal sovereignty has set the stage for nations to pursue digital sovereignty. Moreover, within this global struggle, the GS faces a distinct and compounded set of challenges. Its pursuit of sovereignty is not merely a reaction to corporate power or Northern regulations. At its core, it is a project of post-colonial economic self-determination and state-building. The threat is not merely dependency, but what scholars term as digital colonialism — understood as the risk of being permanently locked into a peripheral role as data providers and technology consumers in the global digital economy.

4 | Different Models of Digital Sovereignty

The divergent positions of the EU and GS within the global digital hierarchy have given rise to contrasting models of digital sovereignty, summarized in the table below.

Table 1 | **Summary of models between the EU and GS nations**

Dimension	Region/Country				
	European Union	India	Brazil	Africa	ASEAN
Core Motivation	Defend its single market, democratic values, and strategic autonomy from the overdependence on US and Chinese technology.	Achieve technological self-reliance and drive inclusive development at scale, moving from being a consumer to a creator of digital value.	Assert democratic self-determination and national jurisdiction over digital platforms seen as threatening public order and institutional integrity.	Overcome fragmentation and achieve developmental agency by escaping the digital sovereignty trap of one-sided deals with foreign powers.	Build a single digital market and harness digital transformation for growth, while balancing relations with major tech powers (U.S., China).
Tools	**1. The Brussels Effect:** Using market size to set global standards (GDPR, DMA). **2. Federated Infrastructure:** Building alternatives (e.g., Gaia-X) via industrial policy.	**1. Digital Public Infrastructure (DPI):** State-led creation of open, interoperable "digital rails" (Aadhaar, UPI). **2. Data Protection Laws:** Establishing comprehensive domestic frameworks for data governance (e.g., DPDP Act, 2023)	**1. Judicial Assertiveness:** Supreme Court rulings applying "constitutional immediacy" to digital space. **2. Comprehensive Legislation & DPI:** Laws like the LGPD (data protection) and Pix payment system **3. Industrial Policy:** Initiatives like Redata to spur domestic data center growth	**1. Regional Coordination:** Harmonizing policy via the African Union Data Policy Framework. **2. Strategic Localization:** Mandating in-country data storage while seeking foreign investment for green data centers (e.g., Kenya).	**1. ASEAN Framework on Digital Data Governance (2021):** Promotes data flows with trust, but stops short of a common data law. **2. Regional Harmonization:** Model Contractual Clauses for Cross-Border Data Flows **3. Projects for digital trade & payments integration:** ASEAN Payments Connectivity initiative.
Examples	GDPR, DMA, Gaia-X, EuroStack	India Stack	Suspension of platform X	Kenya's suspension of Worldcoin	Yet to be implemented
Core Tension	Regulation v/s innovation struggle	Sovereignty v/s pragmatism struggle	Geopolitical tensions	Severe infrastructural deficits	Regional fragmentation due to diverse priorities and state capacities

4.1 | European Perspective on Digital Sovereignty

The idea of digital sovereignty in the European Union (EU) is primarily a defensive geopolitical project focused on strategic autonomy. It is driven by the threat of dependency on foreign (US and Chinese) technology, which is seen as a vulnerability to coercion and a loss of regulatory control. Perspectives range from building a comprehensive 'EuroStack' of sovereign digital infrastructure to leveraging the 'Brussels Effect' and establishing global rules. A critical view warns against the co-option of these efforts by U.S. hyperscalers marketing "sovereign" but foreign-owned data centres, arguing true sovereignty requires publicly coordinated alternative assets. More recently, France has moved to ban government officials from using video tools produced by US tech companies; instead they are to use Visio, the French alternative.

4.2 | Global South Perspective on Digital Sovereignty

In contrast, GS broadly frames sovereignty as a developmental imperative. The primary goal is not only autonomy but also the development of foundational capacity for growth and leapfrogging. The threat is not just dependency but exclusion from digital value chains and technological irrelevance, risking permanent peripheral status in the digital economy.

However, the GS is not a monolith, and the idea of digital sovereignty varies across nations. For example, India and Brazil complement their regulatory arsenal with deep investment in Digital Public Infrastructure (DPI), such as the Unified Payments Interface (UPI) in India and Pix in Brazil. This vision of sovereignty as active capability-building, rather than passive technology consumption, was heard at the 2026 AI Impact Summit:

> *"Developing countries cannot remain mere consumers of technology. They must build their own capabilities through technology transfer, talent development, and sovereign infrastructure."*
> ***Luciana Santos (Brazil's Minister of Science, Technology, and Innovation)***

South Africa, on the other hand, operates from a more constrained position. Lacking the technological and economic resources of India or Brazil, it leverages foreign technology while focusing on rights-based regulation anchored in its post-apartheid constitution, using domestic data laws like the Protection of Personal Information Act (POPIA) to assert sovereignty where it can.

Elsewhere in Africa and Southeast Asia, nations are navigating the competing overtures of US and Chinese technology powers. Data centre investments, 5G deployments, and digital infrastructure projects from both sides force countries like Nigeria, Kenya, Indonesia, and Vietnam to make strategic choices or to hedge, accepting investment from both while maintaining policy space. This has spurred a rise in data protection initiatives across the region, as countries assert regulatory authority even where they lack technological self-sufficiency.

> *"If Africa does not define its own AI future, others will, and they are already trying to define it for us."*
> ***Ambassador Philip Thigo (Kenya's Special Envoy on Technology)***

Thigo's warning underscores the common thread across this diversity: the cost of inaction is not merely dependency but having one's future defined by others. The challenge for Global South nations is not to replicate any single model, but to build the institutional capacity, regulatory expertise, and strategic agency to participate in shaping the digital order on their own terms.

This warning is given urgent material reality by the scale of Big Tech's current infrastructure push across the Global South. Hyperscalers like Google, Amazon, Microsoft, and Meta are racing to build massive data centre networks across Latin America, Africa, and Southeast Asia. These infrastructure projects are not neutral. Instead, they embed foreign-owned and foreign-controlled physical assets deep within national territories, often accompanied by generous tax incentives and weak local governance requirements. Rafael Grohmann highlights how this dynamic has given rise to a new idea of Big Tech selling Sovereignty as a Service to GS governments.

> *"If you are a government in the Global South and you want to be sovereign but you don't have infrastructure or money to be sovereign, we can sell sovereignty to you."*
> ***Rafael Grohmann (Assistant Professor, University of Toronto)***

This idea of reducing sovereignty to a product offers the appearance of control while leaving the underlying structures of ownership, intellectual property, and jurisdictional power untouched. Therefore, for GS nations, the challenge is not merely to attract infrastructure investment, but to build the governance frameworks and technical capacity that make genuine ownership possible.

4.3 | Similarities Between Both Regions

Despite their divergent methods, the EU and GS models of digital sovereignty are fundamentally aligned in their diagnosis of the problem and their rejection of the status quo. At their core, both models are strategic reactions to a world where technological power is overwhelmingly concentrated. They share a recognition that the dominance of global rivalry has created an untenable situation. This shared geopolitical reality sets the scene for the EU to achieve strategic autonomy and GS to pursue developmental agency.

As a result, both blocs are realizing the value of infrastructure to support their legal architecture. They acknowledge that abstract governance or regulatory posturing is insufficient. Meaningful sovereignty requires a foundation of physical or operational control over key digital assets, whether it is the EU investing in Gaia-X and semiconductor plants to reduce critical external dependencies, or India and Brazil building digital public infrastructure (UPI, Pix) and data localization frameworks.

The EU seeks to rebalance this interdependence by dictating the rules of engagement through its regulatory superpower. GS seeks to rebalance it by increasing its infrastructural leverage and bargaining power. Their paths differ, but the destination is aligned: a shift from passive integration into global digital supply chains to active, strategic management of those connections to serve national and regional interests.

5 | Need for Equitable EU-GS Collaboration on Digital Sovereignty

Experts describe a partnership defined by shared pressures but divergent logics. Both the EU and GS seek to reduce dependency on tech hegemonies. While the EU pursues digital sovereignty as a rights-based regulatory project, key GS powers treat it as a fluid strategic narrative focused on development, economic security, or post-colonial autonomy. This ambiguity reflects a structural constraint. GS nations face a persistent tradeoff between developmental dependency and status aspirations, often resulting in strategic agnosticism. This can materialise as engagement on technical, low-controversy issues while avoiding positions that risk vital economic partnerships.

Despite these asymmetries, a strategic collaboration between the EU and GS offers an opportunity to reshape the global digital order. It charts a third path beyond the binary of market extractivism and state cybernationalism. This path would be rooted in rights, interoperability, and strategic autonomy, but would hinge on equity as a non-negotiable foundation. This collaboration has the potential to incentivize high-standard innovation and offer emerging economies a route to digital development that does not compromise fundamental rights. As the EU-Brazil model shows, collaboration must be grounded in mutual recognition and respect for each region's own regulatory frameworks and developmental objectives. It is important to avoid a dynamic where the GS serves merely as a market or a source of skill. An equitable approach requires shared agenda-setting, co-investment in capacity, and benefits designed to strengthen domestic innovation ecosystems in both regions.

This vision must also extend beyond state diplomacy to include bottom-up sovereignty — the agency of communities and civil society in shaping digital ecosystems that reflect their own needs. This grassroots layer is a vital source of resilience. When governance gaps emerge, Big Tech rushes to fill the vacuum, and in the ensuing struggle between state and corporate power, citizens' voices are systematically lost. Creating channels for people-to-people connections roots collaboration in shared practical challenges and democratic accountability, preventing outcomes that reinforce top-down power imbalances. Conceptualising sovereignty as a multi-layered practice, from the community up, can make EU-GS partnerships more responsive to the needs they aim to serve.

Trade agreements have regained prominence as instruments of geopolitical alignment, with the EU pursuing ambitious Free Trade Agreements with key Global South partners, including the recently signed EU-India FTA. These agreements signal political commitment and create frameworks for economic cooperation. However, in their current form, FTAs are ill-suited to drive meaningful collaboration on digital sovereignty. They still contain power asymmetries, which inevitably shape outcomes in favor of the stronger party. Furthermore, they remain fundamentally too broad to address the granular, layer-specific challenges that define digital sovereignty. While they may include chapters on data flows or e-commerce, they cannot operationalise the targeted, issue-specific collaboration needed to build shared capacity.

Therefore, a more useful way to think about equitable EU-GS collaboration is by identifying and targeting specific sites or leverage points where common interests can be met or aligned upon. The path forward lies in issue-specific, granular collaboration, where pooled resources, regulatory insight, and shared technical standards can incrementally reshape dependencies.

The following section elaborates on these factors, offering a framework for moving beyond the limitations of broad trade diplomacy towards targeted and reciprocal partnerships.

6 | Driving Factors for Equitable EU-GS Collaborations[2]

The analysis of existing narratives indicates a five-pronged approach that could support the identification of equitable pathways or sites where collaboration could be explored.

6.1 | Sharing Best Practices

This driver leverages proven practices originating from GS countries, such as Brazil's instant payment system (Pix), to inform solutions for similar problems faced across the EU. For this to function as a driver for collaboration, it must be framed as peer learning and not technical assistance. This requires the EU to acknowledge innovation leadership from the GS in specific domains and move towards a reciprocal exchange of knowledge.

6.2 | Bridge-building and Norm-setting

This driver utilises mutual regulatory recognition to create trusted, rules-based spaces that offer an alternative to the US-China tech polarisation. It positions certain GS countries as conveners capable of facilitating dialogue on technical standards and governance norms. However, the success of this driver is contingent on the EU's willingness to share agenda-setting power. The viability of this driver depends heavily on the bridge-builder's technical capacity, diplomatic credibility, and perceived non-alignment.

6.3 | Value-based Convergence

This driver fosters partnerships in which domestic political imperatives within a GS country align with the EU's rights-based framework. The recent EU-Brazil tech diplomacy corridor for trusted data is a significant milestone for collaborations between both regions. For this driver to be equitable, convergence must be issue-specific, institutionally grounded, and reciprocally structured, so that the collaboration becomes a diplomatic commitment to continuous regulatory dialogue rather than a static compliance exercise. Value-based partnerships cannot be built on the EU projecting its rules outward, but on recognising and investing in the regulatory agency and constitutional trajectories of its GS partner.

6.4 | Infrastructure Partnerships

This driver addresses the foundational layer of digital sovereignty: the physical and logical infrastructure upon which data and services depend, including subsea cables, cloud facilities, and 5G networks. For EU-GS collaboration, this means moving beyond treating infrastructure as a turnkey import towards co-investment, joint ownership, and technology transfer that build long-term domestic capacity. Equitable conditions require that GS partners hold meaningful governance stakes in shared infrastructure, that procurement processes do not replicate dependencies on European vendors, and that intellectual property and operational control be negotiated as shared assets rather than conceded as market access.

2 These driving factors are derived from multiple expert interviews conducted as part of the research for this primer.

6.5 | Talent Partnerships

This driver moves beyond the extractive “brain drain” dynamic toward structured, reciprocal capacity-building in the knowledge economy. This can encompass co-funded research fellowships, regulator-to-regulator exchange programs, and joint research consortia with equitable intellectual property frameworks. Success in this driver is measured not by the volume of talent, but by the durable strengthening of research ecosystems, policy expertise, and technical leadership. This requires explicit provisions for co-authorship, co-patenting, as well as EU investment in Global South-led research agendas rather than simply hosting GS researchers within European priorities.

7 | Possible Nodes of Collaboration

The five driving factors outlined in section 6 provide a conceptual framework for understanding how equitable collaboration can occur. However, identifying these drivers and their nuances is only the first step. To derive operational value and actionable policy, they must be mapped to specific layers of the digital stack where collaboration can manifest. The table in Annexure A illustrates this mapping of how each driver can present across six critical nodes of the global supply chain — data, models, compute, talent, applications, and governance. These nodes of collaboration stem from the core tenet of this paper — digital sovereignty cannot be pursued as a monolithic project. It must be built across layers and at specific points where dependencies converge with shared interests.

The six layers outlined here represent the essential components of the digital stack. Data serves as the foundational asset over which sovereignty is established. Models reflect the algorithmic logic that influences economic and social outcomes. Compute provides the necessary infrastructure to support both data and models. Talent is the human capital required to drive innovation. Applications deliver digital services to citizens, while governance establishes the rules that connect all the layers.

Existing attempts illustrate the different collaboration models possible for the EU and GS by mapping the driving factors across this stack. For example, the EU-Brazil data exchange corridor exemplifies bridge-building and value-based convergence for data. This layered approach ensures that collaboration is targeted, context-sensitive, and capable of addressing specific challenges, rather than merely relying on broad diplomatic statements.

This framework of drivers and stack layers also informs the three-year roadmap of collaboration (section 8). Phase 1, focused on foundation building and trust-building, is designed precisely to operationalize the granular logic. The core idea is to identify which layers offer the most immediate potential for pilot projects on collaboration.

The mapping exercises and pilot projects proposed in Phase 1 will test the conceptual linkages between drivers and layers, building the evidence base for scaled collaboration in subsequent phases. In this way, the annex table is not merely an analytical exercise but a practical toolkit for prioritizing where and how to begin. The roadmap then provides the temporal structure to move from diagnosis to action, ensuring that the granular, issue-specific approach this paper advocates is translated into concrete institutional practice.

The following two examples illustrate different nodes of EU-GS collaboration. Example 1 examines the EU-Brazil Data Corridor, a currently operational initiative that demonstrates value-based convergence in practice. Example 2 is an illustrative scenario exploring DPIs as a potential avenue for peer learning and future interoperability, reflecting the kind of collaboration this paper argues is both necessary and achievable.

Example 1 | The EU-Brazil Data Corridor: Value-based Convergence in Practice

The EU-Brazil mutual adequacy decision, adopted in January 2026, stands as the most mature and significant example of equitable digital sovereignty collaboration between the EU and a Global South partner. The agreement creates the world's largest trusted data corridor, covering 670 million people, where personal data can flow freely for commercial, administrative, and research purposes without additional legal barriers.

What makes this case instructive is its foundation in mutual recognition, not unilateral certification. Brazil did not adopt its General Data Protection Law (LGPD) to satisfy European demands; the law emerged from a decade of domestic legislative debate, was anchored in constitutional recognition of privacy as a fundamental right, and is enforced by a nationally empowered authority, the ANPD. The EU's adequacy finding recognized that two distinct legal orders, shaped by different historical and political contexts, had arrived at essentially equivalent levels of protection.

The agreement's architecture embeds equity in its design. It is a mutual adequacy decision, where both parties find each other adequate, creating symbolic and legal parity. A four-year review clause and structured regulatory dialogue between the EDPB and ANPD transform data protection into a *living diplomatic commitment*, requiring ongoing negotiation on enforcement practices, surveillance powers, and redress mechanisms. This ensures the partnership evolves with technology and law, rather than becoming a static certification.

Example 2 | Digital Public Infrastructure: Peer Learning & Future Interoperability[3]

One of the most promising frontiers for collaborative efforts based on the sharing best practices (Annexure A) lies in Digital Public Infrastructure (DPI). India and Brazil have emerged as global leaders in building DPI that is state-led, interoperable, and designed as public goods rather than proprietary platforms. India's India Stack, including Aadhaar (digital identity), UPI (real-time payments), and DEPA (consent-based data sharing), has demonstrated how modular infrastructure can achieve massive scale while fostering private innovation. Brazil's parallel achievements, such as Pix (real-time payments), Gov.br (centralised platform for federal services), and the LGPD framework, have transformed service delivery and financial inclusion for over 200 million people.

These systems are not flawless: Aadhaar has faced criticism over exclusion errors and privacy concerns; Pix operates within a digital divide that still excludes millions. Yet their imperfections do not negate their achievements. Both countries have built working infrastructure at scale and with speed, offering valuable lessons in what works, what fails, and what can be improved.

The EU, despite its advanced digital economy, could benefit from DPI solutions for problems such as fragmented digital IDs, cumbersome cross-border data sharing, and uneven public service quality. An *illustrative collaboration* could begin with structured peer learning. EU technical delegations and policymakers can undertake deep-dive studies of India's DPI architecture, governance models, and adoption strategies, alongside parallel engagement with Brazil's experience in designing Pix and integrating digital identity with service delivery. The EU learns from GS's ingenuity, including its mistakes, in building systems that work at scale.

However, this collaboration would not be one-way. EU's GS counterparts can gain from their expertise in rights-based regulation, offering frameworks to address the very critiques their systems face. Access to European markets and alignment with global standards also offer tangible benefits for GS countries. The natural evolution would be interoperability talks: *if the EU builds infrastructure informed by DPI principles, can these systems talk to each other?*

3 Illustrative Example

8 | Three-Year Roadmap for Collaboration

Phase & Timeline	Objectives	Proposed Actions	Expected Outcomes
Phase 1 0–12 months	**Establish dialogue to scope core areas of collaboration, tangible value, and shared thinking on solutions.**	• Launch an EU-GS Digital Dialogue forum co-chaired by the EU and a rotating Global South partner, functioning as a dedicated dialogue space to scope complementary strengths and resilience gaps. • Commission joint sovereignty mapping exercises of existing Global South digital innovations that could inform EU use cases. • Initiate 2 low-risk pilot projects in non-controversial domains with clear peer-learning frameworks. • Embed GS civil society and researchers into existing EU knowledge-exchange communities of practice, strengthening ecosystem diversity. • Map and secure funding pipelines across EU instruments, multilaterals, and development banks — building the co-investment scaffolding needed for Phase 2.	• Formal establishment of the EU-GS Digital Dialogue with agreed terms of reference. • Documentation and publication of joint mapping reports identifying at least 3 concrete GS innovations with transfer potential. • Signed Memoranda of Understanding for 2 pilot projects with defined equity conditions. • Operational knowledge exchange platform with initial communities of practice in identified areas of priority. • Identified funding pipeline with committed resources from both EU and GS instruments for Phase 2 pilots.
Phase 2 12–24 months	**Initiate pilot programs, formalise co-investment tools, and align on standards to build interdependent capacity.**	• Scale successful pilots into broader programs with dedicated funding streams. • Establish a co-funded EU-GS Digital Sovereignty Fund for joint R&D in priority areas (from Phase 1). • Launch a regulator exchange program embedding officials from Global South authorities in European counterparts and vice versa.	• At least 2 pilot programs transitioned to scaled initiatives with multi-year funding. • Operational co-funding mechanism with the first call for proposals launched and projects selected. • The first cohort of 10-15 regulators completes an exchange program with a joint training curriculum.
Phase 3 24+ months	**Embed collaboration into institutional practices, establish permanent joint bodies, and leverage partnerships to influence the global governance landscape.**	• Transition the EU-GS Digital Dialogue into a permanent Digital Council with rotating co-leadership, extending the EU's tech diplomacy architecture to embed Global South partners in values-based standard-setting and digital governance. • Launch a Digital Diaspora Fellowship enabling researchers trained in Europe to return to Global South institutions with matched funding, echoing the Tech Erasmus model within a bilateral frame. • Jointly table a global norms initiative (e.g., Principles for Equitable AI Governance) at the UN or G20, positioning the EU-GS partnership as a values-based barycentre for global digital governance.	• Permanent EU-GS Digital Council established with an agreed work programme. • The first cohort of 10 fellows completes the program, with return placements secured. • Joint diplomatic proposal formally tabled in at least one multilateral arena with visible coalition support.

8.1 | Situating the Roadmap within the ETRS Framework[4]

The roadmap above is designed to complement the European Technological Resilience Strategy's inward-facing agenda. Where the ETRS focuses on building Europe's internal capabilities across knowledge, investment, productivity, and ecosystems, this roadmap proposes an external dimension animated by the same foundational values — technological agency, equitable governance, and sovereignty as a shared good. The phased approach mirrors the ETRS's Now — Tomorrow — Day After logic, and deliberately engages three of its four strategic pillars:

- **Act on Knowledge (Phase 1):** Early actions build trust and institutional scaffolding through joint sovereignty mapping and shared knowledge infrastructure.
- **Act on Investment (Phase 2):** Mid-term initiatives co-invest in shared capabilities through a bilateral Digital Sovereignty Fund and a regulator exchange programme.
- **Act on Ecosystems (Phase 3):** Long-term measures anchor the partnership in permanent tech-diplomacy institutions and multilateral norm-setting, thereby realising ecosystem-building at a global scale.

Critically, this bilateral logic does not ask the EU to look outward at the expense of its internal priorities — it recognises that sustainable European technological sovereignty requires partners who share its commitment to open, values-based digital governance. The Global South is not a recipient of European digital policy; rather, it is a co-architect of the global digital order that the ETRS ultimately seeks to shape.

4 ETRS Policy Brief – From Reactive to Proactive Measures: Proposing a Strategic Playbook for a Phased Approach towards European Technological Agency

Annexure A | Potential Nodes for Collaboration

Driving Factor	Area of Collaboration					
	Data	Model	Compute	Talent	Applications	Governance
Sharing Best Practices						
Bridge-building and Norm-setting						
Value-based Convergence						
Infrastructure Partnerships						
Talent						
Partnerships						

Address | Contact

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Phone +49 5241 81-0
www.bertelsmann-stiftung.de

Murali Nair
Senior Project Manager
Democracy and Social Cohesion
Phone +49 5241 81-81521
murali.nair@bertelsmann-stiftung.de
https://indopazifik.de/