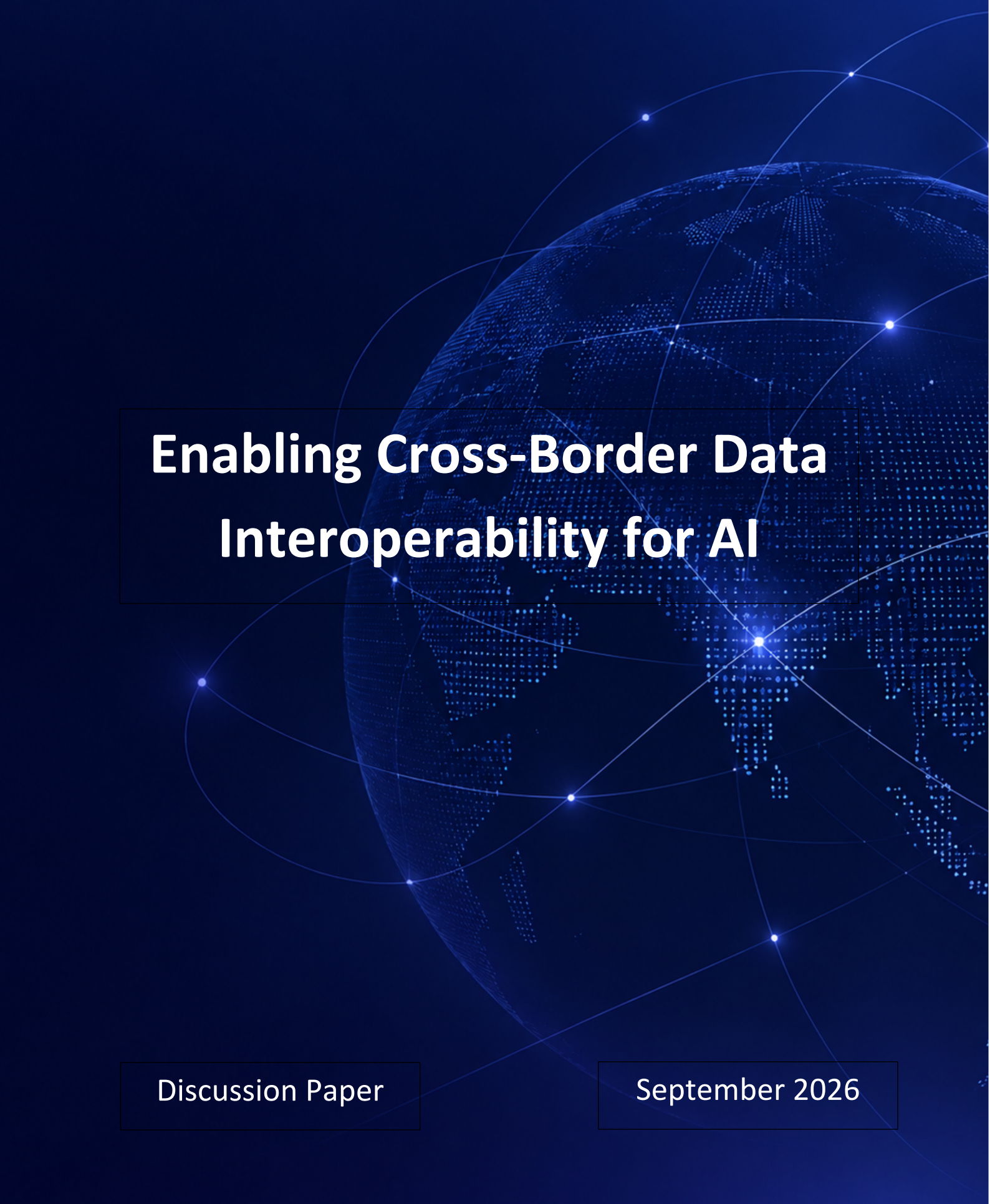
भारत सरकार के प्रधान वैज्ञानिक सलाहकार का कार्यालय
Office of the Principal Scientific Adviser
to the Government of India



# Enabling Cross-Border Data Interoperability for AI

Discussion Paper

September 2026

**Acknowledgement**

This Discussion paper has been prepared with inputs and feedback from domain experts, stakeholders and colleagues during various stages of its development. We are grateful for advice, review and inputs from Dr. Parvinder Maini, Scientific Secretary, Office of Principal Scientific Adviser to the Government of India; Dr. Preeti Banzal, Adviser/Scientist 'G', Office of Principal Scientific Adviser to the Government of India; Mr. Akhil Kumar, CEO, Digital India Corporation, Ministry of Electronics and Information Technology (MeitY), Government of India; Dr. Harpreet Singh, Scientist G and Professor, ICMR-National Institute for Research in Digital Health (NIRDH); Mr. Gaur Sunder, Scientist F & Head, NRCeS, C-DAC, Pune; experts from iSPIRT: Dr. Sunu Engineer; Mr. Harshit Kacholiya and Mr. Vinayak Godse, CEO, Data Security Council of India (DSCI). The views expressed in this paper do not necessarily reflect those of the reviewers, contributors or their respective institutions.

**About: Discussion Paper on Emerging Policy Priorities for India's AI Ecosystem**

To foster informed deliberation and action among stakeholders engaged in shaping India's artificial intelligence (AI) policy and governance landscape, the Office of the Principal Scientific Adviser to the Government of India is producing this Discussion Paper. This paper is conceived as an explanatory brief that examines specific structural gaps in enabling cross-border data interoperability for AI systems and its associated nuances, with the aim of enabling broader understanding and constructive societal engagement. The Discussion Paper is developed by drawing on collective insights from the extended AI ecosystem, including inputs from multi-stakeholder consultations, bilateral and multilateral AI policy engagements and subsequent expert reviews. They are intended solely as explanatory documents that highlight identified policy priority and stimulate further discussion. The views presented in this Paper should not be construed as formal policy positions of the PSA Office.

**Prepared by:**
Mr. Animesh Jain, Senior Policy Fellow
Mr. Kunal Thakur, Policy Analyst
Office of the Principal Scientific Adviser to the Government of India

# Table of Contents


**1. Introduction** ..... **4**

1.1 Why AI Changes Cross-Border Data Governance ..... 4

1.2 Governance Spectrum of International Data Interoperability ..... 5

**2. Why India Needs Risk-Based International Data Interoperability** ..... **7**

**3. Informed & Balanced International Data Interoperability** ..... **10**

3.1 Challenges Raised by Cross-Border Data Transfer for Data Sovereignty ..... 10

**4. Global Approaches to Cross-Border Data Flows** ..... **12**

4.1 National approaches: Principles Governing Cross-Border Data Flow ..... 12

4.1.1 India ..... 12

4.1.2 European Union ..... 13

4.1.3 United States ..... 14

4.1.4 China ..... 16

4.2 Regional Approaches: Framework-Based Coordination for Cross-Border Data Flows ..... 17

4.2.1 Association of Southeast Asian Nations (ASEAN) ..... 17

4.2.2 African Union (AU) ..... 18

4.2.3 Asia-Pacific Economic Cooperation (APEC) ..... 19

4.3 Common Principles for Governing Cross-Border Data Flow ..... 20

**5. AI Specific Framework for Cross-Border Data Interoperability** ..... **21**

5.1 Framework Architecture and Core Building Blocks ..... 22

5.1.1 Risk-Based Classification and Access Pathways: ..... 22

5.1.2 Enablers of Framework ..... 25

5.2 Demonstrating the Framework: Cross-border Health Data ..... 32

5.3 Key Recommendations for Operationalising the Framework in India: ..... 34

**6. Conclusion** ..... **36**

**References** ..... **37**

**Annexure** ..... **44**

**List of Abbreviations:** ..... **45**

# 1. Introduction

In the contemporary global digital economy, data has emerged as a strategic asset that shapes economic competitiveness, technological advancement and geopolitical influence. The rapid expansion of data-driven trade, artificial intelligence (AI) systems and digital public infrastructure has transformed how states approach domestic governance and global economic integration. Globally, the digital economy was estimated to account for 15% of global GDP in 2024, reflecting its growing centrality to economic activity. In India, it accounted for about 11.74% of GDP, equivalent to approximately ₹31.64 lakh crore (over US$400 billion), in 2022-23 and is projected to reach nearly one-fifth of GDP by 2030 [1] [2].

At the heart of this transformation lies a fundamental policy dilemma: how to maintain data sovereignty with the imperatives of openness, innovation and interoperability that underpin global digital ecosystems [3].

Data sovereignty in general refers to a country's efforts to exercise national control over data generated within its territorial boundaries, including its storage, processing, and cross-border transfer. It is closely tied to strategic autonomy in digital infrastructure, the protection of citizens' personal data, the safeguarding of critical information assets and the mitigation of risks from foreign surveillance and external dependence [4]. For countries like India, data sovereignty is an important aspect of digital governance, particularly as data plays a significant role in public administration, national security, technological innovation and socio-economic growth.

International data interoperability refers to the ability of data systems, regulatory frameworks and digital infrastructure across countries to exchange, access and use data in a secure and meaningful manner. It can be operationalised through four main components: technical interoperability (including common standards, APIs and protocols), legal interoperability (including lawful transfer mechanisms, safeguards and enforceable obligations), semantic interoperability (including data definitions, taxonomies, classifications and metadata) and institutional interoperability (coordination among regulators, governments and other relevant institutions). These components can support trusted cross-border data flows without requiring participating countries to adopt identical legal or technical systems [5].

## 1.1 Why AI Changes Cross-Border Data Governance

In the case of AI, data interoperability also goes beyond the transfer and exchange of datasets. In AI systems, the object crossing the border may be raw data, model parameters, analytical outputs or a trained model. A model trained on sensitive or restricted data may retain, reproduce or enable inferences about information contained in its training records, even where the underlying data remain within the country [75]. AI systems may also combine

apparently non-sensitive information to infer sensitive attributes. The data governance therefore needs to include both datasets and the models derived from them.

Cross-border data governance in the context of AI can therefore be understood as an access layer, through which individuals or institutions obtain authorised access. Depending on the nature of the data, purpose of use and level of risk, such access may be enabled through different mechanisms, including controlled access and other safeguards. It provides a recognisable basis for partner countries to assess and coordinate with domestic mechanisms. This distinction is important because data transfer, data access, data processing and transfer of AI-derived outputs are not necessarily the same activity. A governance framework should therefore consider the form of access and processing alongside the location of the underlying data.

## 1.2 Governance Spectrum of International Data Interoperability

Cross-border data-governance approaches can be understood as a spectrum ranging from strict data localisation to fully open data flows, with intermediate mechanisms such as conditional transfers, adequacy-based arrangements, controlled access, trusted data corridors and distributed processing. Each approach reflects different trade-offs between sovereignty and openness. The appropriate pathway may vary depending on the sensitivity and criticality of the data, the sector involved, the purpose of processing, the capabilities of the AI system and the safeguards available.

This discussion paper explores the importance of balancing data sovereignty with international data interoperability for India's AI systems. India's emerging data-governance architecture, including the National Data Governance Committee (NDGC), already recognises the importance of coordinated data sharing, standardised metadata, APIs, auditability and legal compliance [6]. For AI, in addition to these functions, contextual risk, classifications, controlled access, model-to-data processing, downstream use and other nuances also need to be addressed.

The paper first reviews national and regional approaches to cross-border data flows and then proposes a framework based on the principles of coordination, compatibility and accountability. As an example, the framework is further demonstrated through the health-data ecosystem, which has relatively well-developed semantic, syntactic and institutional arrangements. The understanding of Indian initiatives such as Medical Imaging and Information Datasets for India (MIDAS) and Metric-based Integrity and Data Assessment System (MIDAS 2.0) by ICMR has also been utilised to demonstrate the framework for the assessments of quality, interoperability, AI readiness and residual privacy risk. These health-sector examples are used to assess how the broader principles proposed in this paper may be translated into approaches for cross-border AI-data interoperability in other sectors.

While several such initiatives are still emerging, bilateral cooperation is beginning to demonstrate how these principles can be operationalised. At the AI Impact Summit 2026 in New Delhi, the French Health Data Hub and ICMR announced a collaboration to test the Data Empowerment and Protection Architecture (DEPA) for secure and traceable access to Indian and French health data for public-interest research [76]. This emerging collaboration illustrates how an interoperability layer may be operationalised through Digital Public Infrastructure (DPI) and techno-legal mechanisms. In particular, the India-France health-data collaboration demonstrates how DEPA can enable secure, purpose-specific and traceable access to health data for research and healthcare purposes. As a techno-legal approach, DEPA illustrates how technical architecture can work alongside consent, access conditions, purpose limitation and accountability requirements to support trusted data use across institutions and jurisdictions [77].

## 2. Why India Needs Risk-Based International Data Interoperability

The governance of cross-border data flows is often framed as a binary choice between strict data localisation and unrestricted openness. However, both extremes carry significant economic, technological and strategic risks. Evidence shows that balanced approaches, where data flows are enabled with appropriate safeguards, can increase global GDP by around 1.77% and global exports by about 3.6%. Conversely, highly restrictive or fragmented data regimes may reduce global GDP by nearly 4.5% and exports by around 8.5%. This highlights the economic costs of limiting data flows [7][1]. For India, the policy challenge is therefore to move beyond this binary and adopt an evidence-driven, context-specific approach to international data interoperability, one that balances sovereign control with the benefits of global digital integration.

Excessive data localisation regulations, while often justified on grounds of national security and regulatory oversight, can impose substantial costs on the domestic ecosystem. Mandating local storage and processing infrastructure raises compliance burdens, particularly for startups and MSMEs [8]. It can also fragment global AI research ecosystems by limiting access to diverse datasets and constraining collaborative innovation. Additionally, stringent localisation measures may trigger retaliatory trade actions, affecting digital trade and services exports [9]. Over time, these factors risk weakening both domestic innovation capacity and international competitiveness.

At the other end of the spectrum, unrestricted cross-border data flows raise different concerns. These include exposure to foreign surveillance, reduced regulatory oversight when data is processed in jurisdictions with weaker safeguards, and the risk of data concentration in the hands of a few global technology firms [10]. Such asymmetries can undermine fair competition and limit the growth of domestic digital economy ecosystems. Together, these risks highlight that openness without adequate safeguards can be as detrimental as over-restriction.

Despite these challenges, cross-border data flows remain critical to the development of AI and the broader digital economy. Advanced AI systems depend on access to large, diverse and high-quality datasets, which are often distributed across geographies. International data flows improve model performance, enable linguistic and contextual diversity and support innovation across sectors such as healthcare, agriculture and logistics.

---

[1] The figures are computable general-equilibrium simulations based on hypothetical global scenarios, rather than observed economic outcomes, and their effects may vary across countries. Earlier ECIPE (European Centre for International Political Economy,) modelling, also discussed by ITIF (Information Technology and Innovation Foundation.), estimated a GDP impact of around 0.1% for selected localisation measures in India and approximately 0.8% under an economy-wide localisation [73] [74].

They also underpin global research collaboration, shared infrastructure, and the development of foundation models; therefore, restrictive regimes risk isolating domestic ecosystems from these global networks.

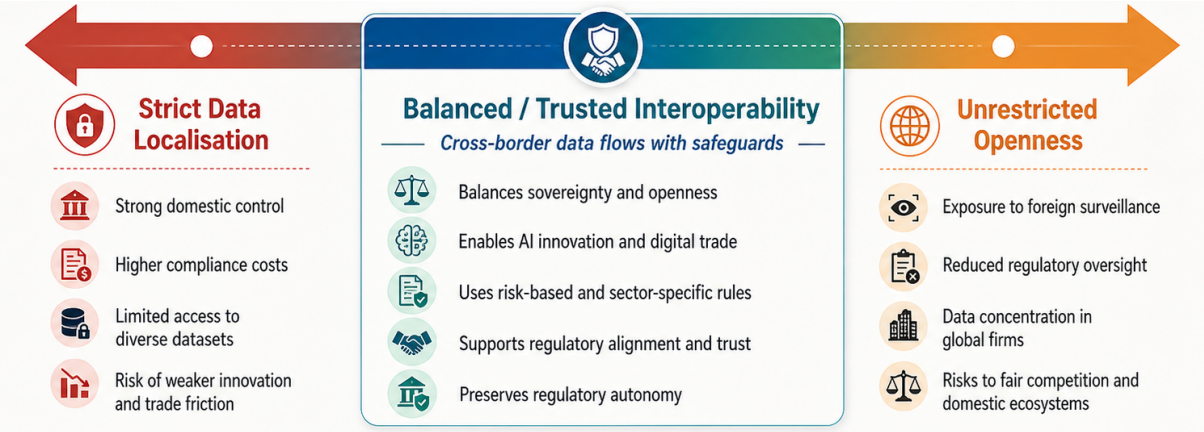



***Fig. 1:*** *Governance spectrum of data interoperability*

Uncoordinated national approaches to data governance further risk fragmenting the global digital landscape, often described as the "splinternet" [11]. Such fragmentation can increase compliance costs, disrupt digital trade, and limit cross-border innovation. Avoiding this outcome requires greater alignment through interoperable regulatory frameworks, baseline data protection standards and institutionalised mechanisms for international cooperation. A coherent middle path lies in developing international data interoperability frameworks that enable trusted data flows while preserving regulatory autonomy [12]. These can take multiple forms; some of the examples are

- Trusted Data Corridors: Bilateral or plurilateral arrangements that enable data sharing under common safeguards, standards, and enforcement mechanisms, tailored to sectoral needs [13].
- Mutual Recognition Frameworks: Agreements that recognise equivalence between data protection regimes, allowing cross-border transfers based on shared privacy principles. (Example – Adequacy decisions [14])
- Standards-Based Interoperability: Use of open technical standards, privacy-enhancing technologies (PETs), secure multiparty computation, and federated architectures to facilitate data exchange without exposing raw data [15]. (Example – NIST – Infrastructure for Secure Data Sharing)
- Data Embassies and Sovereign Clouds: Hybrid models that ensure sovereign control while allowing secure cross-border data management and operational continuity [16].

Central to these approaches is a risk-based and sector-specific governance model. Sensitive domains such as defence, critical infrastructure, financial systems and health may require stricter controls or conditional transfers, while less sensitive data can be governed through

more open regimes. To operationalise this effectively, reducing regulatory ambiguity by establishing clear, tiered and predictable rules for cross-border data flows is essential. This will be particularly important for startups and emerging firms, for whom uncertainty remains a significant barrier.

# 3. Informed & Balanced International Data Interoperability

As discussed in earlier sections, to maintain effective cross-border data flows, we need robust mechanisms for data interoperability. It is a technical prerequisite for the smooth flow of data across borders [17]. Further, a combined technical, legal, semantic and institutional framework will enable data to be exchanged, understood and used in a reliable and trusted manner.

At a minimum, cross-border data flow requires common technical conditions for exchange [18]. Data should move through structured and machine-readable formats, common protocols, secure interfaces, and reliable authentication and security systems. In their absence, data exchange may be technically or operationally limited, even if it is legally permitted [19]. The different types of interoperability can be understood as follows:

Technical interoperability requires that different digital systems can connect, exchange, and process data securely through common protocols, APIs, data formats, authentication systems, encryption standards, and secure digital infrastructure. Legal interoperability requires a lawful basis for transfer, clearly defined transfer conditions, safeguards, rights and obligations, and an enforceable mechanism for compliance and redress. Semantic interoperability requires definitions, taxonomies, metadata standards, classifications, and a shared understanding of data fields and categories so that data retains the same meaning across systems and jurisdictions. Organisational or institutional interoperability requires effective coordination among institutions, regulators, and organisations involved in data governance and exchange [20].

These are the necessary interoperability requirements for effective cross-border data flow. Still, data sovereignty is a critical component as countries continue to seek control over data classification, protection, and accessibility. It is especially important for countries such as India, as the country's digital economy is expanding rapidly, its digital public infrastructure operates at a population scale, and data governance is closely linked to strategic autonomy [21] [22]. Therefore, enabling international data interoperability, standard-setting, and a degree of regulatory alignment are required. However, such alignment also needs to be approached carefully so that data remains uniform and trustworthy across jurisdictions without weakening sovereign control over sensitive data, critical systems, and public-interest safeguards, as discussed in the following section [23].

## 3.1 Challenges Raised by Cross-Border Data Transfer for Data Sovereignty

While data interoperability enables cross-border data flows, it also raises sovereignty concerns for countries. Approaches to governing data flows vary considerably across countries, and they regulate cross-border data flows for legitimate public policy reasons, including privacy, national security, and economic development objectives [24]. Some key effects of cross-border data transfer on data sovereignty are:

a. **Loss of domestic control over data governance –** The first challenge is that interoperability may reduce domestic control over data classification, transfer, and use after it leaves the jurisdiction. If external standards, foreign legal protocols or private contractual arrangements effectively determine how data is treated, domestic regulatory space may narrow. Therefore, any global approach needs to allow sufficient policy space for countries at varying levels of digital capability to pursue national priorities and development objectives [25].

b. **Sovereignty risks in strategic sectors –** The second challenge concerns strategic and high-risk sectors. Interoperability may be easier to justify for lower-risk data (product and pricing data, anonymised data/statistics or any non-sensitive commercial datasets). Still, it raises more difficult questions when the data relate to strategic sectors, such as finance, health, telecommunications or other strategic functions.

c. **Asymmetry in digital dependence –** The third challenge concerns asymmetries in digital economic capacity and value capture across countries. The UNCTAD report notes that the data-driven digital economy is marked by large imbalances and concentration in value creation and capture, with major power concentrated in a few countries and firms (e.g., the US and China) [26]. In this case, interoperability may benefit some actors more than others, raising concerns about dependency.

d. **Foreign access and downstream transfer risk –** The fourth challenge involves forward transfers and foreign access. Once data becomes interoperable across borders, the country of origin may find it more difficult to retain visibility and control over subsequent transfers, downstream processing, or access by foreign public authorities.

These are some of the principal concerns; additional concerns may arise on a case-by-case, sector-by-sector or country-by-country basis, depending on the type of data and the strategic importance attached to it by the concerned state. For example, in India, semantic interoperability may require standardised definitions, taxonomies, and metadata that do not fully reflect the country's linguistic diversity, administrative structure and socio-cultural context. In such cases, interoperability may improve cross-border comparability, but it may also reduce the accuracy and contextual integrity of Indian data.

# 4. Global Approaches to Cross-Border Data Flows

This section reviews selected countries and regional approaches that have mentioned cross-border data flows and data interoperability in their laws and legal documents. The purpose is to identify the principal legal and policy models through which different countries enable data exchange while preserving privacy, security, and regulatory control. This section outlines the primary approaches identified in practice and clarifies their operational implications.

## 4.1 National approaches: Principles Governing Cross-Border Data Flow

This section reviews the approaches adopted by different countries, such as India, the EU, the United States and China. It identifies the various principles in the operational laws that enable CBDF in these countries.

### 4.1.1 India

#### 4.1.1.1 Controlled and Selective Interoperability

Personal data transfers in India are permitted under the Digital Personal Data Protection Act, 2023, but remain subject to sovereign restrictions. Sectoral rules apply stricter controls where systemic risk or public security is involved [27]. At the same time, India has built major digital public infrastructure systems on an interoperable, API-based architecture, and its policy on non-sensitive government data encourages access to and sharing of machine-readable, interoperable data [28]. These features demonstrate that India enables interoperability for supporting service delivery, innovation, and digital participation, while preserving stronger control when privacy, security, or strategic interests are involved.

#### 4.1.1.2 Negative-List Approach to Personal Data Transfers

Section 16 of the Digital Personal Data Protection Act, 2023, allows the central government to restrict transfers of personal data to notified countries or territories while also preserving stricter sectoral rules where they apply. It gives India a negative-list model under which cross-border transfers are generally permitted but remain subject to sovereign control through notification and sector-specific regulation. Under the notified phased commencement of the Act, the substantive cross-border transfer provisions are scheduled to become operational in May 2027.

#### 4.1.1.3 Localisation-First Approach to Sectoral (Payment) Data

India adopts a localisation approach to payment system data under the RBI's Storage of Payment System Data direction dated 6 April 2018. Under this direction, payment system providers are required to ensure that all data relating to payment systems they

operate is stored only in India. Although processing may take place abroad in limited cases, the data must be brought back to India and deleted abroad within the prescribed time. This may be described as localisation-first, with domestic storage remaining the default and only narrow operational exceptions permitted [29].

#### 4.1.1.4 Co-ordinated Data Governance Mechanism

India also has an institutional mechanism, the national data governance committee, to support coordinated data sharing across government institutions. The committee will guide and oversee the adoption of data exchange platforms and support the implementation of purpose limitation, auditability, anonymisation and other compliance-related measures within government and with private entities. However, AI-related cross-border data flows will still require more specific operational protocols for classification, downstream use, re-identification risk and metadata quality to support interoperability.

#### 4.1.1.5 Emerging Bilateral Model for Controlled Health-Data Access

India is also beginning to explore bilateral arrangements for controlled and purpose-specific access to health data. As mentioned above, the ICMR and the French Health Data Hub announced a collaboration to test the DEPA to enable secure, traceable access to Indian and French health data for public-interest research. The proposed arrangement uses regulated access and defined purposes rather than unrestricted data sharing. A Letter of Intent between ICMR, the Department of Health Research (DHR) and the French Health Data Hub was subsequently signed to support the governance and management of secondary use of health data [78].

### 4.1.2 European Union

#### 4.1.2.1 Principle of Continuity of Protection

Chapter V of the GDPR establishes a principle of continuity of protection for cross-border transfers. Article 44 requires that the safeguards applicable to personal data are not undermined after transfer, including through onward transfers [79].

#### 4.1.2.2 Adequacy-Based Transfers

As per Article 45 of the GDPR, a transfer may take place where the European Commission has decided that a third country, a territory or one or more specified sectors within that third country, or an international organisation ensures an “adequate level of protection" [30]. Where such a decision exists, the transfer “shall not require any specific authorisation.” In this way, the EU allows cross-border transfers through an adequacy-based model, but only where the continuity of

protection is recognised in advance. The EU–U.S. Data Privacy Framework operates through this same adequacy mechanism [31].

#### 4.1.2.3 Appropriate Safeguards for Conditional Transfers

Where no adequacy decision exists, Article 46 of the GDPR permits a transfer only if the controller or processor has provided “appropriate safeguards” and on condition that “enforceable data subject rights and effective legal remedies for data subjects are available" [32]. The GDPR identifies mechanisms such as standard data protection clauses, binding corporate rules, and other approved safeguards. The EU allows conditional transfers, but only through structured legal routes that preserve continuity of protection.

#### 4.1.2.4 International Agreement for Foreign Disclosure

The GDPR also places limits on foreign disclosure demands. Article 48 states that a judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may be recognised or enforced “only if based on an international agreement", such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State [33].

#### 4.1.2.5 Controlled-Access Model for Sensitive Health and Genomic Data

The European Genome-phenome Archive (EGA) provides a controlled-access model for sharing sensitive human genomic, and clinical data. Data access is governed by a Data Access Committee (DAC), which reviews requests and determines whether access should be granted in accordance with the dataset's conditions and GDPR [80].

Each dataset is linked to a Data Access Agreement (DAA), which specifies the terms and conditions for its use, including permitted purposes, storage requirements and other restrictions. This model enables research access to sensitive data without making the datasets publicly available and provides a useful example of purpose-specific, institutionally governed data access.

### 4.1.3 United States

#### 4.1.3.1 Restricted and Prohibited Transactions Model

The United States does not regulate cross-border data transfers through a single federal framework comparable to GDPR. It addresses specific risks related to data access, especially when such access may affect national security or law enforcement. On February 28, 2024, the President issued Executive Order (E.O.) 14117 (Preventing

Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern) [34]. The E.O. directed the Department of Justice to develop and implement the Data Security Program (DSP) [35]. The Department's final rule, codified in 28 CFR Part 202, prohibits and restricts certain data transactions with certain countries or persons. The rule became effective on 8 April 2025 [36]. It applies where such transactions could provide access to “bulk U.S. sensitive personal data” or “government-related data".

#### 4.1.3.2 Access-Based Security Framework

The U.S. approach also relies on an access-based security framework. The Department of Justice mentioned that the Data Security Program is designed to “prevent access to Americans’ bulk sensitive personal data and U.S. government-related data by countries of concern or covered persons." [37] Its emphasis is on who can access the data and under what conditions. This model supports cross-border data movement in general while using national security tools to restrict access when security risks arise.

#### 4.1.3.3 Executive Agreement Framework for Lawful Data Access

The Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018, creates an executive agreement framework for cross-border access to electronic evidence in serious criminal investigations [38]. First, it makes clear that a provider subject to U.S. jurisdiction may be required to produce data within its “possession, custody, or control, regardless of where the data is stored". Second, it authorises the United States to enter into “executive agreements” with foreign governments that satisfy the statutory requirements. This is a selective model for lawful cross-border access to data in criminal matters.

#### 4.1.3.4 Controlled-Access Model for Genomic and Health Data

The Genotypes and Phenotypes database (dbGaP) provides a controlled-access model for sharing sensitive genomic research data in the United States [81]. Access to controlled datasets is reviewed by the relevant National Institutes of Health (NIH) Data Access Committee (DAC). Researchers are required to submit a Data Use Certification (DUC) that describes the proposed research use and agrees to the applicable data-use and security conditions. Access is granted only where the proposed use is consistent with the consent conditions and restrictions attached to the dataset.

### 4.1.4 China

#### 4.1.4.1 Data Localisation for Critical and Important Data

China applies localisation and outbound-security requirements to personal information and important data collected or generated by critical information infrastructure operators in their domestic operations. This provision is Article 39 of the Cybersecurity Law as amended in 2025 and effective from 1 January 2026; it was Article 37 in the original 2016 law [39]. Article 31 of the Data Security Law connects important-data exports by these operators to the Cybersecurity Law and provides for rules governing exports by other processors [40].

#### 4.1.4.2 Security Assessment Framework

For higher-risk transfers, China relies on a security assessment framework. Article 38 of the Personal Information Protection Law provides that where a personal information processor “truly needs" to provide personal information to a party outside the territory of the PRC, it shall meet one of the recognised requirements, including “passing the security assessment organised by the national cyberspace department.” [41] Security assessment is therefore one of the principal legal routes for cross-border transfers of personal information.

#### 4.1.4.3 Standard Contract and Certification Routes

Alongside security assessments, China recognises standard contracts and certification routes. Article 38 of the Personal Information Protection Law also permits cross-border transfers through “obtaining personal information protection certification” and through “concluding a contract” in accordance with the standard contract formulated by the national cyberspace department. These are recognised legal routes within China’s cross-border transfer framework [82].

#### 4.1.4.4 Consent for Cross-Border Transfers

Article 39 of the Personal Information Protection Law (PIPL) provides that where personal information is provided outside China, the processor shall notify the individual of the overseas recipient and related matters, and that separate consent. Separate consent is therefore a distinct compliance requirement in the broader transfer regime inside the PRC [83].

#### 4.1.4.5 Relaxed Compliance for Lower-Risk Transfers

The Provisions on Promoting and Regulating Cross-Border Data Flow of 22 March 2024 introduced a more differentiated approach. Article 1 states that the purpose of the

provisions is to “protect data security, protect personal information rights and interests, and promote the orderly and free flow of data in accordance with law" [42]. The provisions narrow the scope of cases requiring full compliance procedures and ease requirements for routine business scenarios and lower-risk transfers. China’s current model is therefore not one of unrestricted openness. It is a more targeted system in which high-risk transfers remain subject to strict control, while lower-risk and ordinary commercial transfers face lighter compliance requirements.

## 4.2 Regional Approaches: Framework-Based Coordination for Cross-Border Data Flows

This section reviews the approaches followed by regional groups, such as ASEAN, the African Union, and APEC. These groupings generally do not operate through a single binding regional law. Instead, they rely on shared principles, voluntary tools, model clauses, certification systems, and coordination frameworks.

### 4.2.1 Association of Southeast Asian Nations (ASEAN)

#### 4.2.1.1 Regional Frameworks and Voluntary Tools

ASEAN’s cross-border data-flow model is built through regional frameworks and voluntary tools. The ASEAN Framework on Personal Data Protection strengthens the protection of personal data in ASEAN and facilitates cooperation among the Participants, and it does not constitute or create obligations under domestic or international law [43]. The ASEAN Framework on Digital Data Governance likewise sets out strategic priorities, principles, and initiatives to guide Member States in their policy and regulatory approaches toward digital data governance [44]. This gives ASEAN a regional, soft-law model rather than a binding, adequacy-based regime.

#### 4.2.1.2 Trust-Based and Gradual Regulatory Convergence

The Framework on Digital Data Governance states that cross-border data flows should be accompanied by assurances that safeguards are in place to protect and secure the information, regardless of where the data goes [84]. It further mentions that such safeguards should be “harmonised to prevent the development of fragmented regulatory regimes” and that requirements on cross-border data flows should be “proportionate to the risks associated with transferring the data". This approach seeks to maximise the free flow of data while ensuring the necessary protection, but it does so through baseline principles and gradual coordination rather than strict uniformity.

#### 4.2.1.3 Readiness-Based Participation Model

The principles outlined in the Framework on Digital Data Governance aim to provide ASEAN Member States with guidance tailored to each Member State's readiness and development. This allows participation without requiring immediate full alignment across the region. The same framework also preserves exemptions for matters relating to “national sovereignty, national security, public safety” and other areas that Member States deem suitable for exemption.

#### 4.2.1.4 Model Contractual Clauses

ASEAN uses Model Contractual Clauses (MCC) as a transfer tool. The ASEAN Model Contractual Clauses for Cross Border Data Flows state that the MCCs are “primarily designed for intra-ASEAN flow of personal data” and that they are “a voluntary standard designed to provide guidance on baseline considerations for transferring personal data". [45] They may also be adapted for transfers to non-ASEAN jurisdictions, and parties remain free to use other valid transfer mechanisms recognised within ASEAN. It reflects ASEAN’s preference for flexible and practical transfer tools rather than a single compulsory mechanism.

### 4.2.2 African Union (AU)

#### 4.2.2.1 Shared African Data Space

The AU Data Policy Framework mentions strengthening and harmonising governance frameworks across Africa and creating shared data spaces and standards for the continent [46]. It shows a continent-wide approach to data governance rather than isolated national systems.

#### 4.2.2.2 Harmonised Data Governance Framework

The AU model is also based on harmonised data governance. The Malabo Convention provides a “legal framework for cybersecurity and personal data protection” in Africa [47]. The AU Data Policy Framework and the AfCFTA Protocol on Digital Trade support harmonised rules, common principles, and standards for digital trade and data governance [48]. Article 2 of the Digital Trade Protocol calls for the establishment of “harmonised rules and common principles and standards” to support trusted digital trade and cross-border data flows.

#### 4.2.2.3 Reciprocity-Based Transfer Principle

The AU Data Policy Framework also recommends providing “minimum standards for cross-border data flows and ensuring reciprocity as a central principle for permitting

cross-border data flows". This indicates that the AU does not support completely open transfers. It supports trusted circulation based on balanced obligations and mutual recognition.

#### 4.2.2.4 Supporting Interoperability Through Common and Open Standards

The AfCFTA Protocol on Digital Trade promotes “common and open standards” to enable interoperability of frameworks and systems for digital trade. The AU Interoperability Framework for Digital ID adds a practical layer to this approach. It states that interoperable digital IDs can facilitate access to online services in other countries and enhance the integrity and accessibility of cross-border payments and financial services in Africa [49]. It indicates that the AU is moving from broad principles toward operational interoperability for digital trade and trusted digital transactions.

### 4.2.3 Asia-Pacific Economic Cooperation (APEC)

#### 4.2.3.1 Compatible and Flexible Privacy Framework

The APEC Privacy Framework (2015) promotes “a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows." [50] It does not create a single binding regional law. Instead, it sets out common privacy principles and encourages economies to develop compatible domestic frameworks. This gives APEC a flexible and principles-based privacy model for cross-border data flows.

#### 4.2.3.2 Certification-Based Privacy Rules

The APEC Cross-Border Privacy Rules (CBPR) System mentions that members should implement privacy policies and practices consistent with the CBPR program requirements and that these policies and practices should be evaluated by an APEC-recognised accountability agent for compliance with those requirements [51]. CBPR functions as a certification-based model for trusted cross-border transfers of personal information.

#### 4.2.3.3 Cross-Border Privacy Enforcement Cooperation

APEC also supports enforcement cooperation through the Cross-border Privacy Enforcement Arrangement (CPEA) [52]. The arrangement states that it creates a “practical multilateral mechanism” for privacy enforcement authorities to cooperate in cross-border privacy enforcement by establishing a framework under which they

may, on a voluntary basis, share information and request and render assistance in certain ways.

## 4.3 Common Principles for Governing Cross-Border Data Flow

- Cross-border data governance is increasingly risk-differentiated rather than uniform.
- Countries seek to preserve domestic regulatory authority.
- Interoperability does not necessarily require identical domestic laws or digital systems.
- Controlled access can provide an alternative to unrestricted data transfer for sensitive data.
- Certification and contractual mechanisms can support trust, but require mutual recognition.
- Institutional coordination is essential where multiple regulators and standards bodies are involved.
- Lower-risk data may support more open pathways, while sensitive or strategic data may require stronger controls.

These common principles will further provide the basis for the proposed framework for India in the next section.

## 5. AI Specific Framework for Cross-Border Data Interoperability

This section builds on the analysis of national and regional approaches discussed in section 4 of this paper. Its purpose is to identify a potential framework that may enable lawful, trusted cross-border data interoperability for AI development. Such a framework could be anchored in three broad pillars:

- Compatibility, through which domestic systems and regulations, while not identical, remain capable of working together.
- Accountability, through which cross-border data flows remain trusted and reviewable.
- Coordination, through which countries work within structured bilateral, plurilateral, or multilateral arrangements.

These three pillars are supported by a cross-cutting risk-based access and processing layer that determines the appropriate pathway for accessing, transferring, or processing data based on the nature of data, intended use, sensitivity, and associated risk, and available safeguards.

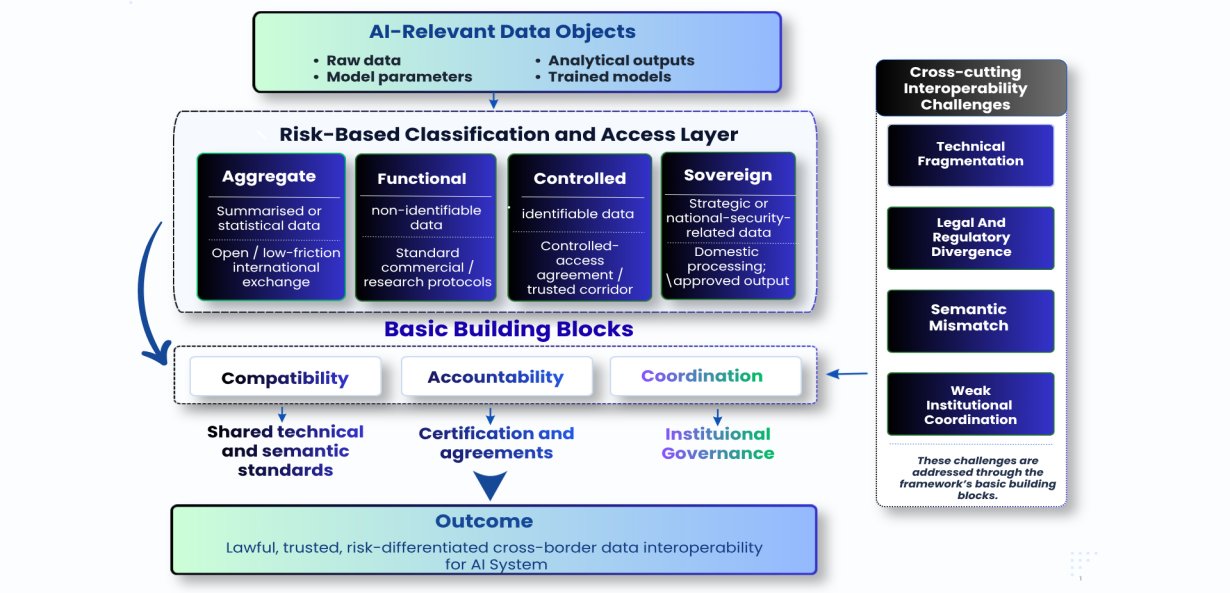



***Fig. 2:*** *Framework for data interoperability through basic building blocks*

Accordingly, the framework may be understood as operating through the following sequence. The AI Data objects are first classified and assessed for risk, after which the appropriate access or processing pathway is identified. After that, the relevant interoperability requirements applied before access or transfer is authorised. Once in use, the arrangement could be monitored and periodically reviewed to account for changes in data use, model capabilities or risk.

The framework is not intended to replace existing data governance instruments and mechanisms or bilateral and multilateral practices. It proposes an AI-specific cross-border interoperability layer that can be built on top of the existing mechanisms for data sharing, safeguards, compliance and institutional coordination while addressing additional AI-related concerns. ***The framework should therefore be understood as an overlaid interoperability layer on extant governance mechanisms, rather than considering as a new AI data-governance regime***. This distinction is important because data transfer, data access, data processing and transfer of AI-derived outputs are not necessarily the same activity. In AI systems, the object crossing the border may be raw data, model parameters, analytical outputs or a trained model. The governance framework should therefore consider the form of access and processing alongside the location of the underlying data.

The access and consent layer utilised in emerging techno-legal approaches, such as DEPA, may be understood along two dimensions: whose access is being governed, whether an individual or an institution, and the stage at which safeguards apply, either when data is made available or during computation, where the underlying data remains in place. For the framework defined in this paper, such a mechanism could provide pathways for matching the form of access with the nature of data, its intended use and the associated level of risk. A table in ***annexure*** provides a way of understanding how different forms of data access may operate within the proposed framework mentioned in this paper.

This framework is intended to provide a standardised and coherent basis for negotiating and operationalising such arrangements. This is increasingly important for the emerging Indian AI ecosystem, which depends on access to diverse, interoperable data across borders, as well as for fruitful partnerships for AI innovation and development with partner countries. While also having appropriate safeguards for privacy, security, accountability and regulatory oversight. The framework is not intended to be final or exhaustive. Rather, it provides entry points through which the Indian AI ecosystem may begin discussion, identify areas of convergence and explore practical pathways for cooperation. It represents the minimum approaches that can be used to support cross-border data flows while preserving the country's sovereignty, security and regulatory control.

This section also applies the proposed building blocks to India’s existing health-data governance and interoperability arrangements to assess their practical applicability. It examines the current regulatory and policy instruments governing health data transfer for AI and identifies opportunities to strengthen interoperability.

## 5.1 Framework Architecture and Core Building Blocks

### 5.1.1 Risk-Based Classification and Access Pathways:

A cross-cutting component of the framework is a risk-based classification and access layer that determines how different categories of data should be treated in cross-border transfers

and what forms of access or processing should be permitted. Rather than applying a single rule to all data flows, the framework follows a differentiated approach in which the applicable pathway depends on factors such as the sensitivity of the data, purpose of use, potential risks and available safeguards. Countries are already adopting category-based and risk-based treatment of data; a few of the examples are mentioned below:

- India allows personal data transfers subject to government-notified restrictions and stricter sectoral rules.
- The EU distinguishes between general personal data, special categories of personal data, and transfer routes such as adequacy and appropriate safeguards.
- The United States has adopted an access-based model for "bulk sensitive personal data" and "government-related data" under Executive Order 14117.
- China also takes a differentiated approach, applying stricter controls to sensitive data and critical information infrastructure. While it's 2024, cross-border data rules relax requirements for certain lower-risk and routine transfers.

However, there are also a few challenges that may affect interoperability for CBDF:

- **Divergent classification criteria:** Countries classify data differently. The EU defines "special categories" by data type; China uses a risk-and-impact test tied to national security; and India relies on sectoral notification. The same data may be "low-risk" in one jurisdiction and "restricted" in another. It creates legal uncertainty for AI developers operating across borders and increases compliance costs and delays.
- **Semantic misalignment:** Terms such as 'anonymised' and 'public interest' lack harmonised technical or legal definitions. Data exchanged across borders may be misinterpreted, misused, or fail regulatory tests despite technical compliance [61].
- **Data reclassification and contextual inference risk:** AI systems can infer sensitive attributes from non-sensitive data, creating downstream risks of re-identification when data is reused, combined, or applied in new contexts. (e.g., deriving health status from behavioral data) [62]. Existing anonymisation guidance recognises that these risks depend on context and on evolving techniques. Category-based rules may become obsolete post-transfer, undermining intended safeguards [63]. This framework can be considered a flexible and tiered approach to category-based compliance.
- **Downstream and onward-use risk:** Once data is used in a different jurisdiction, its subsequent use, combination with other datasets, or incorporation into AI systems may create new risks that were not present at the point of initial transfer.

Under this framework, the following points can be considered a flexible, tiered approach to category-based compliance.

- **Alignment and Mapping Model:** Countries may retain the authority to define sub-categories or apply stricter controls for national security, critical infrastructure and other public-interest concerns. The common interface should not require participating countries to replace their domestic taxonomies. Where exact equivalence is not possible, the mapping should document contextual differences to ensure that data transfer does not result in the loss or misinterpretation of nationally relevant meaning.
- **Risk-Aligned Data Transfer Matrix:** The framework may use an illustrative risk-aligned matrix that links different levels of data sensitivity to proportionate safeguards and regulatory pathways. This may enable lower-risk data flows while applying stronger controls to sensitive, strategic or national-security-related data. The matrix is intended to provide differentiated pathways rather than a single model for all data. The appropriate pathway may vary depending on the sensitivity of the data, the purpose of processing, the capabilities of the AI system, and the safeguards available.

| Mode | Data Granularity | Primary Security/ Privacy Mechanism | Recommended Regulatory Pathway |
|---|---|---|---|
| Mode I: Aggregate | Summarised or Statistical | De-identification & Aggregation | Open/ Low-friction international exchange |
| Mode II: Functional | Fine-grained (non-identifiable) | Differential Privacy & Perturbation | Standard commercial/ research protocols |
| Mode III: Controlled | Fine-grained (Identifiable) | Strict Legal Contracts & Audit Trails | Controlled-access agreement / trusted corridor |
| Mode IV: Sovereign | Strategic or National Security | Raw data remains domestic; secure model-to-data/federated processing; strict scrutiny before permitting cross-border transfer of outputs. | Sovereign processing; only approved outputs leave where permitted |

***Table 1:*** *Risk-aligned Matrix* [2]

- **Controlled Access and Model-to-Data Processing:** For sensitive and high-risk data, interoperability should minimize unnecessary movement of raw data. Controlled-access arrangements may restrict who can access data and under what conditions, while model-to-data or federated approaches may enable analysis while keeping the underlying data within a controlled or local environment. Attribute-Based Access Control (ABAC) may further enforce access based on attributes such as the requesting entity, data sensitivity, authorized purpose, and processing environment. This distinction is important for AI, as the object crossing the border may not be the raw data itself but an analytical output, a model parameter, a trained model, or another derived output. The governance framework should therefore consider both the underlying data and the form of access, processing, and outputs involved.

- **Review and Reclassification:** The framework may include mechanisms to reassess data categories and safeguards when risks change due to new model capabilities, data combinations, processing purposes, inference, re-identification or downstream reuse. Such a review may result in additional safeguards, revised access conditions, or reclassification of the data.

This would allow countries to enable lawful data access for AI development while preserving protection, accountability, and sovereign flexibility.

### 5.1.2 Enablers of Framework

#### 5.1.2.1 Compatibility: Shared Technical and Semantic Standards

The first pillar of the framework is compatibility. Cross-border interoperability requires domestic systems, standards and regulatory arrangements to remain capable of working together even where they are not identical.

##### 5.1.2.1.1 Shared Technical Standards

The framework would require technical standards essential to interoperability, enabling systems across different countries to connect and exchange data securely. Such standards are already being developed by international and technical bodies. Emerging interface protocols such as the Model Context Protocol (MCP) may provide

[2] This table presents one possible approach to data classification. The classification and applicable regulatory pathway for particular datasets may be determined according to their criticality and the recommendations of the concerned organisation or sectoral regulator.

a reference for standardised AI-system access. Existing and emerging examples include the following:

- **AI Standards:** ISO/IEC JTC 1/SC 42 is one of the key international standards forums for AI-related standards, including foundational AI standards, data quality, trustworthiness, and terminology.
- **Secure infrastructure standards:** The IETF (Internet Engineering Task Force) for the infrastructure layer of the broader data-governance stack has also developed widely used standards, such as TLS 1.3, for secure communication between systems by protecting data while it is being transmitted [53]. Newer developments, including emerging OAuth 2.1 and updated OAuth security and protected-resource standards, support more secure authorisation and access management [54]. It means that systems can define who is authorised to access data, under permissible conditions, and through which secure channels.
- **Identity and trust standards:** OpenID Federation 1.1 supports federated trust by enabling entities, such as institutions, platforms, or service providers, to establish trust through recognised trust anchors[3] or federation authorities[4]. This is important as a system in one country may need to verify whether a user, institution, or service provider from another jurisdiction is trusted, authorised, and operating within an accepted trust framework. W3C Verifiable Credentials Data Model v2.0 supports portable and machine-verifiable digital credentials, enabling claims, permissions, or authorisations issued by one system to be electronically verified by another system. This can reduce dependence on manual checks and support more trusted digital interactions across borders [55] [56].

Despite these developments, several practical challenges continue to limit technical interoperability for cross-border data flows:

- **Different implementation practices:** Technical interoperability is supported by several secure data exchange and communication protocols [57]. However, differences in how these standards are adopted and implemented across jurisdictions and sectors, such as variations in system architecture, data formats and operational practices, can constrain interoperability.

[3] Trusted entities that act as the starting point for verifying whether another system, issuer, or service provider can be trusted within a federation.

[4] Organisations or authorities within a federation that help establish trust relationships between participating entities, such as federation operators, organisations, departments, or sites.

- **Compatibility gaps:** Even where common standards are used, different implementation methods can make systems incompatible in practice. As mentioned in the above pointer, differences in API design, data formats, authentication flows, encryption settings, logging practices, or credential-verification methods can prevent smooth data exchange. This is why implementation monitoring[5], conformity assessment[6], and interoperability testing[7] remain necessary.

- **Evolving security requirements:** Updated guidance, such as RFC 9700, shows that common standards require continuous security improvements and implementation discipline [58].

- **Policy and regulatory barriers:** Differences in data protection rules, localisation requirements, national security concerns, and government access to data can restrict cross-border data flows even when systems are technically capable of exchanging data.

The framework may address these challenges by:

- **Creating a minimum common technical baseline:** Participating countries may agree on core technical requirements for secure exchange, authentication, API connectivity, identity federation, encryption and testing. The framework should not require countries to adopt identical systems. It should allow domestic systems to remain distinct while enabling them to work together.

- **Using existing international and operational references:** The World Bank's ID4D work highlights the role of technical standards in building trusted and interoperable digital identification systems [60]. This may serve as a useful reference for establishing common technical baselines without limiting domestic flexibility.

- **Supporting interoperability sandboxes:** The framework may create testing environments where countries and institutions can test cross-border data exchange before wider deployment.

---

[5] Tracking whether agreed standards and specifications are actually being applied consistently during implementation.

[6] A formal process to demonstrate that a product, service, process, system, or claim meets specified requirements.

[7] Testing whether two or more systems can work together end-to-end as required by the standards on which they are based.

- **Enabling periodic review:** Technical standards, security practices, and implementation profiles may be reviewed regularly to reflect new risks, technologies, and regulatory changes.

- **Enabling capacity building:** Countries with varying levels of digital readiness may receive technical assistance, shared guidance, and training to implement agreed-upon standards.

This framework would allow countries to retain their domestic technical systems while ensuring secure, trusted, and technically reliable cross-border interoperability.

#### 5.1.2.1.2 Shared Semantic Standards and Metadata

Technical compatibility alone does not ensure that data carries the same meaning across systems and jurisdictions. Semantic interoperability, therefore, requires definitions, taxonomies, metadata standards, classifications and a shared understanding of data fields and categories.

The framework may encourage machine-readable metadata to describe datasets, provenance, permitted uses, retention conditions, transfer restrictions and privacy-related attributes, drawing on standards such as W3C DCAT, PROV-O, ODRL, DPV, and ISO/IEC 11179. This would help classify, trace and audit data across systems.

Countries may retain the authority to define sub-categories or apply stricter controls for national security, critical infrastructure and other public-interest concerns. The common interface should not require participating countries to replace their domestic taxonomies. Where exact equivalence is not possible, the mapping should document contextual differences so that interoperability does not result in the loss or misinterpretation of nationally relevant meaning.

### 5.1.2.2 Accountability: Certification and Agreements

A framework for international data interoperability would also require certification standards, agreements and assurance mechanisms to assess whether cross-border data-sharing arrangements meet agreed levels of safety, reliability, and protection. These mechanisms provide a recognised basis for demonstrating compliance and defining the conditions under which data may be accessed, used and transferred. Existing examples include:

- Under the GDPR, certification mechanisms, seals, and marks are encouraged to demonstrate compliance with data-protection requirements, and certification may be issued by certification bodies or competent supervisory authorities.

- The Global CBPR Forum similarly enables trusted cross-border data flows through international privacy certifications, with recognised accountability agents certifying organisational compliance with programme requirements.

- China's Personal Information Protection Law also recognises certification by a specialised body as one route for cross-border transfers of personal information.

Certification can create trust, support compliance and reduce uncertainty in cross-border data-sharing arrangements. However, several challenges limit adoption and mutual recognition for effective interoperability.

- **Fragmented certification:** As we have seen in the earlier section, multiple systems coexist (ISO, APEC, and CBPR) with differing scopes, criteria, and oversight. No single scheme is universally accepted for cross-border AI-related data flows. As a result, organisations may face duplicative assessments, and regulators may hesitate to rely on foreign certifications without equivalence determinations.

- **Asymmetric access and capacity:** Advanced economies concentrate accredited certification bodies, while costs and expertise requirements disadvantage SMEs and institutions in developing countries [70]. This may create a two-tier system in which only well-resourced actors can obtain recognised certifications, limiting inclusive participation.

- **Static certification vs dynamic systems:** Certifications are typically time-bound, but AI systems and data flows evolve rapidly [71]. Most lack mechanisms for continuous assurance or real-time monitoring. This can make certification a snapshot of compliance rather than a continuous assurance mechanism, especially for adaptive AI applications.

- **Scope misalignment with AI-specific risks:** Existing certifications focus on security or privacy management but often lack criteria for AI-specific concerns such as data provenance, explainability, or downstream use restrictions [71] [72]. As a result, certified systems may still pose unaddressed risks in cross-border AI deployment.

This framework may address the above issues through a modular approach combining certification and interoperable agreements:

- **Minimum certification profile:** Participating countries may agree on a minimum certification profile for cross-border data-sharing arrangements, covering security controls, privacy safeguards, auditability, incident response, conformity assessment, and other necessities. The framework can draw from

existing standards such as ISO/IEC 27001, ISO/IEC 27701 and ISO/IEC 42001, while avoiding the need for full harmonisation.

- **Mutual recognition and interoperable agreements**: The framework may also support mutual recognition pathways, where certifications, audit reports, or compliance assessments issued by accredited bodies are recognised bilaterally or plurilaterally, starting with low-risk data categories or specific sectors. Standard data-sharing agreements may similarly define purpose limitation, access conditions, retention, onward transfer, confidentiality, security, accountability, reporting, publication, intellectual property and other relevant conditions.

- **AI-specific assurance:** For AI-related data flows, additional certification modules may be developed for data lineage, bias testing, model documentation, and usage restrictions [71]. Technical capabilities such as data lineage, cryptographic provenance and machine-readable policy attributes may complement legal and organisational safeguards by helping to keep data-use conditions traceable during cross-border processing.

- **Continuous and risk-adaptive assurance:** Rather than relying only on periodic certification, the framework may encourage programmatic monitoring of system logs, data lineage and relevant privacy or security controls, with review triggers when systems, models, processing purposes or risks change. The framework may therefore move from static certification towards continuous and risk-adaptive assurance, particularly for AI systems whose capabilities and uses may change after the initial transfer or authorisation.

#### 5.1.2.3 Coordination: Institutional Governance

In this framework, it is important to address the institutional interoperability challenges observed in the earlier section. Currently, such coordination could be observed within emerging forums. For example:

- Interoperable Europe Act: It creates an Interoperable Europe Board, mandatory interoperability assessments, a common portal, regulatory sandboxes, and support measures to strengthen cross-border public-sector interoperability.

- Global CBPR Forum: It builds on the APEC CBPR System and brings together jurisdictions, certification bodies, and organisations to support trusted cross-border personal data flows through privacy certifications and enforcement cooperation.

- International Network of AI Safety Institutes: Enables cooperation among government-mandated bodies on AI safety research, testing, guidance, and information sharing.

It shows that interoperability requires institutions capable of coordinating implementation, review and trust-building across jurisdictions. However, regional or issue-specific groupings currently largely coordinate such efforts. Despite these efforts, several challenges continue to limit effective institutional coordination for cross-border data interoperability:

- **Fragmentation:** Different institutions focus on different issues. AI safety institutes focus on technical risk, data protection institutions focus on privacy and trade bodies focus on market access [64] [65]. Integrated coordination often remains limited. This can result in the same cross-border data flow facing different and sometimes conflicting requirements from multiple institutions.

- **Asymmetric Participation:** There is an imbalance in participation in international digital standards setting between developed and developing countries, as developing-country stakeholders often face financial, technical, expertise and institutional capacity constraints [66] [67]. This can lead to frameworks reflecting the priorities of advanced economies, reducing trust and adoption in under-represented regions.

- **Enforcement Gaps:** As observed in section 4, some mechanisms are voluntary or non-binding. For example, ASEAN frameworks are largely voluntary, APEC CBPR relies on accountability agents, and cooperation among AI safety institutes does not confer enforcement authority. As a result, compliance may depend on voluntary action and breaches may not have uniform remedies across jurisdictions.

- **Lack of Legal Recognition:** Technical certifications, audit reports or institutional assurances are not automatically recognised across jurisdictions. Cross-border use often requires formal recognition under domestic legal frameworks, which can limit interoperability even where systems are technically compatible.

- **Misalignment:** Data laws, AI regulations and security requirements evolve at different speeds across countries and institutions. This creates regulatory misalignment, making frameworks difficult to maintain and increasing the cost of cross-border implementation [68].

Under this framework, participating countries may address institutional gaps by:

- **Create a structured coordination mechanism:** participating countries may establish one for cross-border data interoperability without supplanting domestic regulators.
- **Designate nodal authorities:** Each country may designate a competent authority or inter-agency unit as the main point of contact for interoperability-related coordination.
- **Set up issue-specific working groups:** The framework may create working groups on technical standards, certification recognition, safeguards, incident response, and review of transfer conditions [69].
- **Develop mutual recognition pathways:** Countries may recognise each other's certifications, audit reports, conformity assessments, or compliance checks, starting with lower-risk data categories or specific sectors.
- **Enable periodic review:** A regular review mechanism may assess emerging risks, regulatory changes, implementation gaps, and technological developments.
- **Preserve sovereign flexibility:** Countries would retain domestic regulatory authority while using the framework as a coordination layer to support trusted and accountable cross-border data interoperability.

The institutional component would therefore function as the coordination mechanism through which the other elements of the framework can be implemented, reviewed and recognised across jurisdictions.

## 5.2 Demonstrating the Framework: Cross-border Health Data

In this section, a demonstration of the proposed framework is provided for the health data ecosystem. Health data already has relatively well-developed technical, semantic and institutional arrangements, while also presenting significant privacy, ethical and security risks that require differentiated approaches. The framework may be applied for different sectors by first determining the nature and risk of the data, identifying an appropriate access or processing pathway, and then applying the necessary requirements for compatibility, accountability, and coordination.

**Risk Classification and Access Pathways for Health Data**

The desired pathway for health data may depend on several factors, including whether the data is aggregated or identifiable, its sensitivity, the purpose for which it is being used, the possibility of re-identification or inference, and the safeguards available. Lower-risk, aggregated or sufficiently de-identified datasets may support relatively low-friction exchange,

while identifiable or sensitive clinical and genomic data may require controlled-access arrangements. For highly sensitive datasets, as proposed in the framework, federated approaches may allow analysis while keeping the underlying data within a controlled environment. The access pathway should be determined before considering whether the systems involved are technically capable of exchanging the data.

**Technical and Semantic Compatibility for Health Data**

Once the appropriate access pathway is identified, the compatibility layer could, under this framework, determine whether health data systems can securely exchange and interpret information. India already has a substantial technical foundation. The Electronic Health Record (EHR) Standards for India provide a national framework for structuring and exchanging electronic health records [59]; HL7 FHIR R4 [85], including its implementation through the ABDM FHIR Implementation Guide [86], enables machine-readable and API-based exchange of clinical information; and DICOM [87] provides standard formats for medical imaging such as X-rays, CT and MRI. Initiatives such as MIDAS are also developing health datasets for AI research using interoperable imaging formats, standardised metadata and annotations.

However, the availability of technical standards does not by itself make health datasets interoperable or AI-ready. Here, the proposed framework could support common health-data implementation profiles that specify how existing standards should be applied for cross-border use, including requirements for APIs, security, metadata, provenance, de-identification and documentation. These profiles could be tested through interoperability sandboxes before wider use. Evolving initiatives such as MIDAS 2.0 may also provide useful approaches for assessing data quality, interoperability, AI readiness and residual privacy risks [88].

According to the framework, the subsequent layer is semantic compatibility. It ensures that clinical information retains the same meaning across institutions and jurisdictions. Existing standards, such as SNOMED CT, support consistent representation of clinical concepts [89]; LOINC standardizes laboratory tests, measurements, and observations [90]; and ICD and other WHO-FIC classifications support disease classification and statistical reporting [91]. The challenge is less the absence of terminology standards than their consistent implementation, including standardised labels, complete metadata and reliable mappings between systems.

For this purpose, common semantic profiles may also be utilised. The International Patient Summary provides a useful example of a defined core dataset for exchanging essential patient information, with jurisdiction-specific implementations such as the Indian Patient Summary under ABDM. However, such specifications are designed primarily for individual patient summaries rather than bulk datasets for AI research. Cross-border AI applications would therefore require additional dataset-level metadata and documentation describing provenance, permitted use, data quality, access restrictions and other relevant conditions.

**Legal Accountability and Assurance Conditions for Health Data**

Once technical and semantic compatibility is established, another building block under this framework is accountability. This determines the legal and assurance conditions under which the data may be accessed or used. India currently has several relevant instruments, including HMSC (Health Ministry's Screening Committee) clearance [92], clearance for international collaborative health research, ICMR ethical guidance on AI in healthcare [93], the Digital Personal Data Protection Act 2023 (Section 16), and Material Transfer Agreements involving biological material [94]. These mechanisms address issues such as anonymisation, purpose, confidentiality, intellectual property, publication and security. However, they do not create a single operational pathway for cross-border AI-health collaboration, particularly for issues such as secondary use, downstream transfer, model outputs, benefit-sharing and controlled access.

The proposed framework could address this by linking the selected risk and access pathway to standard data-sharing or data-use agreements. These agreements could specify the authorised purpose, permitted users, onward transfer, confidentiality, treatment of derived models or outputs, audit requirements and conditions for termination or further use. Legal approval could therefore be linked directly to the technical safeguards applied to the dataset. For higher-risk uses, continuing assurance through audit logs, data lineage and periodic review could help ensure that the conditions remain appropriate where the data, model capabilities or intended use change. Controlled-access models such as EGA and dbGaP, discussed in the above section, provide useful references for purpose-specific and institutionally governed access.

**Institutional Pathway for Coordination in Health Data Transfer**

Finally, the coordination layer would connect these technical, semantic and accountability requirements with the institutions responsible for implementing them. India already has multiple relevant bodies: ICMR, DHR and HMSC provide research-governance and approval functions; ethics committees address consent, privacy and participant protection [95]; and ABDM and National Health Claims Exchange (NHCX) provide domestic infrastructure for interoperable health-information exchange [96] [97] [98]. However, these arrangements do not currently provide a single coordinated pathway.

## 5.3 Key Recommendations for Operationalising the Framework in India:

1. **Create a Risk-Based Access Mechanism**

The first layer for enabling cross-border data is to classify the data and determine the appropriate access or processing pathway. Data classification can be done through a graded approach based on the associated risk mentioned in the document. This allows countries to enable interoperability without giving up control over sensitive data and helps to balance

cross-border data use with data sovereignty. The classification and access mechanism may be further developed with sectoral experts and relevant regulators, as the nature of risk and appropriate safeguards will differ across areas such as health, finance, agriculture, or critical infrastructure.

2. **Establish a technical baseline for cross-border data transfer:**

A minimum technical interoperability baseline could be developed for cross-border use of AI-related data. In India, this could be coordinated by BIS and relevant sectoral standards bodies and may define minimum requirements for secure exchange. The baseline may be applied through sector-specific implementation profiles and interoperability sandboxes, followed by periodic testing and review. This would allow domestic systems to remain different while ensuring that they can work together securely and reliably for cross-border data use.

3. **Operationalise Continuous and Risk-Adaptive Assurances**

For accountable Cross-border data transfer, a common assurance protocol needs to define the minimum conditions that apply before access or transfer and how compliance will be maintained afterward. Certification may be used as an initial trust mechanism, but it should be complemented by continuous monitoring and traceability of how the data is used, including whether agreed conditions on purpose, retention, onward transfer and derived outputs are being followed.

4. **Establish an integrated AI-specific layer in the existing instrument for Institutional Coordination**

Globally, responsibilities for cross-border data use are distributed among data-protection authorities, sectoral regulators, standards bodies, cybersecurity institutions and other agencies. This can create overlapping requirements, unclear responsibilities, and fragmented approval pathways. The newly constituted National Data Governance Committee in India is mandated to coordinate and support functions related to data sharing, safeguards, compliance and audit. However, AI-related cross-border data transfer raises additional concerns. Within this body itself, a central interdisciplinary AI-data interoperability coordination body may be constituted as a nodal institution mechanism for this purpose. This body would not replace existing regulators but coordinate with them by bringing together technical experts, sectoral regulators, legal and ethics experts, cybersecurity institutions, AI researchers and standards bodies.

## 6. Conclusion

The challenge identified in this paper for cross-border data governance is to balance trusted data flows for AI innovation, development and international cooperation while preserving national control over sensitive data. Excessive localisation can restrict innovation and global collaboration, while unrestricted openness can weaken regulatory oversight, privacy protection, and sovereign control.

The framework proposed in this paper does not require the country to adopt laws, systems or standards identical to those of other countries. Instead, it enables working together with partner countries while retaining domestic regulatory authority and sovereign flexibility. The framework can support lawful, secure and trusted cross-border data flows for AI development through a minimum interoperability layer, while ensuring that data sovereignty, security and accountability remain central to the governance of the digital economy.

This framework is not intended as a prescriptive recommendation for any specific institution, government or organisation. Rather, it is proposed as a basis for deliberation and further discussion on how to enable international data interoperability. Such deliberation can help refine the framework, identify practical gaps and support the development of more comprehensive and context-appropriate solutions.

******

## References


1. International Data Centre Authority. (2025). *Global digital economy report (2025)*.
2. Mishra, D., Kedia, M., Reddy, A., Fernandez, C., Shukla, S., Ramnath, K., & Vanguri, S. (2025). *Estimation and measurement of India's digital economy.* Indian Council for Research on International Economic Relations; Ministry of Electronics and Information Technology.
3. United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development: For whom the data flow*. United Nations.
4. World Bank. (2021). *World development report 2021: Data for better lives*.
5. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations*.
6. National e-Governance Division. (2026). National Data Governance: Interoperable & Integrated Government Databases. Accessed on 27th July 2026.
7. OECD, World Trade Organisation, (2025), Economic implications of Data Regulation.
8. Cory, N., & Dascoli, L. (2021, July 19). *How barriers to cross-border data flows are spreading globally, what they cost, and how to address them*. Information Technology and Innovation Foundation.
9. Deane, F., Woolmer, E., Cao, S., & Tranter, K. (2024). Trade in the digital age: Agreements to mitigate fragmentation. *Asian Journal of International Law*, *14*(1), 154–179. https://doi.org/10.1017/S204425132300036X
10. Aaronson, S. A. (2020). Data is dangerous: Comparing the risks that the United States, Canada, and Germany see in data troves. *International Journal of Communication*, *14*, 2686–2713.
11. Global Commission on Internet Governance. (2016). *Our Internet: The collected research papers of the Global Commission on Internet Governance* (Vol. 1). Centre for International Governance Innovation.
12. World Economic Forum. (2023). *Data free flow with trust (DFFT): Paths towards free and trusted data flows*.
13. Asia-Pacific Economic Cooperation. (2019). *APEC Cross-Border Privacy Rules system: Policies, rules and guidelines.*
14. European Commission. (Accessed on May 3, 2026 ). *Adequacy decisions*.

15. DeFranco, J., Roberts, J., FJoanna F DeFranco, Joshua Roberts, David Ferraiolo, D Chris Compton, An infrastructure for secure data sharing: a clinical data implementation, *JAMIA Open*, Volume 7, Issue 2, July 2024, ooae040.

16. e-Estonia. (Accessed on May 3, 2026). *Data embassy.*

17. *Interoperability: Towards a data-driven public sector (2022)*. World Bank.

18. Ibid., 17

19. Hinderer, A. (2023, January 10). *Why cross-border data flows are so important.* World Economic Forum.

20. European Commission. (2017). *New European interoperability framework: Promoting seamless services and data flows for European public administrations*.

21. Ibid., 2

22. Centre for Digital Property and Governance. (2024). *State of India's digital public infrastructure (DPI) report*. Indian Institute of Management Bangalore.

23. Organisation for Economic Co-operation and Development. (2022). *Fostering cross-border data flows with trust*.

24. United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development: For whom the data flows.* United Nations.

25. United Nations Conference on Trade and Development. (2023). G20 members' regulation on cross-border data flows. (UNCTAD/DTL/ECDC/2023/1). United Nations.

26. United Nations Conference on Trade and Development. (2021). *Digital economy report 2021: Cross-border data flows and development: For whom the data flow*. United Nations.

27. Ministry of Electronics and Information Technology. (2023). *The Digital Personal Data Protection Act, 2023* (No. 22 of 2023). Government of India.

28. Department of Science and Technology. (2012). *National Data Sharing and Accessibility Policy (NDSAP)*. Government of India. [Gazzate]

29. Reserve Bank of India. (2019, June 26). *Storage of payment system data*.

30. Intersoft Consulting. (Accessed on May 3, 2026). *Art. 45 GDPR: Transfers based on an adequacy decision*. General Data Protection Regulation (GDPR).

31. International Trade Administration. (Accessed on May 3, 2026). *Program overview.* U.S. Department of Commerce.

32. Intersoft Consulting. (Accessed on May 3, 2026). *Art. 46 GDPR: Transfers subject to appropriate safeguards*. General Data Protection Regulation (GDPR).

33. Intersoft Consulting. (Accessed on May 3, 2026). *Art. 48 GDPR: Transfers or disclosures not authorised by Union law*. General Data Protection Regulation (GDPR).

34. Department of Justice. (2024). *Preventing access to Americans' bulk sensitive personal data and United States government-related data by countries of concern* (89 FR 15780). Federal Register.

35. U.S. Department of Justice. (2024, February 28). *Fact sheet: Justice Department to implement Executive Order on preventing access to Americans' bulk sensitive personal data and United States government-related data by countries of concern*.

36. National Security Division, (2024) Department of Justice, 28 C.F.R. § 202.

37. Ibid., 35

38. U.S. Department of Justice. (2019, April). *The CLOUD Act: A white paper*.

39. Standing Committee of the National People's Congress. (2016, November 7). *Zhonghua Renmin Gongheguo wangluo anquan fa* [Cybersecurity law of the People's Republic of China]. Cyberspace Administration of China.

40. Supreme People's Procuratorate of the People's Republic of China. (2021, June 10). *Data Security Law of the People's Republic of China*.

41. Supreme People's Procuratorate of the People's Republic of China. (2021, December 29). *Personal Information Protection Law of the People's Republic of China*.

42. China Law Translate. (2024, March 22). *Provisions on promoting and regulating the cross-border flow of data*.

43. Association of Southeast Asian Nations. (2016). *ASEAN framework on personal data protection.*

44. Association of Southeast Asian Nations. (2018). *ASEAN framework on digital data governance.*

45. Association of Southeast Asian Nations. (2021). *ASEAN model contractual clauses for cross-border data flows.*

46. African Union. (2024). *African Union data policy framework* (V2).

47. African Union. (2014, June 27). *African Union convention on cyber security and personal data protection*.

48. African Union. (2024, February). *Protocol to the agreement establishing the African Continental Free Trade Area on digital trade*.

49. African Union. (2022, February). *Interoperability framework for digital ID*.

50. Asia-Pacific Economic Cooperation. (2015). *APEC privacy framework*.

51. Asia-Pacific Economic Cooperation. (2019, September). *APEC Cross-Border Privacy Rules system: Policies, rules, and guidelines*.

52. Asia-Pacific Economic Cooperation. (2019). *APEC cooperation arrangement for cross-border privacy enforcement*.

53. Rescorla, E. (2026, July). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 9846), Internet Engineering Task Force.

54. Hardt, D., Parecki, A., & Lodderstedt, T. (2024, July 31). *The OAuth 2.1 authorisation framework* (Internet-Draft draft-ietf-oauth-v2-1-12). Internet Engineering Task Force.

55. Hedberg, R., Jones, M. B., Bradley, J., Lizar, M., & Solberg, Andreas. (2026, Feb 17). *OpenID federation 1.0* (Implementer's Draft 4). OpenID Foundation.

56. Sporny, M., Longley, D., Zundel, B., Yasuda, K., & Thibodeau, T., Jr. (Eds.). (2025, May 15). *Verifiable credentials data model v2.0*. W3C.

57. European Commission. (2017, March 23). *Annex 2 to the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: European interoperability framework – implementation strategy* (COM(2017) 134 final). EUR-Lex.

58. Bradley, J., Lodderstedt, T., & Salo, J. (2025, February). *OAuth 2.0 security best current practice* (RFC 9700). Internet Engineering Task Force.

59. National Resource Centre for EHR Standards. (Accessed on 27 Aug 2026). EHR Standards for India.

60. Mittal, A. (2022, August). *Catalog of technical standards for digital identification systems.* World Bank.

61. Albertoni, R., Browning, D., Cox, S., Beltran, A. G., Perego, A., & Winstanley, P. (Eds.). (2024, August 22). *Data catalog vocabulary (DCAT) - version 3.* W3C.

62. *Artificial intelligence risk management framework:* (2024, July 25). *Generative AI profile* (NIST AI 600-1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.AI.600-1

63. Agencia Española de Protección de Datos & European Data Protection Supervisor. (2021, April 27). *10 misunderstandings related to anonymisation*.

64. International Network of AI Safety Institutes. (2024, November 20). *Mission statement: International Network of AISIs*—National Institute of Standards and Technology.

65. Organisation for Economic Co-operation and Development. (2021). *Digital trade inventory: Rules, standards and holistic policy responses*. OECD Publishing.

66. International Institute for Sustainable Development. (2025, November). *Technical standards and digital trade: Navigating the path to sustainable and inclusive growth*.

67. World Bank Report (2025), Standards for development, Part 4: Making Standards a Springboard for Development, Rather Than a Straitjacket.

68. International Scientific Report on the Safety of Advanced AI. (2026, February). *International AI safety report 2026*.

69. Ibid 44.

70. The International Monetary Fund, the Organisation for Economic Co-operation and Development, the United Nations, The World Bank and the World Trade Organisation (2023). *Digital Trade for development*.

71. National Institute of Standards and Technology. (2023, January). *Artificial intelligence risk management framework (AI RMF 1.0)* (NIST AI 100-1).

72. International Organisation for Standardisation. (2024, February 14). *ISO/IEC 42001 explained: What it is and why it matters*.

73. Bauer, M., Lee-Makiyama, H., van der Marel, E., & Verschelde, B. (2014). *The Impact of Data Localisation on India's Economy*. ECIPE.

74. Cory, N., & Dascoli, L. (2021). *How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*. Information Technology and Innovation Foundation.

75. Carlini, N., et al. Extracting Training Data from Large Language Models. 30th USENIX Security Symposium (USENIX Security 21), (2021, August 11) ISBN: 978-1-939133-24-3

76. Health Data Hub. (2026). France-India: A technological collaboration to secure access to health data for research and care.

77. iSPIRT. (2026). DEPA Private Inferencing.(Accessed on 27th Aug 2026)

78. Indian Council of Medical Research. (2026). Letter of Intent between the Indian Council of Medical Research (ICMR), Department of Health Research, Government of India and Platforme Des Données de Santé (“Health Data Hub”), France.

79. GDPR-Info.eu. (Accessed on 27 Aug 2026). Art. 44 GDPR – General principle for transfers.

80. European Genome-phenome Archive. (Accessed on 27 Aug 2026).

81. National Institutes of Health. (2025). How to Register and Submit a Study in dbGaP.

82. Supreme People's Procuratorate of the People's Republic of China. (2021). Article 38 Personal Information Protection Law of the People's Republic of China.

83. Supreme People's Procuratorate of the People's Republic of China. (2021). Article 39 Personal Information Protection Law of the People's Republic of China.

84. Association of Southeast Asian Nations. (2018). ASEAN Framework on Digital Data Governance.

85. National Resource Centre for EHR Standards. (2026). HL7 FHIR.

86. National Resource Centre for EHR Standards. (Accessed on 27 Aug 2026). FHIR Implementation Guide for ABDM (Ayushman Bharat Digital Mission).

87. National Resource Centre for EHR Standards. (Accessed on 27 Aug 2026). DICOM.

88. Indian Council of Medical Research. (Accessed on 27 Aug 2026). Medical Image Data for AI and Standardization (MIDAS).

89. National Resource Centre for EHR Standards. (2026). SNOMED CT.

90. National Resource Centre for EHR Standards. (Accessed on 27 Aug 2026). Guide for using LOINC in ABDM FHIR Resources.

91. World Health Organization. (2026). ICD-11 for Mortality and Morbidity Statistics (Version 2026-01): Certain infectious or parasitic diseases.

92. Indian Council of Medical Research. (Accessed on 27 Aug 2026). Health Ministry's Screening Committee (HMSC).

93. Indian Council of Medical Research. (2023). Ethical Guidelines for Application of Artificial Intelligence in Biomedical Research and Healthcare.

94. Indian Council of Medical Research. (Accessed on 27 Aug 2026). Transfer of Human Biological Material.

95. Indian Council of Medical Research. (2017). National Ethical Guidelines for Biomedical and Health Research Involving Human Participants.

96. Press Information Bureau, Ministry of Health and Family Welfare. (2026, May 6). *Swasth Bharat Portal Unveiled: Unifying Fragmented Health Systems to Power India's Digital Health Transformation*. Government of India.

97. National Health Authority. (Accessed on 27 Aug 2026). Health Claims Exchange (HCX) Sandbox.

98. National Health Authority. (Accessed on 27 Aug 2026). Health Information Exchange and Consent Manager (HIE-CM) Specifications.

## Annexure

The table below distinguishes access according to the party whose access is being governed and the stage at which safeguards apply. This distinction is relevant to cross-border AI interoperability because different forms of data and AI use may require different access pathways rather than a single mechanism for all data flows.

| Stage | Access concerning an individual — AI in use/inference | Access concerning an institution — AI development/training |
|---|---|---|
| At the point of data access or exposure | **Consent-based access:** The individual authorises access to data under specified purposes and conditions. | **Data exchange:** A custodian makes an approved dataset available to authorised parties under defined access and use conditions. |
| During computation, while data remains in place | **Controlled/private computation:** Processing takes place within a protected environment and only authorised outputs are returned, subject to applicable legal and consent requirements. | **Data collaboration:** Two or more custodians enable joint computation under agreed conditions, including model-to-data or federated approaches, without requiring the underlying raw data to move between participants. |

Table 2: Potential forms of data access under the framework

## List of Abbreviations

| Abbreviation | Full Form |
|---|---|
| ABAC | Attribute-Based Access Control |
| ABDM | Ayushman Bharat Digital Mission |
| AfCFTA | African Continental Free Trade Area |
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| APEC | Asia-Pacific Economic Cooperation |
| ASEAN | Association of Southeast Asian Nations |
| AU | African Union |
| BIS | Bureau of Indian Standards |
| CBDF | Cross-Border Data Flows |
| CBPR | Cross-Border Privacy Rules |
| CFR | Code of Federal Regulations |
| CLOUD Act | Clarifying Lawful Overseas Use of Data Act |
| CPEA | Cross-border Privacy Enforcement Arrangement |
| CT | Computed Tomography |
| DAA | Data Access Agreement |
| DAC | Data Access Committee |
| DCAT | Data Catalog Vocabulary |
| DEPA | Data Empowerment and Protection Architecture |
| DHR | Department of Health Research |
| DICOM | Digital Imaging and Communications in Medicine |
| DPI | Digital Public Infrastructure |
| DPV | Data Privacy Vocabulary |
| DSCI | Data Security Council of India |
| DSP | Data Security Program |

| | |
|---|---|
| DUC | Data Use Certification |
| EGA | European Genome-phenome Archive |
| EHR | Electronic Health Record |
| EU | European Union |
| FHIR | Fast Healthcare Interoperability Resources |
| GDP | Gross Domestic Product |
| GDPR | General Data Protection Regulation |
| HL7 | Health Level Seven |
| HMSC | Health Ministry's Screening Committee |
| ICD | International Classification of Diseases |
| ICMR | Indian Council of Medical Research |
| ID4D | Identification for Development |
| IEC | International Electrotechnical Commission |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| ISO/IEC JTC 1/SC 42 | ISO/IEC Joint Technical Committee 1, Subcommittee 42 on Artificial Intelligence |
| LOINC | Logical Observation Identifiers Names and Codes |
| MCC | Model Contractual Clauses |
| MCP | Model Context Protocol |
| MIDAS | Medical Imaging and Information Datasets for India |
| MIDAS 2.0 | Metric-based Integrity and Data Assessment System |
| MRI | Magnetic Resonance Imaging |
| MSME | Micro, Small and Medium Enterprise |
| NHCX | National Health Claims Exchange |
| NIH | National Institutes of Health |
| NIRDH | National Institute for Research in Digital Health |

| | |
|---|---|
| NIST | National Institute of Standards and Technology |
| NRCeS | National Resource Centre for EHR Standards |
| OAuth | OAuth Authorization Framework |
| ODRL | Open Digital Rights Language |
| PETs | Privacy-Enhancing Technologies |
| PIPL | Personal Information Protection Law |
| PRC | People's Republic of China |
| PROV-O | PROV Ontology |
| PSA | Principal Scientific Adviser |
| RBI | Reserve Bank of India |
| RFC | Request for Comments |
| SME | Small and Medium-sized Enterprise |
| SNOMED CT | Systematized Nomenclature of Medicine – Clinical Terms |
| TLS | Transport Layer Security |
| UNCTAD | United Nations Conference on Trade and Development |
| U.S. / US | United States |
| W3C | World Wide Web Consortium |
| WHO-FIC | World Health Organization Family of International Classifications |
| dbGaP | database of Genotypes and Phenotypes |

भारत सरकार के प्रधान वैज्ञानिक सलाहकार का कार्यालय
Office of the Principal Scientific Adviser
to the Government of India

www.psa.gov.in

/prinsciadvoff @prinSciAdvOff @prinSciAdvOff @PrinSciAdvOff