世界互联网大会
World Internet Conference

Comparative Study on Global Cross-Border Data Flow Policies

World Internet Conference Data Working Group

April 2025

World Internet Conference Data Working Group

- Chair

LIANG Hao	Executive Deputy Secretary-General of World Internet Conference

- Vice Chairs

LEE Xiaodong	Founder & CEO of Fuxi Institution, Researcher of Chinese Academy of Sciences (Coordinator)
MENG Qingguo	Director of Center for Internet Governance of Tsinghua University, Professor of the School of Public Policy and Management of Tsinghua University
Andrew Christopher Macmyn BROWN	Director of Uk-China Business Environment Programme, British Standards Institution

- Consultants

XUE Lan	Distinguished Professor of Arts, Humanities and Social Sciences at Tsinghua University and Dean of Schwarzman College
JI Weidong	Distinguished Professor of Arts, Humanities and Social Sciences at Shanghai Jiao Tong University and President of China Institute for Socio-Legal Studies

- Members

BAI Fengjun	Senior Director of Public Affairs, IBM
GU Wei	Deputy Director of Legal Research Center, Alibaba Group
WU Fangfang	Senior Data Security Engineer, Baidu
SUN Shuo	Senior Expert of Data Security, Baidu
YAN Yong	Chief Scientist for Blockchain, State Grid Zhejiang Electric Power Co., Ltd.
CHENG Wenbo	Senior Director of Information Research and Development Center, Hangzhou Anheng Information Technology Co., Ltd.
LIU Shaopeng	Head of Union Studies Association Ecology, Hangzhou Anheng Information Technology Co., Ltd.
LI Li	Executive Director of JD Legal Research
SONG Yulun	Senior Vice President and Member of the Party Committee, Unicom Digital Tech Co., Ltd.
PAN Deng	Department Manager, Big Data Innovation Application Product Department, Unicom Digital Tech Co., Ltd.
ZHANG Xin	Senior Legal Counsel for Data Security and Privacy Protection, Lenovo
HU Yongqi	Director of Government Affairs, Lenovo
LV Yao	Director of Compliance and Public Affairs Department, Ant Group
Danil KERIMI	Board Member, SealSQ (Nasdaq: LAES).

QU Guangfei	China Data Protection Officer and Greater China Data Protection Privacy Coordinator, SAP
ZHANG Hao	Director of Policy Research, SAP
WEI Hang	Chief Architect, Cisco Systems
ZHANG Xin	Deputy Director (in Chair), Data Development Center of China Telecom
ZHOU Weihua	Deputy Director of Data Cooperation Department, Data Development Center of China Telecom
LANG Ping	Director of National Security Research Office, Institute of World Economics and Politics, Chinese Academy of Social Sciences
HAN Bing	Deputy Director and Associate Researcher of National Security Research Office, Institute of World Economics and Politics, Chinese Academy of Social Sciences
WEI Sha	Deputy Chief Engineer of Informatization and Industrialization Integration Research Institute, CAICT
ZHANG Chunfei	Deputy Director of Policy and Economics Research Institute, CAICT
TAO Tao	Deputy General Manager of China Mobile Information Technology Center
LIN Lin	Director of the User and Market Research Institute, China Mobile Research Institute
ZHU Ji	Director of Data Management Division, Information Technology Management Department of CITIC Group Co., Ltd.

- Editors

Fuxi Institution: YU Nisi, CHENG Kai

Foreword

Cross-border data flows have become an important component of global digital commerce, supporting economic growth and enhancing social welfare. According to statistics from the World Trade Organization (WTO), the scale of global digital services trade exceeded $4.25 trillion in 2023, with an average annual growth rate of nearly 11% over the past five years, accounting for more than half of global services trade[1] , most of which was contributed by cross-border data flows. According to the estimation of the International Chamber of Commerce (ICC), by the end of 2025, the contribution of cross-border data flows to global GDP will grow to $11 trillion[2] .

Nevertheless, different countries have implemented distinct policy approaches to cross-border data flows, data sovereignty, and data ownership, leading to a fragmented landscape in global legislation on cross-border data flows. The current governance framework for cross-border data flows has, in effect, increased the compliance costs, operational complexity, and uncertainty of expectations for enterprises and other data trading entities.

In response to this challenge, Chinese President Xi Jinping proposed the *Global Cross-Border Data Flow Cooperation Initiative* during the 31st APEC Leaders' Informal Meeting in November 2024. He called on the international community to sincerely contemplate the interests and apprehensions of all stakeholders concerning data security and development, while fully respecting the diverse policies, regulations, and practices implemented by different countries and regions due to their specific national and social conditions, and to foster consensus on cross-border data flow regulations among nations and regions through dialogue.

The World Internet Conference has attached great importance to the issue of cross-border data flows. During the 2024 Wuzhen Summit, the Data Working Group released the research report titled *Promoting Open, Collaborative, and Mutually Beneficial Global Data Cooperation.* The report proposes that global data cooperation policies should be formulated based on the principles of openness and inclusiveness, with due respect for the diversity of data governance propositions.

Against the above mentioned backdrops, a total of 194 policy documents concerning cross-border data flows, issued by 136 countries (or regions), international organizations, and trade agreements up to the end of 2024 are reviewed and compared in this report. It systematically extracts policy provisions and practices related to data possession, transfer, and receiving, and categorizes prevailing policy paradigms based on the mechanisms and instruments described in the texts. Building on this analysis, the report offers policy recommendations to facilitate cross-border data flows, with the aim of contributing to the development of an inclusive and open international policy framework for data cooperation.

[1] WTO. Digitally delivered services trade dataset. Available at: https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm (Accessed: 1 April 2025)

[2] ICC. What is the importance of global data flow in international trade? Available at: https://iccwbo.org/global-insights/digital-economy/data-flows/ (Accessed: 1 April 2025)

Table of Content

I.

Core Conclusions of the Report

A. Global Cross-Border Data Flow Policies Exhibit Three Main Paradigms

The fundamental policy paradigms[3] regulating global cross-border data flows are classified into three categories: the Framework-based Facilitation Approach, the Prudent and Flexible Approach, and the Restrictive Approach. The Framework-based Facilitation Approach employs a "principle + accountability" model, depending on corporate responsibility and ex post accountability mechanisms to streamline regulatory processes. The Prudent and Flexible Approach employs an "assessment + instruments" model, aligning adequacy assessments are paired with compliance instruments to achieve a balance between data mobility and privacy protection. The Restrictive Approach employs an "approval + restriction" strategy, characterized by stringent ex ante approval and regional bans to ensure comprehensive control throughout the data lifecycle.

B. Prudent and Flexible Approach Are Widely Adopted in Global Cross-Border Data Flow Policies

The Prudent and Flexible policy represents the predominant approach, accounting for approximately 59.28% of global cross-border data flow policies, whereas the Framework-based Facilitation Approach accounts for about 26.29%, and the Restrictive Approach constitutes about 14.43%. The adoption of Prudent and Flexible policies reached its peak in 2018, primarily driven by the implementation of the European Union's *General Data Protection Regulation* (GDPR).

[3] In this report, "policy paradigms" refer to the value hierarchy, intervention logic, and combination of policy instruments reflected in a given policy document. It represents the document's underlying governance philosophy on cross-border data flows, and can be identified through elements such as the degree of obligation, flexibility, and stated objectives of its provisions.

C. Some Countries Are Gradually Tightening Their Policy Paradigms

Moreover, since 2018, there has been a steady rise in Restrictive Approach policies. Some economies including the United States, Russia, and Brazil have implemented stricter security-focused regulations. For instance, Russia's 2020 issuance of the *List of Foreign Countries Approved for Adequate Protection of Personal Data Subjects* and the United States' 2024 *Final Rule on "Addressing Foreign Adversaries' Acquisition of Sensitive Personal Data of U.S. Citizens"* are both examples of Restrictive Approach policies.

D. Combinations of Policy Mechanisms and Instru-ments in Global Cross-Border Data Flow Policies Are Growing

Analysis indicates that 71.79% of policies address data subject's right to informed consent. The primary mechanisms[4] and instruments[5] that reconciling development and security include adequacy assessments (45.64%), enterprise-specific contractual clauses (38.46%), and standard contractual clauses (30.26%), with many policies permitting integrated application of these measures. Ex-post accountability (35.38%) and business accountability (28.72%) are also widely applied. Overall, standardized instruments aimed at promoting data flow predominate, whereas restrictive measures demonstrate limited prevalence. Although the adoption of ex-ante approvals and regional restrictions has increased since 2016, their overall proportions remain below 10%.

E. Each of the Three Policy Paradigms Has Its Own Suitable Application Scenarios

The Framework-based Facilitation Approach is beneficial due to its robust regulatory adaptability, minimal compliance costs, and capacity to promote innovation. However, this approach exhibits limitations including insufficient regulatory supervision and fragmented rules. It pertains to situations involving the cross-border flow of high-frequency non-critical data[6] and to the regional collaboration. The Prudent and Flexible Approach achieves equilibrium between data flows and data protection, featuring relatively high regulatory compatibility. However, it is constrained by high compliance costs and procedural complexity. It is appropriate for cross-border scenarios involving critical high-value data[7] , and relies on cooperation between countries with developed data industries. The Restrictive Approach prioritizes on national security, the advancement of domestic digital industry, and the safeguarding of privacy, but may also hinder the expansion of the digital economy, elevate business expenses, and diminish international trust. This paradigm is primarily adopted for critical data related to national security and the initial phases of cultivating domestic digital industries.

F. Global Cooperation on Cross-Border Data Flow Primarily Aims to Promote Development

Global cooperation policies on cross-border data flow are characterized by: plurilateral arrangements typically adopt either the Framework-based Facilitation Approach or the Prudent and Flexible Approach, emphasizing combination of instruments such as standard contractual clauses, tiered management, and informed consent, and promoting unrestricted data flows through data localization exemptions; conversely, trade agreements prioritize the principle of free flow while minimizing procedural controls. The Restrictive Approach paradigm is rarely utilized in either mechanism type.

[4] In this report, "policy mechanisms" refer to systematic arrangements designed to achieve policy objectives.

[5] In this report, "policy instruments" refer to specific means or methods directly used to achieve policy objectives.

[6] In this report, "high-frequency non-critical data" refers to data that is frequently collected, transmitted, and used in the course of daily business activities and societal operations, but which has limited impact on personal privacy, national security, or core commercial interests.

[7] In this report, "critical high-value data" refers to data whose content is highly sensitive and, if leaked or misused, may pose potential risks to corporate interests, economic activity, social stability, or national security. At the same time, such data carries significant economic, social, or scientific value and holds broad application prospects. This type of data is typically subject to stricter legal and regulatory protections, but when used appropriately under compliant and controlled conditions, it can generate substantial benefits in areas such as innovation-driven development, industrial upgrading, and public governance.

II.

Basic Paradigms of Global Cross-Border Data Flow Policies

Cross-border data flows generally encompass three operational stages: Data Possession[8] , Data Transfer[9] , and Data Receiving[10] .This report primarily identifies and summarizes policy paradigms derived from the stipulations outlined in policy documents regarding the Data Transfer stage.

Methodologically, the report utilizes the United Nations Conference on Trade and Development (UNCTAD)'s Data Protection and Privacy Legislation Worldwide database[11] and DLA Piper's Data Protection Laws of the World database[12] . A provision-level analysis was conducted across the policy documents covered in these databases for each country, with exclusion criteria applied to non-transmission-related documentation. In cases where multiple provisions originated from identical policy document, the textual consolidation was implemented accordingly. Furthermore, through systematic content analysis of the policy texts, the primary policy mechanisms and policy instruments were taxonomized and codified using established coding protocols. This report examines a total of 194 policy documents concerning cross-border data flows from 136 countries, international organizations, and trade agreements worldwide by the end of 2024. By referring to classification criteria published by relevant academic groups[(13-18)] —and based on the type of **mechanisms and instruments** in the policy content (see Table 1)—three dominant policy paradigms of global cross-border data flow emerge: (1) the Framework-based Facilitation Approach, (2) the Prudent and Flexible Approach, and (3) the Restrictive Approach.

[8] In this report, "Data Possession" refers to the storage, management, and control of data by entities such as enterprises or institutions within their respective jurisdictions.

[9] In this report, "Data Transfer" refers to the process by which data is transmitted from the possessing party to the receiving party, including technical cross-border transmission activities such as API calls, cloud synchronization, or physical media transfers.

[10] In this report, "Data Receiving" refers to the act whereby an overseas entity (such as an enterprise, institution, or individual) acquires and exercises control over the cross-border data.

[11] UNCTAD. Data Protection and Privacy Legislation Worldwide. Available at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide (Accessed: 1 April 2025)

[12] DLA PIPER. Data Protection Laws of the World. Available at: https://www.dlapiperdataprotection.com (Accessed: 1 April 2025)

[13] Casalini F, González J L. (2019). Trade and cross-border data flows. OECD Trade Policy Papers, 220.

[14] Casalini F, González J L, Nemoto T. (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. OECD Trade Policy Papers, 248.

[15] World Bank. (2021). World development report 2021: Data for better lives. World Bank Publications.

[16] Feng, S., & Xue, S. (2024). Global distribution of policy preferences for cross-border data flows: A comparative study of governance models at the national level. Russian Journal, 14(3), 8 – 28.

[17] Li, C., & Wu, X. (2024). A comparative analysis and implications of data governance policies and practices in the US, EU, and Japan. Digital Library Forum, 20(7), 11 – 18.

[18] Kong, W., & Chen, L. (2025). Reinterpreting the driving factors of cross-border data flow governance models: A configurational analysis based on cross-national comparisons. E-Government, Advance online publication.

The typological differentiation criteria stipulate: the Framework-based Facilitation Approach primarily adopts mechanisms such as business Accountability or Ex-post Accountability, with explicit exclusion of Ex-ante Approval, Adequacy Assessment or Jurisdictional Restriction Rules. The Prudent and Flexible Approach is characterized by the use of any combination of Adequacy Assessment, Restricted/Exempt List, Binding Corporate Rules (BCRs), and Contractual Clauses, with exclusion of Ex-ante Approval or Jurisdictional Restriction Rules. The Restrictive Approach, by contrast, primarily relies on Ex-ante Approval mechanisms or Jurisdictional Restriction Rules.

Table 1 outlines the predominant policy instruments commonly associated with each paradigm. Notably, Data Subject's Right to Informed Consent is widely adopted across all three paradigms. Additionally, in the Restrictive Approach, Adequacy Assessment may also be employed as supplementary measures.

Content \ Paradigm	Framework-based Facilitation Approach	Prudent and Flexible Approach	Restrictive Approach
Policy Mechanism	Business Responsibility	Adequacy Assessment	Adequacy Assessment
	Ex-post Accountability		
Policy Instrument		Restricted/Exempt List	Ex-ante Approval
		Binding Corporate Rules (BCRs)	Jurisdictional Restriction Rules
		Contractual Clauses	
	Data Subject's Right to Informed Consent	Data Subject's Right to Informed Consent	Data Subject's Right to Informed Consent

Table 1: Policy Paradigms and Representative Policy Instruments for Cross-Border Data Flows

A. Framework-based Facilitation Approach

1. Overview

Framework-based facilitation policies enable cross-border data flows with minimal restrictions. Their defining feature is the reliance on enterprise self-regulation and ex-post accountability mechanisms inside public sectors. This indicates that enterprises are not obligated to get certain approvals or prerequisites before participating in global cross-border data flow, which significantly diminishes the initial expenses and intricacies associated with data transfer.

However, this paradigm imposes significant demands on the integrity and compliance capabilities of enterprises. In the event of post-transfer misuse or leakage, the data-exporting enterprise will incur severe ex-post sanctions, including substantial fines and legal action. The rationale behind the policy here is to compel enterprises to proactively adopt appropriate protective measures during cross-border data flows by reinforcing post-event supervision and accountability, thereby ensuring the security and legality of the data.

2. Representative Policies

Examples include the United States' *Federal Trade Commission Act* and *California Consumer Privacy Act*, China's *Cybersecurity Law of the People's Republic of China*, Canada Alberta's *Personal Information Protection Act*, Mexico's *Federal Personal Data Protection Law*, and Australia's *Federal Privacy Law*.

In addition, many policy documents issued by international organizations and regional trade agreements tend to follow the Framework-based Facilitation Approach. Notable examples include the United Nations' Global Digital Compact, the OECD Guidelines on Privacy and Transborder Flows of Personal Data, the Regional Comprehensive Economic Partnership (RCEP), and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP).

3. Policy Rationale

The core rationale of the Framework-based Facilitation Approach is to minimize pre-clearance requirement and administrative barriers for cross-border data flows, thereby mitigating the economic costs and compliance burdens faced by enterprises. This regulatory framework seeks to optimize the global allocation efficiency of data resources. By facilitating more adaptable and effective cross-border business collaboration, it helps optimize digital value chains, improve the mobility and accessibility of data as a production factor, and better address the requirements of a swiftly evolving digital economy—ultimately fostering industrial innovation and bolstering market competitiveness.

The implementation of the Framework-based Facilitation Approach is primarily motivated by several critical elements. First, it fulfills geopolitical strategic calculus by differentiating between cooperative and adversarial entities to safeguard the economic interests and international reputation of the data-holding country, or by attracting multinational enterprises to establish operations, thereby positioning the country as a regional data hub. Second, it satisfies the rule-of-law expectations of market participants, by placing significant trust in corporate responsibility and building equilibrium between unrestricted data flows and compliance through principles of privacy protection and Ex-post accountability mechanisms. Third, it facilitates the development requirements of emerging technologies—such as cloud computing and artificial intelligence—which rely on a more open environment for cross-border data flows. This policy paradigm leverages a robust data-driven economy and advanced data infrastructure to provide efficient data circulation and effective governance. Lastly, the public expectations for a harmonious balance between privacy and innovation have also contributed to the formulation of regulations that are more adaptable and open in design.

4. Policy Mechanisms and Instruments

(1) Business Accountability

The business accountability prioritizes autonomous determination of the cross-border transfers through compliance management and sector-specific self-regulatory protocols for their operational data and non-personal data. This policy mechanism is designed to ensure unimpeded cross-border data flows. Such an arrangement facilitates the free circulation of general data within specified regions, minimizes excessive governmental intervention, and improves the operational flexibility and efficiency of enterprises to better address their practical business needs.

For instance, the *California Consumer Privacy Act* (USA), South Korea's *Personal Information Protection Law*, Cameroon's *Law No. 2024-017 on the Protection of Personal Data* and Canada's *Personal Information Protection Act* (PIPA) of Alberta establish that, without imposing restrictions on the free flow of cross-border data, the responsibility for data privacy protection is clearly assigned to the enterprises engaged in cross-border data processing activities.

(2) Ex-post Accountability

Ex-post accountability is a unilateral policy mechanism that emphasizes restricting cross-border data flows through intensified post-event supervision and punitive actions. This mechanism typically presupposes "informed consent" as a prerequisite and does not impose additional preconditions for cross-border data transfers, concentrating instead on stringent post-event accountability for data exporters in cases of data misuse abroad. Its scope encompasses all types of data not explicitly regulated by domestic legal frameworks concerning global cross-border data flows.

In general, ex-post accountability requires that legislation grants extraterritorial applicability to pertinent data flow regulations and mandate that data controllers establish comprehensive data security assessment mechanisms. This arrangement can significantly reduce the compliance thresholds for enterprises' cross-border operations and diminish enforcement costs for regulatory bodies, while maintaining the risks associated with cross-border data flow within acceptable limits—provided there is robust capacity for detecting violations and executing accountability measures.

This mechanism is evident in various data policies, primarily targeting violations related to personal data and privacy protection, cybersecurity breaches, and other electronic crimes. Penalties may include fines, injunctions, and criminal sanctions. For example, Mexico's *Federal Personal Data Protection Law* and Australia's *Federal Privacy Law* primarily address personal data and privacy issues, whereas China's *Cybersecurity Law of the People's Republic of China* and Cameroon's *Cybersecurity and Cybercrime Law* focus on cybersecurity, and Pakistan's *Prevention of Electronic Crimes Law* targets electronic crimes.

(3) Data Subject's Right to Informed Consent

The conditions for data subject's right to informed consent are grounded in three jurisdictional pillars. First, the **principle of transparency** mandates that data controllers provide explicit disclosures—such as the purpose of data processing, the identity of the recipient, potential risks, and available remedies—to data subjects before collection, use, or cross-border data transfer, and establish a straightforward consent procedure to guarantee that consent is granted voluntarily and with comprehensive understanding. Second, the **principle of data subject autonomy** underscores that, with proactive information disclosure, data subjects are empowered to make informed and logical decisions based on complete information. Third, the **principle of risk prevention** compels enterprises to consistently optimize their internal compliance management systems to mitigate risks associated with data loss, prompted by the requirement

for data subject authorization. **The regulatory efficacy of these principles is predominantly contingent upon the regulatory authorities' capacity to differentiate between "superficial consent" and "substantive consent."**

For instance, the *California Consumer Privacy Act* in the United States employs an "opt-out" mechanism to construct its consent logic by requiring enterprises to proactively disclose data flows and empower consumers with the right to block commercial data transactions; Canada Alberta's *Personal Information Protection Law* emphasizes a dynamic notification obligation during cross-border transfers, mandating that any change in a service provider's geographic location triggers a secondary notification; and Mexico's *Federal Law on the Protection of Personal Data Held by Private Parties* differentiates between "data transfer" and "data transmission," setting differentiated consent standards accordingly.

It is important to note that data subject's right to informed consent has now become a widespread requirement in policies governing global cross-border data flows, and is reflected across all three policy paradigms.

B. Prudent and Flexible Approach

1. Overview

Prudent and flexible policies typically center on adequacy assessments as the core mechanism for cross-border data flow. This paradigm incorporates policy instruments including restricted/exempt lists, binding corporate rules, and contractual clauses as integral components.

Prudent and flexible policies require that data exporters must verify—through an adequacy assessment mechanism—that the overseas recipient maintain adequate data protection capabilities prior to initiating cross-border data flows. Where verification fails, the data holder shall implement alternative measures such as signing contractual clauses or establishing legally binding internal enterprise-specific rules to ensure compliant cross-border transfers. This conditional safeguard model typically mandates the data subject's right to informed consent and may incorporate the establishment of regulated lists for data categories and transaction types (e.g., "white lists" or "black lists").

These policies generally impose an increasing number of prerequisites on enterprises engaged in cross-border data flows, thereby subjecting them to heightened legal responsibilities and obligations.

2. Representative Policies

Representative policies include European Union's *General Data Protection Regulation* (GDPR), China's *Provisions on Promoting and Regulating Cross-Border Data Flows*, the United Kingdom's *UK General Data Protection Regulation* (UK GDPR), Singapore's *Personal Data Protection Act* (PDPA), Japan's *Act on the Protection of Personal Information* (APPI), South Korea's *Personal Information Protection Act* (PIPA), India's *Digital Personal Data Protection Act*, South Africa's *Protection of Personal Information Act* (POPIA), and Brazil's *Law of General Data Protection* (LGPD) are among the key legislative frameworks worldwide that regulate personal data protection and cross-border data transfers. Each reflects varying approaches to balancing data privacy, national interests, and the facilitation of international data flows.

At the same time, some policy documents issued by international organizations also follow the Prudent and Flexible Approach. Notable examples include the ASEAN Personal Data Protection Framework (ASEAN PDP Framework), the Council of Europe's Convention

108+, and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

3. Policy Rationale

The justification for prudent and flexible policies is to strike a balance between fostering the digital economy and ensuring data security via moderate regulatory frameworks. This policy paradigm is primarily driven by the market value of data as a crucial production factor, while simultaneously institutionalizing data regulation as a routine policy mechanism to safeguard national security, data sovereignty, public interest, and individual privacy. Consequently, this approach enables enterprises to benefit from cross-border data flow while also accepting associated obligations for risk mitigation.

The implementation of the Prudent and Flexible Approach is typically motivated by several fundamental considerations. First, it seeks to circumvent bloc-based confrontations and align with the requirements of regional integration, creating strategic buffers while promoting economic convergence within the region. Second, it responds to technological uncertainty with a stance of cautious optimism toward emerging technologies. Third, it aims to mitigate security risks while enabling the orderly development of nascent industries. Fourth, it strives to maintain current privacy concerns while reformulating extensive mechanisms of social trust.

4. Policy Mechanisms and Instruments

(1) Adequacy Assessment in Prudent and Flexible Policies

Adequacy assessment, as a regulatory mechanism for cross-border data flows, is primarily manifested in the systematic evaluation and ongoing oversight of the data recipient's protection capabilities. Applicable legislation generally mandates that third countries or international organizations demonstrate, through statutory evaluation procedures, that their data protection standards are substantively equivalent to those of the exporting country. The primary function of this mechanism is to establish a reliable ecosystem for data circulation. Typical requirements include the comprehensiveness of the legal framework, the creation of autonomous regulatory authorities, the efficacy of judicial redress mechanisms, and the adequacy of technical safeguard measures.

The scope and level of detail of adequacy assessments vary across policies. For example, Canada's *Access to Documents Held by Public Institutions and Protection of Personal Information,* India's *Draft Personal Data Protection Bill,* and Turkey's *E-commerce Regulation* primarily require adequacy assessments of the destination country (or region) for data transfer. In contrast, the European Union's GDPR, the United Kingdom's *Data Protection and Digital Information Bill,* Japan's *Supplementary Rules for the Processing of Personal Data Received from the EU and the UK under Adequacy Decisions in the Personal Information Protection Law*, Singapore's *Personal Data Protection Law,* and Brazil's *General Personal Data Protection Law* impose specific ex-post supplementary responsibilities.

(2) Contractual Clauses

Contractual clauses are primarily categorized into standard contractual clauses and enterprise-specific contractual clauses.

Standard contractual clauses are uniformly formulated by national administrative authorities to regulate data transfers to recipients in foreign countries. These clauses are deemed sufficient to protect data transfers, regardless of whether the destination country has obtained an acceptable decision. Although standard contractual clauses are comparatively convenient, their applicable contexts are more rigorously delineated, and the approval and registration process are frequently intricate. For instance, China's Standard Contractual Clauses for personal information cross-border transfers,

the European Union's GDPR—which outlines three scenarios applicable to standard contractual clauses—and South Africa's related policies under its 2013 *Personal Information Protection Law No. 4* serve as examples.

Enterprise-specific contractual clauses are generally utilized when the conditions for employing standard contractual clauses are not satisfied. In such cases, enterprises are required to independently draft and sign contractual clauses in accordance with the applicable laws of both the data exporting and receiving countries, thereby fulfilling the compliance requirements of cross-border data flows. The provisions of these clauses generally include the relevant legal and regulatory requirements, the technical and organizational safeguard measures to be implemented, and explicit terms and conditions regulating the data transfer. For example, Canada's *Federal Law on Personal Information Protection and Electronic Documents* requires enterprises to sign contracts with data recipients to achieve an equivalent level of data protection, while Argentina, through *Regulation No. 60-E/2016*, recognizes the protective standard provided by enterprise-specific contractual clauses.

(3) Restricted/Exempt Lists ("White/Black Lists")

Restricted/exempt lists are designed to regulate or facilitate cross-border data flows by explicitly delineating the categories of data or transactions that are subject to restrictions or exemptions. This policy instrument typically includes explicit provisions regarding the categories of data and transactions involved.

Restricted lists usually enumerate the data types necessitating heightened scrutiny or subject to restrictions during cross-border transfers, such as sensitive personal information and data related to national security. Exempt lists typically identify data types that are not bound by such restrictions. However, data types eligible for the exempt list are often subject to additional preconditions during cross-border data flows, including—but not limited to—the privacy protection level of the recipient's country, limitations on the purpose of data transfer, and the data subject's right of informed consent.

The global practice of implementing restricted/exempt list policies is relatively straightforward. For instance, Australia's 1988 *Federal Privacy Law* stipulates exemptions for certain analogous laws and specific modes of information disclosure; China's *Regulations on Promoting and Regulating Cross-Border Data Flows*, the European Union's GDPR, and the United Kingdom's GDPR all incorporate exempt lists under particular circumstances; and South Korea's *Personal Information Protection Act* (PIPA) along with Argentina's *Personal Data Protection Law* both provide for restrictions and exemptions in the context of cross-border data transfers.

(4) Binding Corporate Rules

Binding Corporate Rules (BCRs) are a fundamental policy instrument regulating cross-border data flow within multinational corporations, exemplified by the stipulations of the European Union's GDPR. BCRs mandate that when a multinational group shares data among its subsidiaries across various countries, it must adhere to uniform legal obligations and remedial measures to guarantee the adequate protection of personal data, regardless of whether the countries involved recognize each other's data protection standards. Although these rules offer some flexibility, in practice they typically require pre-approval from the data protection authorities of the pertinent countries; the approval process is often time-consuming, and the outcomes can be uncertain.

In terms of legal enforceability and substantive content, BCRs require that multinational corporate groups and their subsidiaries comply compulsorily, clearly defining the rights of data subjects with respect to accessing, de-

leting, filing complaints about, and obtaining compensation for personal data. The specific provisions of BCRs generally encompass the organizational structure of the enterprise, information regarding group members, and details of data transfers (including data types, processing purposes, and the countries involved). In addition, BCRs must adhere to principles such as data minimization, purpose limitation, and storage duration, establish channels for data subjects to assert their rights, clarify the joint liability among group members (for example, data holders within the European Union must bear primary responsibility unless they can prove that other group members are not culpable), and implement compliance safeguard measures such as internal audits, training programs, and periodic updates to the regulations.

C. Restrictive Approach

1. Overview

The Restrictive Approach is primarily characterized by implementing full-process governance over data leaving national borders through a stringer ex-ante approval mechanism, or enacting jurisdictional restrictions that completely prohibit data flow to specific jurisdictions. Under this model of cross-border data flows, the process is typically managed through government-conducted adequacy assessments of the data importer's jurisdiction. Where assessment criteria remain unmet, the only viable method is to obtain ex-ante approval from the designated regulatory bodies (which is not necessarily the data department) before the cross-border data flow procedure can proceed. In some special cases, even if the cross-border data flow has passed the adequacy assessment, it must still undergo ex-ante approval by the relevant authority.

2. Representative Policies

Representative policies include the United States' *Final Rule on "Addressing Foreign Adversaries' Acquisition of Sensitive Personal Data of U.S. Citizens"*, *Executive Order 14117*, Greece's *Data Protection Law*, Russia's *List of Foreign Countries Approved for Adequate Protection of Personal Data Subjects*, Kazakhstan's *Law No. 94-V On Personal Data and Its Protection*, and Egypt's *Personal Data Protection Law No. 151 of 2020*, among others.

3. Policy Rationale

The development of restrictive policies is primarily driven by concerns over national security and data sovereignty. The underlying logic is that data is regarded as a critical strategic asset, and it must be prevented from flowing to untrusted jurisdictions through strict ex-ante approval to mitigate national security risks. Moreover, global geopolitical competition has also become an important factor in the design and implementation of cross-border data flow policies. As competition in the digital economy intensifies, some countries, driven by domestic industrial protectionism, implement restrictions on data flow for specific countries or regions. The resulting data barriers between nations (or regions) have become an essential component of the strategic competition over digital sovereignty.

4. Policy Mechanisms and Instruments

(1) Adequacy Assessment in the Restrictive Ap-proach

Within the restrictive approach of cross-border data flows, adequacy assessment still denotes the review of the data protection level of the data importer jurisdictions via statutory frameworks. However, such assessments typically encompass expanded regulatory oversight over non-personal data and incorporate supplementary compliance obligations. For example, Russia's *List of Foreign Countries Approved for Adequate Protection of Personal Data Subjects* mandates that, prior to

cross-border transfer, the recipient country must be confirmed to provide "equivalent protection" for data subject rights, thereby reinforcing public data protection requirements and, based on national security considerations, may restrict or suspend the transfer.

(2) Ex-ante Approval

Ex-ante Approval is a policy instrument implemented by regulatory authorities that mandates prior review before data transfer across borders. Under this mechanism, an application must be filed and the approval should be obtained from the relevant authority prior to cross-border data flows. The primary objective is to verify that data protection standards in the recipient jurisdiction align with the regulatory mandates of the originating country. Unlike adequacy assessments, which focus on comprehensive jurisdictional evaluations, Ex-ante Approval is generally transaction-specific, subject to periodic renewal, and designed to protect national security and data sovereignty.

In global practice, Ex-ante Approval mechanisms are typically applied to important data and core data. For instance, Vietnam's *Decree No. 13/2023/ND-CP on Personal Data Protection* requires a Trade Impact Assessment to be submitted for each instance of cross-border personal data transfer. Pakistan's draft *Information Technology (Personal Data Protection) Act* proposes that a security assessment report and compliance commitments from the receiving party be submitted to regulators before transferring critical personal data abroad.

(3) Jurisdictional Restriction Rules

Jurisdictional restriction rules are principally designed to restrict data access from designated countries or entities. Implemented through standalone legislation or administrative orders, these rules establish clear prohibitions or restrictions on specified transactions. Such rules typically define the scope of "restricted countries (or regions)" and delineate the specific areas subject to these restrictions, with a focus on imposing differentiated limitations based on the country or region.

For example, the United States' *Final Rule on "Addressing Foreign Adversaries' Acquisition of Sensitive Personal Data of U.S. Citizens"* explicitly prohibits the free cross-border data flow to restricted countries and stipulates that any exceptional transaction types must obtain ex-ante approval from the relevant competent authority. Similarly, South Korea's *Law on the Promotion of the Use of Information and Communication Networks*, India's *Digital Personal Information Protection Law*, and Greece's *Data Protection Law* impose restrictions on countries or regions that threaten national security and infringe on citizens' privacy.

D. Trend Analysis

1. Distribution and Trends of Global Cross Border Data Flow Policy Paradigms

The policies covered in this report are classified by three paradigm types. As shown in Figure 1, the Prudent and Flexible Approach is the predominant paradigm, accounting for approximately 59.28% of global cross-border data flow policies, whereas the Framework-based Facilitation Approach accounts for about 26.29%, and the Restrictive Approach constitutes the smallest segment at approximately 14.43%.

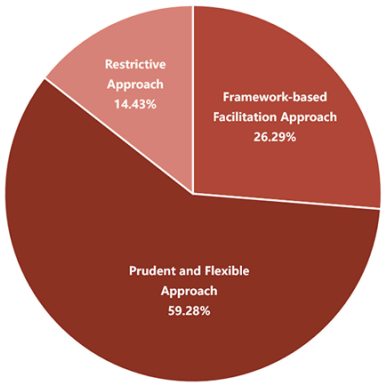


Figure 1: Distribution of Global Cross-Border Data Flow Policy Paradigms

From a temporal perspective (as illustrated in Figure 2), cross-border data flow policies began to concentrate on the Prudent and Flexible Approach after 2005, reaching a peak in 2018 with about 28 policies enacted under this paradigm—largely related to the implementation of the GDPR. The Framework-based Facilitation Approach experienced increases around 2010 and again around 2018, subsequent to which additional Prudent and Flexible policies were frequently issued. However, the average frequency of policy issuance from 2014 to 2024 is significantly lower than that around 2010. Restrictive policies were seldom considered prior to 2016, but progressively emerged as a feasible option around that year.

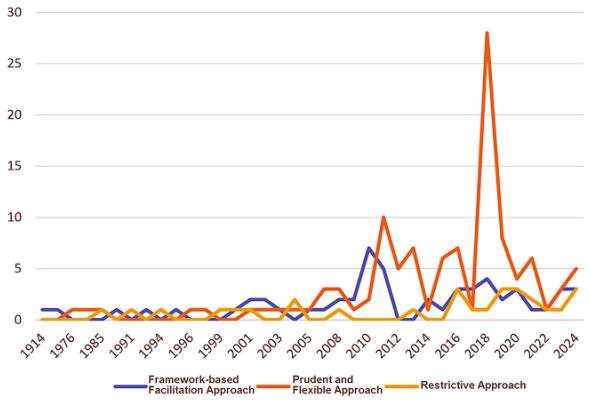


Figure 2: Temporal Trends of Global Cross-Border Data Flow Policy Paradigms

Reviewing the policies enacted over time by various countries, on one hand, a few small and medium-sized countries have frequently implemented a series of policies on cross-border data flows in recent years, but these policies generally adhere to the same paradigm. On the other hand, some economies such as the United States, Russia, and Brazil have, after 2018, generally implemented stricter security-focused regulations. For instance, Russia's *List of Foreign Countries Approved for Adequate Protection of Personal Data Subjects* issued in 2020 and the United States' *Final Rule on "Addressing Foreign Adversaries' Acquisition of Sensitive Personal Data of U.S. Citizens"* issued in 2024 both fall under the Restrictive Approach, while China has moderately eased its ex-ante approval requirements for cross-border data transfers in its recent policy adjustments, embracing the Prudent and Flexible Approach.

2. Distribution and Trends of Policy Mechanisms and Instruments

In terms of the usage of policy instruments in global cross-border data flow policies (as shown in Figure 3), the right of data subjects to be informed is a prevalent condition, featured in 71.79% of the policies. Ex-ante approval and jurisdictional restriction rules are utilized in 8.72% and 6.15% of the policies, respectively, indicating that such restrictive instruments have not been main-

stream in past cross-border data flow policies. Adequacy assessment, enterprise-specific contractual clauses, and standard contractual clauses are the primary instruments adopted when reconciling development and security, used in 45.64%, 38.46%, and 30.26% of the policies respectively. Many policies permit the integrated application of these three instruments, reflecting their high degree of general applicability. Additionally, ex-post accountability and business accountability are widely used, appearing in 35.38% and 28.72% of the policies respectively, with ex-post accountability being marginally more prevalent. In contrast, instruments such as transaction-type restricted/exempt lists and binding corporate rules are implemented in fewer than 5% of policies, indicating relatively lower acceptance of these instruments. In general, security-oriented and restrictive are infrequently utilized, whereas standardized instruments and exemption procedures designed to facilitate data flow or balance security are widely combined and constitute the predominant measures in global cross-border data flow policies.

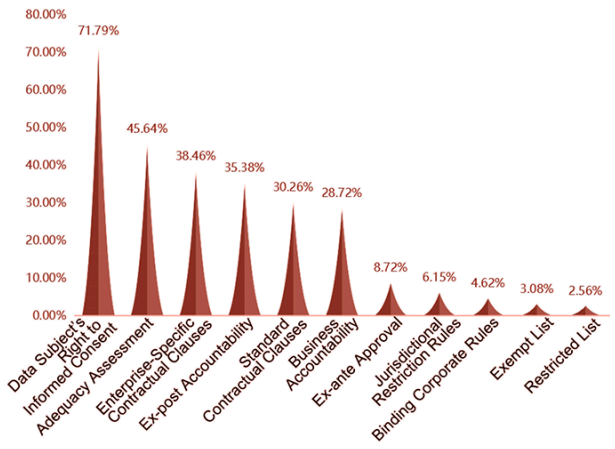


Figure 3: Distribution of Policy Mechanisms and Instruments in Cross-Border Data Flow Policies

Examining the temporal evolution of policy mechanisms and instruments (as shown in Figure 4), the data subject's right to informed consent is frequently referenced in almost every year with significant policy issuance. The prevalence of business accountability, ex-post accountability, and enterprise-specific contractual clauses has been reasonably stable since 2008, indicating their maturity as policy mechanisms and instruments. In 2018, a large number of policies implemented adequacy assessments and standard contractual clauses, presumably related to the introduction of the GDPR. It is particularly noteworthy that both ex-ante approval and jurisdictional restriction rules were rarely acknowledged before 2016; however, after 2016, there was an increase in policies incorporating ex-ante approval, and in 2024, restrictions based on jurisdiction reached a new peak.

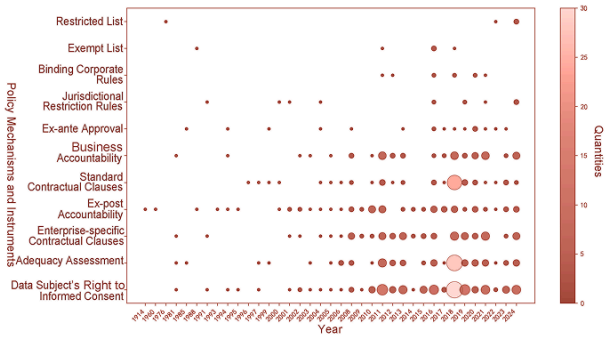


Figure 4: Temporal Trends in the Use of Policy Mechanisms and Instruments in Cross-Border Data Flow Policies

For different types of data and transaction subjects, the corresponding policy paradigm may vary depending on the time of issuance. Overall, various policy mechanisms or instruments are commonly employed in policies addressing distinct domains: business accountability and ex-post accountability are typically aimed at enterprise data and require companies to establish internal evaluation mechanisms; the right of data subjects to be informed is generally a basic condition in personal information protection policies; adequacy assessments are frequently linked to personal data transfers, although the evaluation standards vary significantly across policies; contractual clauses and restricted/exempt lists offer relatively clear and actionable provisions; and jurisdictional restriction rules are gradually being incorporated into the policy instrument toolbox for data regulation.

III.

Policy Comparison in the Data Possession and Utilization Stages

The provisions concerning the data possession and utilization stages can be regarded as interconnected prerequisites for global cross-border data flow policies. Among the policy documents analyzed, approximately 24% include provisions pertaining to the data possession stage, while about 70% address the data utilization stage. This indicates that different policy paradigms do not inherently regulate both stages; when they are mentioned, the provisions tend to exhibit comparable characteristics.

A. Policy Comparison in the Data Possession Stage

1. Framework-based Facilitation Approach

Under the Framework-based Facilitation Approach, the primary characteristic at the data possession stage is that there is the absence of a compulsory necessity for data classification, tiering, or local storage. Such policies may, at most, reference the classification criteria found in the preconditions for cross-border data flows, categorizing data into critical and non-critical types. For critical data—such as data involving national security, sensitive technology, financial information, geographic data, health data, natural resource data, etc.—clear industry norms are established that mandate localization storage and impose restrictions on cross-border data flows. In contrast, for non-critical data, market mechanisms and enterprise self-classification are relied upon, without compulsory localization storage requirements imposed.

2. Prudent and Flexible Approach

In the Prudent and Flexible Approach, policies at the data possession stage typically classify data based on factors such as sensitivity, value, intended use, and potential risks. Simultaneously, they establish requisite criteria for data localization storage and pre-cross-border

data flow processing. For industry-specific data, the specific requirements are determined on a case-by-case basis, typically considering factors such as storage technology, encryption requirements, and localization thresholds.

3. Restrictive Approach

Under the Restrictive Approach, the provisions related to the data possession stage are generally characterized by imprecise definitions of data classification, categorization, and processing methods, accompanied by a higher degree of governmental discretion. This paradigm usually mandates that data must be stored locally; some policies even require that the computational facilities used for data processing be located domestically. In special cases, data processed by an overseas recipient must be returned for local storage.

B. Policy Comparison in the Data Utilization Stage

Currently, the requirements imposed on data users across different cross-border data flow policy paradigms are converging, manifesting primarily in two aspects:

1. Common Usage Principles

All policy paradigms endorse the principles of purpose limitation, data minimization in utilization, and data destruction.

(1) Principle of Purpose Limitation

This principle requires that the collecting and processing of personal data be carried out for specific, explicit, and lawful purposes, and prohibits the utilization of such data for any purposes beyond those originally stated. For example, the European Union's *General Data Protection Regulation* (GDPR) explicitly stipulates that data processing must be grounded in defined, explicit, and lawful purposes, and prohibits additional processing that is incompatible with the original objectives. China's *Personal Information Protection Law* similarly mandates that data processing be directly related to the stated purpose and prohibits the expansion of use through mechanisms such as bundled consent. However, exceptions exist; for instance, the United States' *Foreign Intelligence Surveillance Act* permits intelligence agencies to bypass purpose limitations under the auspices of national security, subject to emergency procedures authorized by court order or Congressional approval.

(2) Principle of Data Minimization in Use

This principle emphasizes that only the minimum amount of data necessary to fulfill the intended objective should be gathered, thereby avoiding excessive collection and processing and mitigating the risk of data leakage and misuse. For example, South Korea's *Personal Information Protection Act* requires enterprises to demonstrate, via a "data necessity assessment," that the data fields collected are directly related to their business functions. India's *Draft Personal Data Protection Bill* categorizes data into "critical data" and "sensitive data," allowing the collection of the latter just with explicit user consent. Significantly, there are practical exceptions; for instance, Mexico's *Federal Personal Data Protection Law* permits the compulsory collection of biometric data for anti-money laundering purposes, constituting an exception to the minimization principle.

(3) Principle of Data Destruction

This principle stresses that once data is obsolete or has reached its storage retention limit, it should be swiftly eradicated to prevent unnecessary long-term storage and mitigate potential risks arising from data breaches. For example, Canada's *Federal Law on Personal Information Protection and Electronic Documents* stipulates that data retention periods must not surpass the duration necessary to fulfill contractual or statutory obligations and mandates that data destruction employ irreversible methods (such as physically shredding storage

media). Singapore's *Personal Data Protection Law* similarly require enterprises to establish data lifecycle management policies and periodically submit destruction records to regulatory authorities.

2. Alignment of Extraterritorial Regulatory Require-ments

Different policy paradigms also advocate that the data-exporting country maintains general rights regarding extraterritorial oversight of data, encompassing rights such as extraterritorial data review and citizen access.

(1) Extraterritorial Data Review

This principle posits that the data-exporting country should maintain the authority to examine data stored or processed abroad, encompassing assessments of legality and compliance, to ensure that such processing adheres violate domestic laws and regulations. For example, the *U.S. CLOUD Act* requires domestic enterprises to provide data stored on overseas servers.

(2) Citizen Access Rights

This right entitles citizens of the data-exporting country to access personal data stored abroad, in accordance with privacy and other statutory rights. This ensures that citizens can access, amend, or delete their data stored in other countries to protect their privacy and information security. For instance, Brazil's *General Data Protection Law* grants citizens a "right to data portability," requiring enterprises to provide a complete copy of data in a structured format (including data stored overseas). Australia's *Federal Privacy Law* similarly allows citizens to request disclosure of cross-border data flow pathways and the identities of data recipients, with enterprises required to respond within 30 days.

(3) General Retention of Rights

This refers to the overarching regulatory authority retained by the data-exporting country over cross-border data flows. It includes the right to require that other countries adhere to its legal standards, maintain uniformity in data processing protocols, and take necessary measures to protect the rights of citizens and organizations.

C. Summary

Regarding the policy instruments for the stages of data possession and utilization (as depicted in Figure 5), there was a notable rise in their application in 2018, coinciding with the implementation of the GDPR. Apart from 2018, following 2008, the principles of data destruction and purpose limitation have been predominantly observed, while the transparency principle was most frequently referenced in 2011, subsequently receiving minimal attention until being reemphasized in 2018. Data localization (storage) requirements have generally been infrequently mentioned.

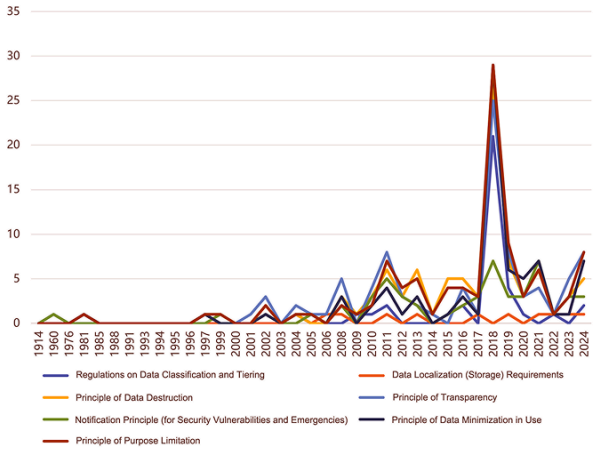


Figure 5: Temporal Trends in the Use of Policy Mechanisms and Instruments for the Data Possession and Utilization Stages

The distinctions in policies between the data possession and utilization stages predominantly emerge in the mandates for data classification, tiering, and localization storage, whereas the commonalities reside in the stipulations regarding personal information processing and the regulatory obligations for data users following cross-border data flows.

1. Personal Information Processing Requirements

National policies consistently underscore the significance of personal information processing, prioritizing the principles of data subject consent, legality, transparency, and security safeguards. Specifically, this includes:

Data Subject Consent: Data processors must secure explicit agreement from data subjects prior to collecting, storing, and utilizing personal information.

Legality and Necessity: Data processing must be conducted for legitimate purposes and adhere to the minimization principle, ensuring that only essential information is collected and processed.

Transparency and Disclosure Obligations: Data processors are required to explicitly convey the purpose, methods, and potential hazards of data processing to data subjects, thereby safeguarding their right to be informed and to retain control over their data.

Security and Protective Measures: Enterprises or institutions must implement rigorous data security measures—including encryption and access controls—to prevent data breaches, misuse, or unauthorized access.

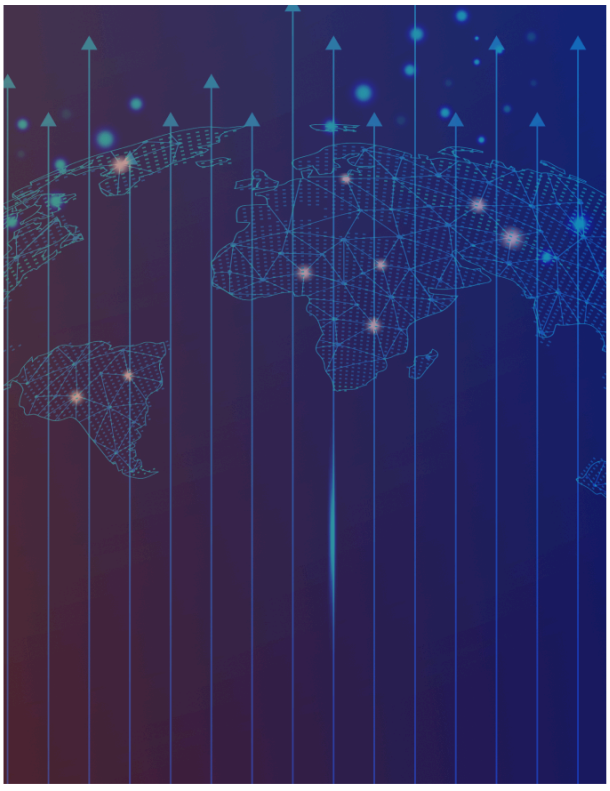
2. Extraterritorial Data Jurisdiction

Extraterritorial data jurisdiction is primarily manifested in the expanded jurisdiction and regulatory mandates that countries impose on data processing after cross-border data flows, with the principal objective of ensuring that data continues to meet domestic security standards post-transfer. Specifically, this encompasses:

Compliance Requirements After Cross-Border Data Flow: This provision mandates that data recipients (such as foreign enterprises or institutions) comply with the data protection standards of the data-exporting country, ensuring the legality and security of data utilization.

Restrictions on Data Utilization: Specific policies explicitly restrict the data processing once it has crossed borders, requiring that data recipients refrain from using the data for unauthorized purposes or transferring it to third parties, thereby ensuring that post-transfer usage aligns with the original consent and protection standards provided by the data subjects.

Overall, policies are progressively differentiating between industry data and critical data. For instance, important data—represented by sectors such as finance, healthcare, geographic information, and government—are typically mandated to be stored locally, whereas policies tend to adopt a more cautious evaluative approach toward broadly defined personal data, public data, and enterprise operational data.



IV.

Policy Comparison in International Cooperation on Cross-Border Data Flows

Countries worldwide have implemented diverse unilateral policies governing cross-border data flows, addressing matters including data ownership, exchange, and usage. The diversity of these measures has contributed to heightened complexity in the global regulatory landscape. In this context, international calls are intensifying for collaborative frameworks and mechanisms designed to reconcile policy conflicts stemming from divergent national policies. The objective is to enhance data openness, data sharing, and data flows. This chapter analyzes the policy texts formed within current plurilateral and bilateral international cooperation mechanisms.

Overall, international coordinated policy on cross-border data flows is predominantly found in Plurilateral Arrangements and Trade Agreements. In plurilateral arrangements, policies are generally executed via through international cooperative instruments involving three or more countries or regions, with the aim of standardizing the cross-border transmission of specific types of data by establishing rules or achieving consensus on fundamental principles[19] . Trade agreements with cross-border data flows are evolving aspect of contemporary trade agreements, primarily designed to regulate the secure data flows in trade among different countries[20] .

A. Policy Paradigms Reflected in Plurilateral Ar-rangements

Plurilateral arrangements for cross-border data flows focus on privacy and data protection, aiming to enhance coordination and interoperability in cross-border data flows among countries (or regions). From the perspective of legal enforceability, these arrangements can be categorized into binding and non-binding frameworks. According to policy paradigms, they generally fall under

19 Casalini F, González J L, Nemoto T. (2021). Mapping commonalities in regulatory approaches to cross-border data transfers. OECD Trade Policy Papers, 248.

20 ibid

the Framework-based Facilitation Approach and the Prudent and Flexible Approach. Accordingly, current plurilateral arrangements on cross-border data flows can be classified into three primary types: **(1) Non-binding, Framework-based Facilitation Arrangements; (2) Non-binding, Prudent and Flexible Arrangements; (3) Binding, Prudent and Flexible Arrangements.**

1. Non-binding, Framework-based Facilitation Ar-rangements

Non-binding arrangements, grounded in soft law principles, encourage all parties to adopt data protection principles and promote the interoperability of privacy protection frameworks, thereby facilitating cross-border data flows. Within plurilateral arrangements represented by the United Nations, the relevant policy documents generally adhere to a Framework-based Facilitation Approach, emphasizing principled and institutional consensus, without imposing binding requirements on specific policy instruments.

For example, the United Nations, through the Global Digital Compact has proposed fundamental objectives including reliable data flow, data protection, and digital empowerment. It advocates for the establishment of multi-tiered, interoperable data governance standards and encourages developing countries to actively participate in the formulation of global rules on data sovereignty and digital security. Meanwhile, the OECD, through the Guidelines on Privacy and Cross-Border Personal Data Flow has established fundamental principles—including purpose limitation, transparency, and security safeguards—while also constructing a three-pronged governance framework supported by trust-building mechanisms, legal and policy coordination, and international law enforcement cooperation, all aimed at promoting free cross-border data flow while effectively safeguarding individual privacy and national interests.

Case Study 1: United Nations (UN) Global Digital Compact

In May 2023, the United Nations issued the Global Digital Compact, which aims to establish common principles, objectives, and pathways for action to build an open, free, secure, and people-centered digital future, thereby promoting inclusive and sustainable development in the global digital domain.

The Compact designates Data Free Flow with Trust as one of its core objectives, emphasizing that free, secure, and efficient cross-border data flow must be achieved on the foundation of protecting individual privacy and data sovereignty. To that end, the Compact proposes the establishment of a multi-layered, interoperable data governance standards framework that enhances compatibility among countries' data governance systems through institutional coordination, standard alignment, and capacity building.

In terms of data governance philosophy, the Compact pays particular attention to ensuring that developing countries have a voice and the right to participate. It advocates for the joint construction and sharing of global data regulations through a multilateral dialogue platform, in order to prevent further widening of the data divide. Simultaneously, the Compact calls for a dynamic balance between data protection and data usage, proposing not only the promotion of innovative data applications but also the safeguarding of data subjects' rights.

2. Non-binding, Prudent and Flexible Arrangements

Regional plurilateral arrangements generally adopt a Prudent and Flexible Approach, incorporating principled policy instrument requirements covering various aspects such as data processing, storage, transfer, and

utilization. Some of these documents serve only as consensus statements and do not impose direct binding legal obligations on the signatory countries.

For instance, in ASEAN, the 2016 ASEAN Personal Data Protection Framework establishes core principles such as informed consent, purpose limitation, and security safeguards. The framework is additionally strengthened by the ASEAN Digital Governance Framework and the ASEAN Digital Economy Blueprint 2025, both of which aim to facilitate cross-border data flows and regional digital economic development.

Similarly, in West Africa, the ECOWAS Supplementary Act on Personal Data Protection (2010) mandates that member states conduct adequacy assessments of recipient countries and establish independent data protection authorities to improve compliance in cross-border data governance.

The Ibero-American States Organization also established the Ibero-American Data Protection Standards (2017), which require adequacy assessment and the use of standard contractual clauses to ensure cross-border data transfers meet unified compliance standards.

Case Study 2: ASEAN Personal Data Protection Framework (ASEAN PDP Framework)

In 2016, ASEAN adopted the ASEAN Personal Data Protection Framework as a plurilateral arrangement aimed at strengthening regional cooperation and standardization in the field of personal data protection, thereby ensuring privacy while promoting efficient cross-border data flow. The framework establishes core principles—including informed consent, purpose limitation, security safeguards, access and correction, and accountability preservation. Although it is non-binding and does not impose legally enforceable obligations, it provides essential policy guidance for domestic legislation in member states and advocates for enhanced governance capacity through cooperative agreements and information sharing.

Building on this framework, ASEAN has subsequently introduced several complementary policies to advance cross-border data flow and digital economic development. The ASEAN Digital Governance Framework, issued in 2018, outlines strategic priorities to guide member states in developing a unified approach to data circulation, privacy protection, and regulatory coordination. Furthermore, the ASEAN Digital Economy Blueprint 2025, adopted in 2021, sets out eight key outcome objectives aimed at constructing a more sustainable and inclusive regional digital economic landscape.

3. Binding, Prudent and Flexible Arrangements

Binding plurilateral arrangements consist of legal agreements, treaties, or enforceable mechanisms that establish data governance frameworks. These frameworks encompass definitive legislate regulations and enforcement mechanisms to ensure privacy protection and data security in cross-border transfers while allowing for regulatory adaptability.

For example, in 2018, the Council of Europe revised and ratified Convention 108+, mandating member states to implement adequacy assessments, contractual clauses, and risk assessment mechanisms to safeguard cross-border data transfers. The agreement also mandates the establishment of autonomous data protection regu-lators to strengthen enforcement and cooperation.

In the Asia-Pacific region, the Asia-Pacific Economic Cooperation (APEC) established the APEC Privacy Framework and the Cross-Border Privacy Rules (CBPR) system, implementing a legally binding privacy certification mechanism. Under the Privacy Recognition

for Processors (PRP) system, APEC also established a tiered certification and regulatory process to enhance compliance and security in cross-border data flows.

Case Study 3: APEC Privacy Framework

In 2005, the Asia-Pacific Economic Cooperation (APEC) issued the Privacy Framework, which established nine core principles—including avoidance of harm, collection limitation, and the reasonable use of personal information—with the aim of harmonizing regional privacy standards and promoting cross-border data flow. This Framework was revised in 2015 to address new challenges brought about by the development of digital technologies.

To implement the Framework, APEC established the Cross-Border Privacy Rules (CBPR) system in 2011, thereby constructing an enforceable privacy certification mechanism supported by government and involving enterprises. Member economies are required to have independent privacy enforcement capabilities and must undergo review through the CPEA mechanism before joining. This mechanism ensures corporate compliance and effective enforcement, laying the foundation for coordinated privacy policies within the region.

Additionally, APEC established a privacy certification system for data processors, known as the Privacy Recognition for Processors. Based on four core principles—accountability, transparency, security, and integrity—and accompanied by 26 requirements and 121 measures, this system employs a three-stage process of self-assessment, third-party evaluation, and continuous monitoring. Through a differentiated assessment mechanism, it enhances the inclusiveness and flexibility of privacy governance.

Plurilateral Arrangement Policy	Legality	Policy Paradigm	Scope of Application	Dispute Resolution Mechanism	Supervision of Compliance and Enforcement	Consequences and Sanctions for Violations	Member Obligations and Rights	Member Autonomy and Flexibility
UN Global Digital Compact	Non-binding	Framework-based Facilitation Approach	Global	No formal mechanism	No supervision mechanism	No sanctions	Establish basic principles for data flows and privacy protection	High flexibility
OECD Guidelines on Privacy and Cross-Border Flows of Personal Data	Non-binding	Framework-based Facilitation Approach	OECD Member States	No formal mechanism	No supervision mechanism	No sanctions	Voluntary compliance to promote privacy protection	High flexibility
ASEAN Personal Data Protection Framework	Non-binding	Prudent and Flexible Approach	Southeast Asia, particularly ASEAN Member States	No formal mechanism	No supervision mechanism	No sanctions	Encourages countries to implement protection principles	High flexibility
ECOWAS Supplementary Act on Personal Data Protection	Non-binding	Prudent and Flexible Approach	West Africa, particularly ECOWAS Member States	Regional coordination mechanism	Supervised by data protection authorities	No sanctions	Reference only, encourages adoption by member states	High flexibility
Ibero-American Data Protection Standards	Non-binding	Prudent and Flexible Approach	Latin America, particularly Ibero-American States	No formal mechanism	No supervision mechanism	No sanctions	Reference only, encourages adoption by member states	High flexibility
Council of Europe Convention 108+	Binding	Prudent and Flexible Approach	Council of Europe Member States, EU Member States, and other signatories	Court trials and international cooperation	Mandatory supervision	Economic or political sanctions	Mandatory compliance with convention requirements	Low flexibility
APEC Privacy Framework	Binding	Prudent and Flexible Approach	Asia-Pacific region, particularly APEC Member States	CPEA (Cross-Border Privacy Enforcement Arrangement)	Third-party certification and supervision	Loss of CBPR certification, trade sanctions	Member states must implement privacy protection requirements	Low flexibility

Table 2: Comparison of Cross-Border Data Flow Policies in Plurilateral Arrangements

B. Policy Paradigms Reflected in Trade Agreements

Trade agreements, historically centered on goods and services, are increasingly addressing cross-border data flows through the incorporation of specific provisions within these agreements as digital trade expands. Because trade agreements are typically founded on mutual trust and are designed to facilitate trade cooperation among parties, trade agreements related to cross-border data flows frequently employ a Framework-based Facilitation Approach. Furthermore, based on the degree of enforceability, they can be categorized as either **(1) Non-binding, Framework-based Facilitation Trade Agreements or (2) Binding, Framework-based Facilitation Trade Agreements.**

1. Non-binding, Framework-based Facilitation Trade Agreements

Non-binding, framework-based facilitation approach trade agreements, while not establishing binding legal obligations, provide facilitative arrangements for data flow through rule coordination, policy dialogue, and cooperation mechanisms. Typically included as e-commerce chapters, these agreements establish principles for data mobility, privacy protection, regulatory cooperation, and national security exceptions, thereby facilitating cross-border data flows without compromising national public policy objectives and security. Their key feature is market openness, allowing member states to balance regulatory flexibility with legal frameworks. Many of these agreements also incorporate regular consultations, supplementary agreements, and joint review mechanisms to adapt to evolving digital trade needs.

For instance:

The Korea-Peru Free Trade Agreement establishes an e-commerce dialogue mechanism, addressing data mobility, localization requirements, and source code protection, which has led to adjustments in bilateral data localization policies.

The Central America-Mexico Free Trade Agreement defines data free flow and prohibits forced data localization, with an e-commerce working group monitoring its implementation. In its 2020 revision, the agreement also incorporated AI-related data governance provisions.

The EU-Japan Economic Partnership Agreement introduces mechanisms for data mobility, personal data protection, and cybersecurity cooperation, ensuring mutual recognition of privacy protection standards. It also includes a joint review mechanism to maintain compliance and security in cross-border data transfers.

Case Study 4: EU-Japan Economic Partnership Agreement (EPA)

In 2019, the European Union and Japan signed and brought into force the Economic Partnership Agreement (EPA), which incorporates provisions on cross-border data flow in both Chapter 8 (E-commerce) and Chapter 16 (Data Protection).

The agreement clearly delineates three core provisions regarding cross-border data flow. **First, the principle of Data Free Flow** (Article 8.71) prohibits the contracting parties from imposing restrictions on cross-border data flow except for non-discriminatory and necessary measures implemented to achieve legitimate public policy objectives. In addition, this provision explicitly stipulates a non-localization requirement, meaning that data localization storage shall not be used as a condition for market access. **Second, the personal data protection provision** (Article 16.4) affirms the equivalence between the EU's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information (APPI), requiring the contracting parties to maintain a "high level of protection" and to establish a joint review mechanism (every two years) to ensure that the standards remain equivalent. **Third, the cyberse-**

curity cooperation mechanism provision (Article 8.76) requires both parties to establish a joint response framework for cybersecurity incidents, which includes a 72-hour cross-border data breach notification mechanism, an information-sharing mechanism for attacks on critical infrastructure, and a mutual recognition procedure for cybersecurity standards.

2. Binding, Framework-based Facilitation Trade Agreements

Binding trade agreements establish legally enforceable rules for data flows and include monitoring and enforcement mechanisms to ensure compliance among member states.

For example:

The Regional Comprehensive Economic Partnership (RCEP) enshrines principles of free cross-border data flow within its e-commerce chapter, aiming to reduce non-tariff barriers and enhance data protection standards. The agreement also introduces a dispute resolution system to address cross-border data governance issues.

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) sets strict regulations on personal data protection, data mobility, and data localization, while allowing for policy exceptions to safeguard public interests.

The Digital Economy Partnership Agreement (DEPA) advances digital trade governance by promoting international standards for privacy protection, enabling free data flows, and discouraging forced data localization. It also advocates for mutual recognition of regulatory frameworks and trusted certification mechanisms, fostering greater digital economy collaboration.

Case Study 5: Digital Economy Partnership Agreement (DEPA)

The Digital Economy Partnership Agreement (DEPA) is the world's first plurilateral arrangement dedicated to the digital economy and digital trade. It was signed by Singapore, New Zealand, and Chile in June 2020 and entered into force on January 7, 2021. China applied for membership in 2021 and commenced formal negotiations in 2022.

With regard to cross-border data flow, DEPA establishes three key policy arrangements: First, personal data protection requires member states to establish legal frameworks that comply with international standards and to promote the mutual recognition of regulatory and certification mechanisms. Second, data free flow is encouraged by reducing unnecessary restrictions on cross-border data flow while retaining public policy exception clauses. Third, DEPA opposes the localization of computing facilities by prohibiting mandatory requirements for enterprises to establish data centers domestically, thereby facilitating digital trade.

Trade Agreement Name	Legality	Data Free Flow Requirement	Data Localization Requirement	Data Protection Mechanism	Enforcement & Dispute Resolution Mechanism	Security Measures	Exception Clauses
Korea-Peru Free Trade Agreement	Non-binding	Yes	No	Yes	E-commerce dialogue mechanism	No special emphasis	Yes, based on public policy
Central America-Mexico Free Trade Agreement	Non-binding	Yes	No	Yes	E-commerce working group, amendment protocol	Cybersecurity cooperation mechanism	Yes, based on public policy
EU-Japan Economic Partnership Agreement (EPA)	Non-binding	Yes	No	Yes	Joint review mechanism	Cross-border data breach notification, mutual recognition of cybersecurity standards	Yes, based on public policy
Regional Comprehensive Economic Partnership (RCEP)	Binding	Yes	No	Yes	E-commerce dialogue mechanism, Joint Committee	Security requirements, capacity-building, information-sharing mechanism	Yes, based on public policy
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Binding	Yes	No	Yes	Encourages dispute resolution through dialogue	Non-discriminatory requirements, cybersecurity cooperation	Yes, based on public policy
Digital Economy Partnership Agreement (DEPA)	Binding	Yes	No	Yes	Not specifically mentioned	Regulatory mutual recognition, trust-based data protection certification	Yes, based on public policy

Table 3: Comparison of Cross-Border Data Flow Policies in Trade Agreements

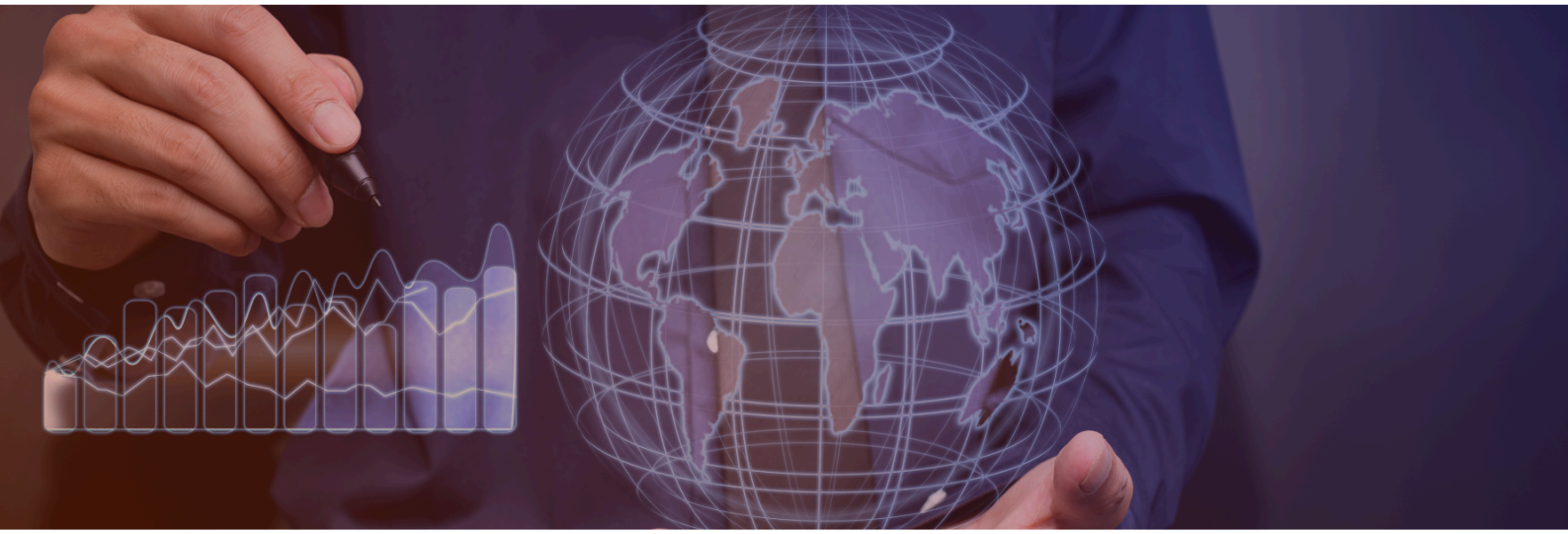
C. Summary

In international cooperation on cross-border data flows, both plurilateral arrangements and trade agreements generally employ the Framework-based Facilitation Approach and the Prudent and Flexible Approach, with a limited number of binding measures. This reflects the demand for policy flexibility and adaptability in the context of digital economic globalization.

In terms of policy instrument design, plurilateral arrangements emphasize the implementation of standard contractual clauses, tiered classification management, exemption lists, informed consent mechanisms, and public policy exception clauses, while underscoring non-localization storage to safeguard data free flow. Conversely, trade agreements focus the facilitation of data free flows and the opposition to localization requirements, but delineate less specific concrete operational instruments.

The legality of policies is primarily determined by the scope and development levels of member states as well as the type of cooperation. Plurilateral arrangements including diverse member states with considerable developmental inequalities typically adopt non-binding mechanisms, prioritizing consensus-building and institutional coordination while preserving space for individual adaptations by member states. Conversely, plurilateral arrangements and multilateral trade agreements among member states with comparable development levels, due to a higher demand for rule uniformity, generally possess stronger legality and enforcement mechanisms.

Overall, current international cooperation is defined by a “soft law-based, flexible governance, and convergence of principles” approach, which, while enhancing institutional compatibility, is progressively establishing a global data governance system that equally emphasizes autonomy and regulation.



V.

Recommendations for Promoting Global Cross-Border Data Flows

A. Reducing Policy Barriers to Facilitate Cross-Bor-der Data Flows

Cross-border data flows are essential for the ongoing advancement of the global digital economy. However, policy divergences among countries and regions have significantly increased compliance costs, operational complexity, and regulatory ambiguity in cross-border data flows. To address this, the international community should promote policy coordination, gradually reduce regulatory barriers, and work toward a more unified global framework for cross-border data flows.

Specifically, countries should establish flexible regulatory frameworks for cross-border data flows, minimizing complex and uncertain approval processes—particularly by reducing pre-approval and administrative licensing requirements. Additionally, multilateral and bilateral cooperation mechanisms should be strengthened to facilitate mutual recognition of adequacy assessments, data protection, and privacy standards, enhancing interoperability between different data governance systems. Furthermore, it is recommended to actively promote policy compatibility and the alignment of standards among major countries and regions, and to establish an inter-system mutual trust mechanism. In addition, it is advisable to set up a dispute resolution mechanism for cross-border data flow that provides institutional pathways—through consultation, mediation, and arbitration—for addressing legal conflicts and standard discrepancies that arise between countries or enterprises during the data flow and compliance process. This mechanism can serve as an extension of existing cooperation platforms, facilitating the efficient resolution of disputes and enhancing the stability and predictability of policy arrangements.

To reinforce policy implementation, national regulatory authorities could also advocate for the establishment of a cross-border data flow regulatory cooperation mechanism, potentially encompassing joint review platforms, the exchange of regulatory liaison officers, and the sharing of compliance case databases, thereby augmenting transparency and coordination during policy execution. At the same time, it is advisable to encourage the formulation of universal guidelines for data classification and tiering, as well as standard contractual clause templates, for multinational enterprises to apply across different legal jurisdictions, thus minimizing redundant compliance costs. Through these measures, more open, transparent, and coordinated environment for cross-border data flow can be created, ultimately unleashing the global potential of digital economic development.

B. Adapting Regulation to Diverse Cross-Border Data Requirements

Given the diversity of data types and transactions, distinct regulatory paradigms should be implemented according to particular circumstances. For instances:

- For high-frequency non-critical data, a Framework-based Facilitation Approach can be adopted to reduce administrative costs and improve data flow efficiency.
- For critical high-value data, a Prudent and Flexible Approach should be used to balance security and privacy protections while ensuring cross-border data mobility is not excessively restricted to maximize its economic value.
- For critical data related to national security or public interests (e.g., military data, biometric data), a Restrictive Approach should be implemented to minimize the risk of data leakage or misuse.

In view of the differences among countries and regions in terms of industrial development, legal systems, and data protection philosophies, it is advisable to implement tailored policy paradigms that reflect each country's specific circumstances to enhance the adaptability and acceptability of regulations governing cross-border data flows. For countries or regions with a relatively sophisticated digital economy and extensive data applications—while also emphasizing data privacy and the protection of individual rights—a Prudent and Flexible Approach is recommended. Under this paradigm, mechanisms such as risk assessment, compliance certification, and in-process review should be flexibly implemented on the basis of ensuring data security and compliance, so as to enable the orderly flow of critical high-value data under controlled risks. For regions with a strong demand for data flow, where the primary objectives are to enhance efficiency and reduce institutional costs and which also possess relatively mature technological governance capabilities, a Framework-based Facilitation Approach is appropriate. By establishing data classification and tiering management systems, streamlining approval procedures, and building registration systems, the cross-border data flow of high-frequency, routine data can be optimized to achieve a balance between efficiency and security. Conversely, for countries or regions where data security risks are pronounced, critical data resources are concentrated, or digital infrastructure is relatively fragile—where risk prevention or data governance capabilities are insufficient—a Restrictive Approach is more suitable. Through the implementation of stricter pre-approval mechanisms for data exports, data localization requirements, and negative list management, national security and public interests can be safeguarded to the greatest extent. These differentiated policy measures not only help to respect the policy autonomy of individual countries, but also provide a practical pathway toward constructing a globally inclusive data governance system characterized by diverse coexistence and mutual trust and recognition.

C. Strengthening Data Subject Rights to Foster Trust in Data Flows

The smooth facilitation of global cross-border data flows depends on robust protections for data subjects' rights. The international community should further define and strengthen essential data subject rights, including:(1) Right to be informed; (2) Right to self-determination; (3) Right to access and erasure; (4) Right to lodge complaints and seek redress.

Countries should establish transparent information disclosure mechanisms for cross-border data processing to ensure that data subjects fully understand the purposes of data processing, transfer destinations, potential risks, and available remedies. Furthermore, international mechanisms for addressing grievances of data subjects should be developed, such as cross-border complaint platforms or arbitration centers, to ensure timely and effective relief in cases of rights violations.

Additionally, multinational enterprises should strengthen internal compliance governance, enhancing transparency and accountability in data management. This will bolster public confidence in cross-border data flows, fostering a favorable cooperation environment for the sustainable development of the global digital economy.

D. Driving Technological Innovation to Strengthen Governance Capabilities

Technological innovation is a key enabler for enhancing regulatory efficiency in cross-border data flow governance. Countries should actively develop and deploy digital platforms for cross-border data flow management, integrating big data analytics, artificial intelligence (AI), and blockchain technology to create more intelligent and automated regulatory systems that improve approval efficiency and transparency.

Specifically, in the process of applying for and approving cross-border data flow, an online approval and registration platform can be established, employing an "automated workflow management system" to handle applications submitted by enterprises. This system automates steps such as document submission, approval process circulation, and result feedback, thereby reducing human interference and enhancing both approval efficiency and traceability. In data compliance reviews, artificial intelligence (AI) and big data analytics can be deployed to automatically classify and identify risks related to data categories, transmission paths, and the nature of recipients as uploaded by enterprises, and to conduct intelligent compliance comparisons using historical cases. Through dynamic supervision and real-time analysis, an intelligent early warning mechanism can be constructed.

In scenarios involving the monitoring of the entire data lifecycle, data identification technologies, blockchain technology, and similar tools can be introduced to build a tamper-proof, fully traceable data flow log that records timestamps and on-chain registration for processes such as data export, transfer, and usage, thereby achieving transparent management across the data lifecycle and enhancing data audit capabilities.

Meanwhile, countries should actively promote the mutual recognition of regulatory technology standards, for instance by jointly formulating interface standards for cross-border data flow, developing a compliance rule modeling language, and creating risk assessment algorithm models. Through the coordinated development and implementation of these standards, the interconnectivity and interoperability of regulatory platforms among different countries and regions can be enhanced, thereby reducing compliance barriers in cross-border data flow.

Appendix: List of Relevant Policies

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
International Organizations and Regional Policies				
1	Global Digital Compact	Framework-based Facilitation Approach	United Nations	Sep-2024
2	Guidelines on the Protection of Privacy and Cross-border Flows of Personal Data	Framework-based Facilitation Approach	OECD	Nov-2013
3	Personal Data Protection Framework	Prudent and Flexible Approach	ASEAN	Nov-2016
4	Personal Data Protection Additional Act	Prudent and Flexible Approach	Economic Community of West African States	Feb-2010
5	Data Protection Standards	Prudent and Flexible Approach	Organization of Ibero-American States	Oct-2017
6	The Council of Europe Convention 108+: Modernised Text of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	Prudent and Flexible Approach	Council of Europe	May-2018
7	Privacy Framework	Prudent and Flexible Approach	APEC	Nov-2015
8	EU-U.S. Data Privacy Framework	Prudent and Flexible Approach	EU-U.S.	Jul-2023
9	Korea-Peru Free Trade Agreement	Framework-based Facilitation Approach	Korea, Peru	Mar-2011
10	Central America-Mexico Free Trade Agreement	Framework-based Facilitation Approach	Central America, Mexico	Nov-2011
11	EU-Japan Economic Partnership Agreement (RCEP)	Framework-based Facilitation Approach	EU, Japan	Feb-2019
12	Regional Comprehensive Economic Partnership Agreement (RCEP)	Framework-based Facilitation Approach	RCEP member countries	Nov-2020
13	Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	Framework-based Facilitation Approach	CPTPP member countries	Dec-2018
14	Digital Economy Partnership Agreement (DEPA)	Framework-based Facilitation Approach	Adoption Time	Jan-2021
Policies of Countries and Territories				
15	Data Protection Law	Prudent and Flexible Approach	Albania	Dec-2024
16	Law No. 18-07	Prudent and Flexible Approach	Albania	Jun-2018
17	Data Protection Law	Prudent and Flexible Approach	Angola	Jun-2011
18	Personal Data Protection Law	Prudent and Flexible Approach	Argentina	Apr-2016
19	Regulation No. 60-E/2016	Prudent and Flexible Approach	Argentina	Jul-2006
20	Federal Privacy Law	Framework-based Facilitation Approach	Australia	Dec-1988
21	Defense Trade Control Law	Prudent and Flexible Approach	Australia	Nov-2012
22	Personal Information Law	Framework-based Facilitation Approach	Azerbaijan	May-2010
23	Law No. 30 of 2018 on Personal Data Protection	Prudent and Flexible Approach	Bahrain	Dec-2018
24	Data Protection Law	Prudent and Flexible Approach	Belgium	Jul-2018
25	Law No. 2009-09 on Personal Identity Information Protection	Prudent and Flexible Approach	Benin	May-2009

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
26	Personal Information Protection Law	Restrictive Approach	Bermuda	Jul-2016
27	Data Protection Law -- Act No. 18 of 2024	Framework-based Facilitation Approach	Bolivia	Feb-2009
28	Article 130 of the Political Constitution of the Plurinational State of Bolivia	Prudent and Flexible Approach	Bosnia and Herzegovina	Jan-2011
29	Data Protection Law	Restrictive Approach	Botswana	Aug-2024
30	Civil Framework for the Internet	Framework-based Facilitation Approach	Brazil	Apr-2014
31	Personal Data Protection Law	Framework-based Facilitation Approach	Brazil	Oct-2011
32	General Personal Data Protection Law	Prudent and Flexible Approach	Brazil	Sep-2020
33	Data Cross-Border Transfer Regulation	Prudent and Flexible Approach	Brazil	Aug-2024
34	Personal Data Protection Law	Prudent and Flexible	Bulgaria	Jan-2002
35	Data Protection Law	Prudent and Flexible Approach	Burkina Faso	Nov-2013
36	Electronic Communications Law	Framework-based Facilitation Approach	Cameroon	Dec-2010
37	Cybersecurity and Cybercrime Law	Framework-based Facilitation Approach	Cameroon	Dec-2010
38	Law No. 2016/007 on Criminal Code	Framework-based Facilitation Approach	Cameroon	Jul-2016
39	Law No. 2010/021 on E-commerce	Framework-based Facilitation Approach	Cameroon	Dec-2010
40	Framework Law No. 2011/012 on Consumer Protection	Framework-based Facilitation Approach	Cameroon	May-2011
41	Decree No. 2019/150 on the Organization and Operation of the National Information and Communication Technology Agency (ANTIC)	Framework-based Facilitation Approach	Cameroon	Mar-2019
42	Regulation No. 03/16CEMAC-UMAC-CMAC-CM on Payment Systems, Instruments, and Events	Framework-based Facilitation Approach	Cameroon	Dec-2016
43	Personal Data Protection Law	Framework-based Facilitation Approach	Cameroon	Dec-2024
44	Personal Information Protection Law	Framework-based Facilitation Approach	Canada	Dec-2003
45	Access to Documents Held by Public Institutions and Protection of Personal Information	Prudent and Flexible Approach	Canada	Jul-1985
46	Federal Law on Personal Information Protection and Electronic Documents	Prudent and Flexible Approach	Canada	Jan-2004
47	Private Sector Personal Data Protection Law	Restrictive Approach	Canada	Dec-1994
48	Private Sector Personal Data Protection Law	Restrictive Approach	Canada	Dec-1994
49	Law No. 132/V/2001	Prudent and Flexible Approach	Cape Verde	Jan-2001
50	Data Protection Law	Prudent and Flexible Approach	Cayman Islands	Sep-2019
51	Articles 15 and 20 of the Constitution of Colombia	Restrictive Approach	Colombia	Jul-1991
52	Protection of Personal Data Processing	Prudent and Flexible Approach	Costa Rica	Mar-2011

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
53	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Croatia	May-2018
54	Law No. 110/2019 on Personal Data Processing	Prudent and Flexible Approach	Czech Republic	Apr-2019
55	Law Establishing Digital Code N°23-010	Framework-based Facilitation Approach	Democratic Republic of the Congo	Mar-2023
56	Data Protection Law	Prudent and Flexible Approach	Denmark	May-2018
57	Article 44 of the Constitution of the Dominican Republic	Framework-based Facilitation Approach	Dominican Republic	Jan-2010
58	Law on the Organization for Personal Data Protection	Prudent and Flexible Approach	Ecuador	May-2021
59	Data Protection Law No. 151 of 2020	Restrictive Approach	Egypt	Jul-2020
60	Law No. L/2016/037/AN on Cybersecurity and Personal Data Protection of the Republic of Guinea	Prudent and Flexible Approach	Equatorial Guinea	Jul-2016
61	Personal Data Protection Law	Prudent and Flexible Approach	Estonia	Dec-2018
62	Constitution of the Federal Democratic Republic of Ethiopia, 1995	Framework-based Facilitation Approach	Ethiopia	Aug-1995
63	Criminal Code of the Federal Democratic Republic of Ethiopia, 2005	Framework-based Facilitation Approach	Ethiopia	May-2005
64	Proclamation No. 958/2016 on Computer Crimes	Framework-based Facilitation Approach	Ethiopia	Jun-1960
65	Proclamation No. 922/2015 on Document Authentication and Registration	Framework-based Facilitation Approach	Ethiopia	Feb-2016
66	Proclamation No. 1072/2018 on Electronic Signatures	Framework-based Facilitation Approach	Ethiopia	Sep-2023
67	Data Protection Law	Prudent and Flexible Approach	Finland	Jan-2019
68	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	France	May-2018
69	Data Protection Law	Prudent and Flexible Approach	Gabon	Oct-2011
70	Federal Data Protection Law	Prudent and Flexible Approach	Germany	May-2018
71	Data Protection Law	Prudent and Flexible Approach	Ghana	May-2012
72	Data Protection Law	Prudent and Flexible Approach	Guernsey	May-2018
73	Cybersecurity and Personal Data Protection Law	Restrictive Approach	Guinea	Jul-2016
74	Transparency and Access to Public Information Law	Framework-based Facilitation Approach	Honduras	Dec-2006
75	Law No. 90/2018 on Data Protection and Personal Data Processing	Prudent and Flexible Approach	Iceland	May-2018
76	Data Protection Law	Prudent and Flexible Approach	Ireland	May-2018
77	Law No. 2024-532 on Tax Exemption for Renewable Energy Equipment	Prudent and Flexible Approach	Ivory Coast	Jun-2024
78	Law No. 2013-546 on Electronic Transactions	Prudent and Flexible Approach	Ivory Coast	Jul-2013
79	Law No. 2013-451 on Combating Cybercrime	Prudent and Flexible Approach	Ivory Coast	Jun-2013

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
80	Law No. 2013-450 on the Protection of Personal Data	Prudent and Flexible Approach	Ivory Coast	Jun-2013
81	Law No. 2012-293 on Telecommunications and Information and Communication Technology	Prudent and Flexible Approach	Ivory Coast	Mar-2012
82	Decree No. 2015-79 on Combating Trafficking in Persons and Similar Acts	Prudent and Flexible Approach	Ivory Coast	Feb-2015
83	Law No. 94-V on Personal Data and its Protection	Restrictive Approach	Kazakhstan	May-2013
84	Data Protection Law	Prudent and Flexible Approach	Kenya	Nov-2019
85	Law No. 06/L-082 on Personal Data Protection	Restrictive Approach	Kosovo	Feb-2019
86	Law No. 20 on Electronic Transactions ("E-commerce Law")	Framework-based Facilitation Approach	Kuwait	Apr-2014
87	Personal Data Law	Prudent and Flexible Approach	Kyrgyzstan	Apr-2008
88	Electronic Data Protection Law	Restrictive Approach	Laos	Jul-2017
89	Personal Data Processing Law	Prudent and Flexible Approach	Latvia	Jul-2018
90	Data Protection Law	Prudent and Flexible Approach	Lesotho	Feb-2012
91	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Lithuania	Jul-2018
92	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Luxembourg	May-2018
93	EU Data Protection Law Implementation Act	Prudent and Flexible Approach	Netherlands	May-2018
94	Data Protection Law	Prudent and Flexible Approach	Pakistan	Aug-2019
95	Prevention of Electronic Crime Law	Framework-based Facilitation Approach	Pakistan	Aug-2016
96	Draft Personal Data Protection Law	Prudent and Flexible Approach	Pakistan	Jun-2023
97	Information Technology (Privacy Protection) Law	Prudent and Flexible Approach	Pakistan	Draft of 2023
98	Data Protection Law	Prudent and Flexible Approach	Panama	May-2021
99	Data Privacy Law	Prudent and Flexible Approach	Philippines	Sep-2012
100	Personal Data Protection Law	Prudent and Flexible Approach	Poland	Aug-1997
101	Data Protection Law	Prudent and Flexible Approach	Qatar	Nov-2016
102	Law No. 190/2018 on Supplementary Measures for the Implementation of the EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Romania	Jul-2018
103	Administrative Offenses Code No. 195-FZ	Framework-based Facilitation Approach	Russia	Dec-2001
104	Personal Data Law	Prudent and Flexible Approach	Russia	Jul-2006
105	List of Foreign Countries Approved for Adequate Protection of Personal Data Subjects	Restrictive Approach	Russia	Oct-2020
106	Law No. 058/2021 on the Protection of Personal Data and Privacy	Restrictive Approach	Rwanda	Oct-2021

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
107	Personal Information Protection Act (PIPA)	Framework-based Facilitation Approach	South Korea	Sep-2011
108	Law on the Promotion of the Use of Information and Communication Networks	Restrictive Approach	South Korea	Jul-2001
109	Guidelines on Personal Information Protection for Overseas Operators	Prudent and Flexible Approach	South Korea	Apr-2024
110	Data Protection Regulation	Prudent and Flexible Approach	United Arab Emirates (UAE)	Feb-2021
111	Data Protection Law No. 5	Prudent and Flexible Approach	United Arab Emirates (UAE)	Jul-2020
112	Cyber and Data Protection Law	Prudent and Flexible Approach	Zimbabwe	Nov-2020
113	Data Protection Law	Prudent and Flexible Approach	Madagascar	Dec-2024
114	Data Protection Law	Prudent and Flexible Approach	Malta	May-2018
115	Data Protection Law	Prudent and Flexible Approach	Mauritius	Jan-2018
116	Federal Trade Commission Act	Framework-based Facilitation Approach	United States (USA)	Sep-1914
117	California Consumer Privacy Act	Framework-based Facilitation Approach	United States (USA)	Jun-2018
118	Executive Order on Preventing the Acquisition of Sensitive Personal Data of U.S. Persons and U.S. Government-Related Data by Countries of Concern	Restrictive Approach	United States (USA)	Feb-2024
119	Final Rule on "Addressing Foreign Adversaries' Acquisition of Sensitive Personal Data of U.S. Citizens"	Restrictive Approach	United States (USA)	Dec-2024
120	CLOUD Act	Restrictive Approach	United States (USA)	Mar-2018
121	Cybersecurity	Framework-based Facilitation Approach	Bangladesh	Feb-2023
122	Personal Data Protection Law	Prudent and Flexible Approach	Peru	Jun-2011
123	Personal Data Protection Law	Prudent and Flexible Approach	Moldova	Jul-2011
124	Data Protection Law No. 1.565	Prudent and Flexible Approach	Monaco	Dec-2024
125	Federal Personal Data Protection Law	Framework-based Facilitation Approach	Mexico	Apr-2010
126	Regulations for the Implementation of the Federal Personal Data Protection Law	Prudent and Flexible Approach	Mexico	Dec-2011
127	Federal Law on the Protection of Personal Data Held by Private Parties	Prudent and Flexible Approach	Mexico	Jul-2010
128	Personal Information Protection Law No. 4	Prudent and Flexible Approach	South Africa	Nov-2013
129	Law No. 787 on Personal Data Protection	Prudent and Flexible Approach	Nicaragua	Mar-2012
130	National Criminal Code	Framework-based Facilitation Approach	Nepal	Aug-2017
131	Personal Privacy Law	Restrictive Approach	Nepal	Sep-2018
132	Personal Privacy Regulation	Restrictive Approach	Nepal	Oct-2020

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
133	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Norway	Jul-2018
134	General Data Protection Regulation	Prudent and Flexible Approach	European Union (EU)	Apr-2016
135	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Portugal	May-2018
136	Supplementary Rules for the Processing of Personal Data Received from the EU and the UK under Adequacy Decisions in the Personal Information Protection Law	Prudent and Flexible Approach	Japan	May-2003
137	Personal Information Protection Law (Law No. 57 of 2003; APPI) - 2015 Amendment	Prudent and Flexible Approach	Japan	Sep-2015
138	Data Protection Law	Prudent and Flexible Approach	Sweden	May-2018
139	Data Protection Law	Prudent and Flexible Approach	Switzerland	May-2018
140	Federal Data Protection Law	Prudent and Flexible Approach	El Salvador	Apr-2021
141	Data Protection Law	Prudent and Flexible Approach	Serbia	Aug-2019
142	Law No. 2008-721 on Electronic Certification	Framework-based Facilitation Approach	Senegal	Jan-2008
143	Decree No. 2008-12 on Personal Data Protection	Prudent and Flexible Approach	Senegal	Jan-2008
144	Law No. 2016-29	Restrictive Approach	Senegal	Nov-2016
145	Law No. 125(I)/2018 on the Protection of Natural Persons with regard to the Processing of Personal Data and the Free Movement of Such Data	Prudent and Flexible Approach	Cyprus	Jul-2018
146	Personal Data Protection Law	Restrictive Approach	Saudi Arabia	Sep-2021
147	Regulation on Cross-border Transfer of Personal Data	Prudent and Flexible Approach	Saudi Arabia	Sep-2024
148	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Slovakia	May-2018
149	EU General Data Protection Regulation (GDPR)	Prudent and Flexible Approach	Slovenia	May-2018
150	Law on Informatization	Framework-based Facilitation Approach	Tajikistan	Aug-2001
151	Information Law	Framework-based Facilitation Approach	Tajikistan	May-2002
152	Personal Data Protection Law	Prudent and Flexible Approach	Tajikistan	Aug-2018
153	Regulation on Certification of Information Security Facilities, Certification of Information Objects, and National Registration Procedures	Restrictive Approach	Tajikistan	Oct-2004
154	List of Nationally Certified Information Security Facilities	Restrictive Approach	Tajikistan	Feb-2008
155	Personal Data Protection Law	Prudent and Flexible Approach	Thailand	May-2019
156	Personal Information Protection Law	Prudent and Flexible Approach	Tanzania	May-2023
157	Data Protection Law	Prudent and Flexible Approach	Trinidad and Tobago	Jun-2011
158	E-commerce Regulation	Prudent and Flexible Approach	Turkey	Jul-2006

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
159	Data Protection Law	Prudent and Flexible Approach	Turkey	Apr-2016
160	Law No. 519-V on Information Regarding Private Life and Its Protection	Framework-based Facilitation Approach	Turkmenistan	Mar-2017
161	Data Protection and Privacy Law	Framework-based Facilitation Approach	Uganda	Mar-2019
162	Personal Data Protection Law No. 2267 VI	Framework-based Facilitation Approach	Ukraine	Jun-2010
163	Decree No. 414/009	Framework-based Facilitation Approach	Uruguay	Aug-2009
164	Decree No. 19.670	Framework-based Facilitation Approach	Uruguay	Oct-2018
165	Decree No. 64/2020	Framework-based Facilitation Approach	Uruguay	Feb-2020
166	Decree No. 20.075	Framework-based Facilitation Approach	Uruguay	Oct-2022
167	Data Protection Law No. 18.331	Prudent and Flexible Approach	Uruguay	Aug-2008
168	Personal Data Law No. ZRU-547	Prudent and Flexible Approach	Uzbekistan	Jul-2019
169	Basic Law on Data Protection and Digital Rights	Prudent and Flexible Approach	Spain	Dec-2018
170	Data Protection Law	Restrictive Approach	Greece	Aug-2019
171	Personal Data Protection Law	Prudent and Flexible Approach	Singapore	Sep-2012
172	Act CXII on the Right of Informational Self-Determination and on Freedom of Information	Prudent and Flexible Approach	Hungary	Jul-2011
173	Personal Data Protection Law	Prudent and Flexible Approach	Armenia	May-2015
174	Privacy Protection Law	Prudent and Flexible Approach	Israel	May-1981
175	Decree No. 101/2018 on the Implementation of GDPR and the Adjustment of Domestic Data Protection Regulations	Prudent and Flexible Approach	Italy	Sep-2018
176	Information Technology Law	Framework-based Facilitation Approach	India	Oct-2000
177	Draft Personal Data Protection Bill	Prudent and Flexible Approach	India	Jul-2018
178	Law No. 27 of 2022 on Personal Data Protection	Prudent and Flexible Approach	Indonesia	Oct-2022
179	Data Protection and Digital Information Bill	Prudent and Flexible Approach	United Kingdom (UK)	May-2018
180	Data Protection Law	Prudent and Flexible Approach	British Virgin Islands	Jul-2021
181	Government Decree No. 13/2023/ND-CP on Personal Data Protection	Restrictive Approach	Vietnam	Apr-2023
182	Data Protection Law No. 3	Prudent and Flexible Approach	Zambia	Mar-2021
183	Law No. 007/PR/2015 on Personal Data Protection	Prudent and Flexible Approach	Chad	Feb-2015
184	Law No. 008/PR/2015 on Electronic Transactions	Prudent and Flexible Approach	Chad	Feb-2015
185	Data Protection Law	Prudent and Flexible Approach	Gibraltar	Jan-2004

Serial Number	Policy Name	Policy Paradigm	Issuing Entity	Adoption Time
186	Law No. 19,628/1999	Restrictive Approach	Chile	Sep-1999
187	Cybersecurity Law of the People's Republic of China	Framework-based Facilitation Approach	China	Nov-2016
188	Law of the People's Republic of China on the Protection of Consumer Rights and Interests	Framework-based Facilitation Approach	China	Oct-1993
189	Regulations on Promoting and Regulating Cross-Border Data Flows	Prudent and Flexible Approach	China	Mar-2024
190	Measures for the Security Assessment of Outbound Data Transfer	Restrictive Approach	China	Jul-2022
191	Regulations for the Administration of Network Data Security	Restrictive Approach	China	Sept-2024
192	Personal Data (Privacy) Ordinance (Chapter 486)	Prudent and Flexible Approach	Hong Kong, China	Dec-1996
193	Personal Data Protection Law	Prudent and Flexible Approach	Macau, China	Aug-2005
194	Personal Information Protection Law	Prudent and Flexible Approach	Taiwan, China	May-2023

Note: The classification of policy paradigms in this report is based on the content mentioned in "II: Basic Paradigms of Global Cross-Border Data Flow Policies."