

全球数据跨境流动政策 比较研究



世界互联网大会数据工作组
2025年04月

世界互联网大会数据工作组

-组 长

梁 昊 世界互联网大会常务副秘书长

-副组长

李晓东 伏羲智库主任、中国科学院计算所研究员（召集人）

孟庆国 清华大学互联网治理研究中心主任、公共管理学院教授

马可明（Chris Brown） 英国标准协会英国-中国商业环境项目主任

-顾 问

薛 澜 清华大学文科资深教授、苏世民书院院长

季卫东 上海交通大学文科资深教授、中国法与社会研究院院长

-工作组成员

白奉军 IBM公共事务高级总监

顾 伟 阿里巴巴集团法律研究中心副主任

吴芳芳 百度高级数据安全工程师

孙 硕 百度资深数据安全专家

颜 拥 国网浙江电力区块链首席科学家

程文博 杭州安恒信息技术股份有限公司信息研发中心资深总监

刘少鹏 杭州安恒信息联盟学协会生态负责人

李 丽 京东法律研究院执行院长

宋雨伦 联通数科高级副总裁、党委委员

潘 登 联通数科大数据创新应用产品部部门经理

张 忻 联想数据安全与隐私保护首席资深法律顾问

胡永启 联想政府事务总监

吕 尧 蚂蚁集团合规和公共事务部总监

Danil Kerimi SealSQ（纳斯达克：LAES）董事会成员

曲广飞 思爱普公司中国数据保护官及大中华区数据保护隐私协调员

张 浩	思爱普公司公共政策研究总监
魏 航	思科公司首席架构师
张 鑫	中国电信数据发展中心副主任（主持工作）
周渭华	中国电信数据发展中心数据合作处处长
郎 平	中国社会科学院世界经济与政治研究所国家安全研究室主任
韩 冰	中国社会科学院世界经济与政治研究所国家安全研究室副主任，副研究员
韦 莎	中国信息通信研究院信息化与工业化融合研究所副总工
张春飞	中国信息通信研究院政经所副所长
陶 涛	中国移动信息技术中心副总经理
林 琳	中国移动研究院用户与市场研究所所长
朱 吉	中信集团信息技术管理部数据管理处处长

—编 辑

伏羲智库：俞逆思，程凯



欢迎微信扫码
关注世界互联网大会



欢迎抖音扫码
关注世界互联网大会

前言

数据跨境流动已经成为全球数字贸易的重要组成部分，为推动经济增长、提升社会福祉提供重要支撑。根据世界贸易组织（WTO）统计，全球数字服务贸易规模2023年已突破4.25万亿美元，过去五年的年均增速接近11%，在全球服务贸易中占比过半¹，其中大多来自数据跨境流动的贡献。另据国际商会（ICC）预计，到2025年底数据跨境流动对全球GDP的贡献将增长至11万亿美元²。

尽管如此，各国在数据跨境流动、数据主权、数据产权等方面的政策取向各异，直接导致全球数据跨境流动规则整体呈现碎片化的趋势。目前的数据跨境流动治理框架变相增加了企业和其他数据交易主体在数据跨境流动中的合规成本、运营复杂性和预期不确定性。

为应对这一挑战，中国国家主席习近平在2024年11月的亚太经合组织第三十一次领导人非正式会议上提出《全球数据跨境流动合作倡议》，呼吁国际社会在充分尊重各国、各地区因具体国情、社情而采取的不同政策法规和实践基础上，认真听取各方数据安全与发展的利益关切，通过协商推动国家间、地区间数据跨境流动规则形成共识。

世界互联网大会国际组织高度重视数据跨境流动议题，于2024年乌镇峰会期间依托数据工作组发布了《促进开放、协作、共赢的数据国际合作》研究报告，提出应基于开放包容原则，尊重数据治理主张的多样性，制定数据国际合作政策框架。

在上述背景下，本报告梳理、比较了截至2024年底发布的全球136个国家（地区）、国际组织及贸易协定中涉及数据跨境流动的共194份政策文本，提炼了数据持有、交换、接收环节的政策规定和做法，基于文本条款所述的机制和工具类型归纳政策范式，提出促进数据跨境流动的对策建议，力求为推动国际社会制订包容、开放的数据国际合作政策框架贡献力量。

报告共包含五部分内容：第一部分总结核心结论；第二部分梳理全球数据跨境流动政策的基本范式，总结其代表性政策、政策出发点、政策机制及工具、政策分布与趋势特点；第三部分比较不同范式在数据跨境前持有及跨境后使用方面的规定；第四部分梳理并比较数据跨境流动国际合作中的政策文件；第五部分提出促进全球数据跨境流动的有关建议。



¹ WTO. Digitally delivered services trade dataset[DB/OL].[2025-4-1].https://www.wto.org/english/res_e/statis_e/gstdh_digital_services_e.htm

² ICC.Whatistheimportanceofglobaldataflowininternationaltrade?[EB/OL].[2025-4-1].<https://icwbo.org/global-insights/digital-economy/data-flows/>

目录

一、 报告核心结论	01
(一) 全球数据跨境流动政策呈现出三种主要范式	01
(二) 全球数据跨境流动政策仍以审慎弹性型为主	01
(三) 部分国家出台的政策在范式上陆续收紧	01
(四) 全球数据跨境流动政策机制及工具包日益丰富	02
(五) 数据跨境流动三种政策范式应用于相应场景	02
(六) 数据跨境流动国际合作多以促进发展为目标	02
二、 全球数据跨境流动政策的基本范式	03
(一) 框架内便利型	05
(二) 审慎弹性型	07
(三) 约束限制型	09
(四) 趋势分析	10
三、 数据持有及使用环节的政策比较	13
(一) 数据持有环节的政策比较	13
(二) 数据使用环节的政策比较	14
(三) 小结	15
四、 数据跨境流动国际合作中的政策比较	17
(一) 不同政策范式在多边安排中的体现	17
(二) 不同政策范式在贸易协定中的体现	20
(三) 小结	23
五、 促进全球数据跨境流动的建议	24
(一) 降低政策壁垒，促进数据跨境流动	24
(二) 明确施策条件，适应不同跨境需求	25
(三) 强化主体权益，培育流动信任环境	25
(四) 推动技术创新，强化治理保障能力	26
附件：相关政策清单	27



01

报告核心结论

(一)

全球数据跨境流动政策呈现出三种主要范式

本报告将全球数据跨境流动政策的基本范式³划分为三类：框架内便利型（Framework-based Facilitation Approach）、审慎弹性型（Prudent and Flexible Approach）与约束限制型（Restrictive Approach）。框架内便利型采用“原则+问责”机制，依托企业负责制和事后问责简化流程。审慎弹性型推行“评估+工具”模式，通过充分性评估匹配合规工具，平衡数据流动与隐私保护。约束限制型实施“审批+限流”策略，以严格事前审批及区域禁令强化全流程管控。

(二)

全球数据跨境流动政策仍以审慎弹性型为主

本报告认为全球数据跨境流动政策以审慎弹性型政策为主流，在所有数据跨境政策中占比约为59.28%，框架内便利型占比约为26.29%，约束限制型政策占比最低，约为14.43%。审慎弹性型政策的发布数量在2018年达到峰值，主要受欧盟《通用数据保护条例》（GDPR）出台的影响。

(三)

部分国家出台的政策在范式上陆续收紧

2018年以后，约束限制型政策逐渐增多，美国、俄罗斯、巴西等经济体普遍强化安全导向的监管措施。例如，俄罗斯2020年发布的《关于批准确保对个人数据主体权利进行充分保护的外国名单》与美国2024年发布的《“应对外国对手获取美国公民敏感个人数据”的最终规则》都属于约束限制性政策。

³ 本文中的“政策范式”指特定政策文本中体现的价值排序、干预逻辑与工具组合模式，反映该政策文本对数据跨境流动问题治理理念的体现，可通过文本条款的强制性、灵活性、目标表述等要素识别。

(四)

全球数据跨境流动政策机制及工具包日益丰富

全球数据跨境流动政策机制⁴及工具⁵的使用特征显示：数据主体知情权覆盖71.79%的政策，发展与安全兼顾的主流政策机制及工具为充分性评估（45.64%）、企业合同条款（38.46%）和标准合同条款（30.26%），多个政策允许三者组合使用。事后问责制（35.38%）与企业负责制（28.72%）也有较广泛的应用。整体而言，注重促进流动的标准化工具占主导，限制性工具占比较低。2016年后事前审批及地域限制规则的使用虽有所增加，但总体占比均在10%以下。

(五)

数据跨境流动三种政策范式应用于相应场景

框架内便利型政策以规则适配性强、合规成本低及促进创新为优势，但存在监管松散、规则碎片化等不足，适用于高频非重要数据⁶流动场景与区域合作。审慎弹性型政策兼顾数据流动与数据保护，规则兼容性较高，但受限于高合规成本与程序复杂性，适用于重要高价值数据⁷跨境场景，依赖数据产业成熟的国家之间的合作。约束限制型政策侧重国家安全、本土数字产业及隐私保障，但可能抑制数字经济发展、抬高企业成本并削弱国际互信，适用于涉及国家安全的重要数据、本土数字产业培育早期。

(六)

数据跨境流动国际合作多以促进发展为目标

国际合作中的数据跨境流动政策呈现以下特征：多边机制倾向于采用框架内便利型与审慎弹性型政策，强调标准合同、分级管理、知情同意等工具组合，并通过非本地化存储推动自由流动；而贸易协定则更突出自由流动原则，弱化流程管控。两类机制均较少采用约束限制型政策范式。

⁴ 本文中的“政策机制”指为实现政策目标而设计的系统性安排。

⁵ 本文中的“政策工具”指直接用于实现政策目标的具体手段或方法。

⁶ 本文中的“高频非重要数据”是指在日常业务活动和社会运行过程中被频繁采集、传输和使用，但其内容对个人隐私、国家安全或商业核心利益影响较小的数据。

⁷ 本文中的“重要高价值数据”是指数据所承载的信息本身具有较高敏感性、在泄露或滥用时可能对企业利益、经济运行、社会稳定、国家安全造成潜在风险，但同时具备显著经济、社会或科研价值，具有广泛应用前景的数据类型。这类数据通常受到较严格的法律法规保护，但若能在合规、可控的前提下进行合理利用，将为创新驱动、产业升级、公共治理等领域带来巨大益处。



02

全球数据跨境流动政策的基本范式

数据跨境流动通常涵盖数据的持有⁸、交换⁹与接收¹⁰三个环节，本报告主要以政策文本中涉及数据交换环节的要求归纳政策的基本范式。

在研究方法上，报告结合联合国贸易和发展委员会（UNCTAD）的全球数据保护和隐私立法（Data Protection and Privacy Legislation Worldwide）数据库¹¹，欧华律师事务所（DLA Piper）整理的全球数据保护法（Data Protection Laws of the World）数据库¹²，对数据库中已收录国家的相关政策文本逐条搜索，排除未提到数据传

输流动（Transfer）的政策，合并部分属同一政策文本的内容。此外，报告还基于政策文本的内容，对主要政策机制或政策工具进行编码分类。

报告最终梳理了全球136个国家和地区、国际组织及贸易协定中，截至2024年底发布的涉及数据跨境流动的共194项政策文本，明确了每项政策文本所使用的政策机制或政策工具，并参考相关学术团体发布的分类依据⁽¹³⁻¹⁸⁾，以政策内容中的**机制和工具类型**为依据，将全球数据跨境流动政策的基本范式划分为三类：（1）框架内便利型（Framework-based Facilitation Approach）、（2）审慎弹性型（Prudent and Flexible Approach）、（3）约束限制型（Restrictive Approach）。

⁸ 本文中的“数据持有”指企业、机构等数据持有方在其管辖范围内对数据的实际存储、管理和控制。

⁹ 本文中的“数据交换”指数据从持有方向接收方传输的过程，包括跨境传输的技术行为（如API接口调用、云端同步、物理介质传输等）。

¹⁰ 本文中的“数据接收”指境外实体（企业、机构或个人）获取并实际控制跨境传输数据的行为。

¹¹ UNCTAD. Data Protection and Privacy Legislation Worldwide[DB/OL].[2025-4-1].<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>

¹² DLA Piper. Data Protection Laws of the World[DB/OL].[2025-4-1].<https://www.dlapiperdataprotection.com>

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

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

¹⁵ World Bank. World development report 2021: Data for better lives[R]. World Bank Publications, 2021.

¹⁶ 封帅,薛世钜.跨境数据流动政策偏好的全球分布：国家维度的治理模式比较研究[J].俄罗斯学刊, 2024, 14(03):8-28.

¹⁷ 李成熙,吴新年.美欧日数据治理政策及实践的比较分析与启示[J].数字图书馆论坛, 2024, 20(07):11-18.

¹⁸ 孔文豪,陈玲.重新理解跨境数据流动治理模式的驱动因素——基于跨国比较的组态分析[J/OL].电子政务, 1-13 (2024-11-13)[2025-01-13].<http://kns.cnki.net/kcms/detail/11.5181.TP.20241112.1234.004.html>.

具体判断标准如下：框架内便利型主要采纳企业负责制或事后问责制，不使用充分性评估、事前审批和受管辖国家（地区）限制规则；审慎弹性型主要采纳充分性评估、“受限/豁免清单”、约束性企业规则和合同条款的任意组合，不使用事前审批和受管辖国家（地区）限制规则；约束限制型主要采纳事前审批或受管辖国家（地区）限制规则。各政策范式采用的主流工具如表1所示。数据主体知情同意在各范式中均会采用，约束限制型政策会采取额外的充分性评估作为补充工具。

政策范式 政策内容	框架内便利型	审慎弹性型	约束限制型
政策机制	企业负责制	充分性评估	充分性评估
	事后问责制		
政策工具		受限/豁免清单	事前审批
		约束性企业规则	受管辖国家（地区） 限制规则
		合同条款	
	数据主体知情同意	数据主体知情同意	数据主体知情同意

表1: 数据跨境流动的政策范式及代表政策工具

(一)

框架内便利型

1. 概述

框架内便利型政策通常允许数据较为自由地跨境流动，典型特征是依靠企业自我监管和公共部门事后问责机制来规范数据跨境流动。这意味着企业在数据跨境传输前无需满足特定的审批或前置条件，显著降低了数据流动的初始成本与复杂性。

不过，这种模式对企业的诚信与合规能力提出了较高要求。一旦数据出境后出现滥用或泄漏情况，数据出口企业将面临严厉的事后追责，包括高额罚款和司法诉讼。其施策逻辑是通过强化事后监管和责任追究，倒逼企业在数据跨境流动过程中主动采取适当的保护措施，确保数据的安全性和合法性。

2. 代表性政策

美国《联邦贸易委员会法案》《加州消费者隐私法案》、中国《中华人民共和国网络安全法》、加拿大《阿尔伯塔省个人信息保护法》、墨西哥《联邦个人数据保护法》、澳大利亚《联邦隐私法》等。

此外，部分国际组织的政策文件和区域的贸易协定多遵循框架内便利型，例如联合国《全球数字契约》、OECD《隐私和跨境个人数据流动保护指南》、《区域全面经济伙伴关系协定》（RCEP）、《全面与进步跨太平洋伙伴关系协定》（CPTPP）等。

3. 政策出发点

框架内便利型政策的核心出发点在于减少数据跨境流动的前置审批程序和行政障碍，减轻企业在数据合规方面的经济成本和管理负担，进而提升数据资源在全球范围内的配置效率。这种政策安排有助于企业更加灵活、高效地开展跨国业务合作，优化数字产业链条，增强数据要素的流通性与可用性，更好地满足数字经济高速发展的需求，推动产业创新与市场竞争力的提升。

框架内便利型政策的出台，一般受以下几方面因素的驱动：一是满足应对地缘政治的竞争需求，通过区分合作与对抗对象，维护数据持有方所在国的经济利益和国际地位，或通过吸引跨国企业布局，成为区域数据枢纽；二是满足市场主体的法治需求，通过充分信任企业主体，依托隐私保护原则与事后问责机制，在自由流动与合规保障之间寻求平衡；三是满足新兴技术的发展需求，云计算、人工智能等服务和技术均依赖更加宽松的数据跨境流动环境，该类政策通过依赖强大的数字经济基础和完善的数据基础设施，支持高效的数据流动与监管；此外，公众对隐私与创新的平衡期望，也使其在政策设计上更具灵活性和开放性。

4.政策机制与工具

(1) 企业负责制

企业负责制强调企业可依靠自身合规管理及行业自律标准，自主决定其运营数据及非个人数据的跨境传输。此举旨在保障数据跨境流动的便利性，有利于促进协定区域内一般数据的自由流通，避免政府过度干预，提升企业经营的灵活性和效率，更有效地满足企业的实际业务需求。

例如，美国《加州消费者隐私法案》、韩国《个人信息保护法》、喀麦隆《关于保护个人数据的第2024-017号法》和加拿大《阿尔伯塔省个人信息保护法》等均提出在不限数据跨境自由流动的前提下，将数据隐私保护的责任主体明确为从事需进行跨境数据流动业务的相关企业。

(2) 事后问责制

事后问责制的核心特点是通过强化事后监管与惩罚机制来规范数据跨境流动行为。此机制通常以“知情同意”为前提，不设跨境数据传输的其他前置审批条件，侧重于对数据持有方在境外数据滥用后的严格追责。

一般而言，事后问责制需通过立法赋予数据流动相关法律的域外效力，并要求数据持有方建立完善的数据安全评估机制。这一安排能够有效降低企业跨境业务的合规门槛和监管部门的执法成本，同时将数据跨境风险控制在可接受范围之内，但前提是必须具备强有力的违规发现能力和问责执行能力。

事后问责制在多个国家的不同数据政策中均有体现，主要针对违反个人信息及数据隐私保护、危害网络安全及其他电子犯罪等行为作出事后惩罚，

处罚内容包括罚款、禁令和刑事处罚。例如墨西哥《联邦个人数据保护法》、澳大利亚《联邦隐私法》、中国《中华人民共和国网络安全法》、喀麦隆《关于喀麦隆网络安全和网络犯罪的第2010/012号法律》、巴基斯坦《预防电子犯罪法》。

(3) 数据主体知情同意

数据主体知情同意包含三类法律原则。一是透明度原则，即要求数据持有方在收集、使用或跨境传输数据之前，清晰地向数据主体披露数据处理目的、接收方身份、潜在风险及权利救济途径等关键事项，并建立明确的同意授权程序，确保数据主体在充分知情基础上自愿作出同意决定。二是主体自主性原则，即通过前置的信息披露机制，提升数据处理的透明度，使数据主体能够基于完整信息做出理性选择。三是风险预防原则，通过主体授权要求，倒逼企业不断优化内部合规管理体系，以防范数据失控风险。**上述法律原则的事实效力高度依赖监管机构对“表面同意”与“实质同意”的鉴别能力。**

例如，美国《加州消费者隐私法案》通过“选择-退出”机制构建同意逻辑，要求企业主动公示数据流向并赋予消费者阻断商业数据交易的权利；加拿大《阿尔伯塔省个人信息保护法》强调跨境传输时的动态告知义务，要求服务提供商地理位置变更必须触发二次通知；墨西哥《联邦个人数据保护法》通过区分“数据转移”与“数据传输”行为，分别设定差异化同意标准。

需要注意的是，在当前全球数据跨境流动政策中，数据知情同意已成为普遍要求，这一点在三种政策范式中均有所体现。

(二)

审慎弹性型

1. 概述

审慎弹性型政策采用“充分性评估”作为数据跨境流动的核心机制，主要工具包括“受限/豁免清单”、约束性企业规则、合同条款等。

审慎弹性型政策要求数据持有方在实施跨境数据流动之前，需通过充分性评估机制确认境外接收方具备足够的数据保护能力。如无法确认，数据持有方可通过签署合同条款或制定具有法律约束力的公司内部规则等替代方案，实现数据的合规跨境传输。此外，这种条件保障型的流动模式通常强调数据主体的知情同意权，并可能结合设立受管制的数据类型和交易类型清单（如“白名单”或“黑名单”）。

审慎弹性型政策通常要求数据跨境流动企业遵守较多的前期要求，因此，受这些政策规制的企业也面临更高的法律责任和义务。

2. 代表性政策

欧盟《通用数据保护条例》（GDPR）、中国《促进和规范数据跨境流动规定》、英国《英国通用数据保护条例》、新加坡《个人数据保护法》、日本《个人信息保护法》、韩国《个人信息保护法》、印度《个人数据保护法案》、南非《个人信息保护法》、巴西《一般数据保护法》等。

部分国际组织的政策文件也采用了审慎弹性型范式，例如东盟的《东盟个人数据保护框架》（ASEAN PDP Framework）、欧洲委员会的《第108号公约+》（Convention 108+）、亚太经合组织（APEC）的《隐私框架》等。

3. 政策出发点

审慎弹性型政策的出发点在于通过适度的监管安排，在促进数字经济发展与数据安全保护间找到平衡点。这种政策范式通常是以发挥数据的市场价值作为核心考量，同时将数据监管落实为一种常态化的政策机制安排，以确保国家安全、数据主权、公共利益、个人隐私不受侵害。因此，这一政策范式使企业既能从数据流动中获益，也要承担相应的风险防范责任。

审慎弹性型政策的出台，一般受以下几方面因素的驱动：一是避免阵营化对抗，支持区域一体化进程，在制造战略缓冲的同时，推动区域经济整合；二是应对技术不确定性，对新兴技术保持谨慎乐观；三是避免安全风险，同时支持新兴产业有序发展；四是维护现有隐私关切，同时重构社会信任机制。

4. 政策机制与工具

(1) 审慎弹性型的充分性评估

充分性评估作为一种跨境数据流动的监管机制，主要表现为对数据接收方保护能力的系统性验证与持续监督。相关立法普遍要求，第三国或国际组织需通过法定评估程序证明其数据保护标准与输出国实质等效。该机制的主要作用体现在构建可信的数据流通生态，典型要件包括法律体系完备性、独立监管机构设置、司法救济渠道有效性以及技术保障措施适配度等。

不同政策充分性评估的对象和标准细化程度有所区别。例如，印度《个人数据保护法案》、土耳其《电子商务条例》主要对数据传输目的国（区域）有充分性评估的要求；欧盟《通用数据保护条

例》、英国《英国通用数据保护条例》通过充分性评估确定第三国、地区或国际组织是否能够提供同等水平的数据保护标准；日本《个人信息保护法》、新加坡《个人数据保护法》、巴西《一般个人数据保护法》则提出事后补充责任要求。

（2）合同条款

合同条款主要包括标准合同条款和企业合同条款两种类型。

标准合同条款由国家行政部门统一制定，用于规范向位于其他国家的持有方传输数据的活动。这些条款在使用时自动被认为能够为数据传输提供足够的保障，即便传输目的地国家没有获得充分性认证。尽管标准合同条款使用较为便捷，但其适配情境较为严格，审批备案流程也较为复杂。中国《个人信息出境标准合同办法》规定了个人信息出境的标准化合同条款；欧盟《通用数据保护条例》提出了三种适用于标准合同条款的数据跨境流动情境；南非则根据其2013年的《个人信息保护法》来制定相关政策。

企业合同条款通常是在不符合标准合同使用情境的情况下，要求企业依照数据出境国及接收方所在国的相关法律规定，自行拟定签署合同条款，以满足数据跨境流动过程中的合规要求。其内容要件通常包括企业必须遵守的相关法律法规、采取的技术和组织保障措施，以及明确数据传输的条款和条件。例如，加拿大《个人信息保护与电子文件法》要求企业与数据接收方签订合同实现相当水平的数据保护；阿根廷则通过《第60-E/2016号规定》认可来自企业合同条款的保护水平。

（3）受限/豁免清单（“白/黑名单”制）

受限/豁免清单旨在通过明确界定数据类型或交易类别的限制或豁免，规范或促进数据跨境流动。这一政策工具通常包含对数据类型和交易类型的明确规定。

受限清单通常列出了在跨境传输时需要特别注意或限制的数据类型，如重要个人信息、国家安全相关数据等。豁免清单通常明确列出不受跨境传输限制的数据类型。不过，满足豁免清单的数据类型通常在跨境流动过程中还会有其他前置条件，包括但不仅限于接收方所在国家的隐私保护水平、数据传输的目的限制、数据主体知情同意等。

受限/豁免清单政策的全球实践相对直接。中国《促进和规范数据跨境流动规定》、欧盟《通用数据保护条例》、英国《英国通用数据保护条例》都包含了特定情境下的豁免清单；韩国《个人信息保护法》、阿根廷《个人数据保护法》对数据跨境传输的限制和豁免均有设定。

（4）约束性企业规则

约束性企业规则（BCRs）是一种适用于跨国公司内部数据跨境流动的重要政策工具，主要以欧盟《通用数据保护条例》的相关要求为典型代表。约束性企业规则通过规定跨国集团在各国子公司之间共享数据时，须遵守统一的法律义务和补救措施，确保个人数据受到充分保护，即便相关国家之间并未相互承认彼此的数据保护水平。尽管这种规则具备一定灵活性，但在实际应用中通常需获得相关国家数据保护机构的前置批准，审批流程较为耗时，且结果有一定不确定性。

从法律约束力和具体内容上看，约束性企业规则要求跨国企业集团及其子公司强制遵守，明确数据主体对个人数据的访问、删除、投诉及赔偿等权利。约束性企业规则的具体内容一般涵盖企业组织架构、集团成员信息、数据传输详情（包括数据类型、处理目的及涉及国家）。此外，约束性企业规则还需遵循数据最小化、目的限制、存储期限等原则，构建数据主体行使权利的通道、明确成员之间的连带责任机制（例如，欧盟境内数据持有方需承担主体责任，除非能证明集团其他成员无过错），以及建立内部审计、培训和规则定期更新等合规保障措施。

(三)

约束限制型

1. 概述

约束限制型政策主要表现为通过严格的事前审批机制强化对数据出境的全流程管控，或制定受管辖国家（地区）限制规则，完全禁止针对某地区的数据流动。在约束限制型的流动模式中，数据的跨境流动通常也依赖于政府部门对数据接收、使用国进行充分性评估，在不满足充分性评估的情况下，唯一可行的方式是由相关公共部门（并不一定是数据部门）进行事前审批，方可进行数据跨境流动程序。在一些特殊的情况下，跨境数据流动即便通过了充分性评估，也必须再次经过相关机构的事前审批。

2. 代表性政策

美国《“应对外国对手获取美国公民敏感个人数据”的最终规则》《14117行政令》、希腊《数据保护法》、俄罗斯《批准确保对个人数据主体权利进行充分保护的外国名单》、哈萨克斯坦《第94-V号法律“关于个人数据及其保护”》、埃及《个人数据保护法2020年第151号》等。

3. 政策出发点

约束限制型政策的制定出发点在于国家安全与数据主权。其隐含的逻辑在于，数据被认为是重要的战略资产，必须通过严格的事前审批防止其外流至不受信任的司法管辖区，以规避国家安全风险。

全球地缘政治竞争是此类政策形成的重要因素之一。随着数字经济的竞争日益加剧，部分国家出于获得竞争优势的需要，针对特定国家或地区实施数据流动限制，形成的国家（地区）间的数据壁垒，成为数字主权博弈的重要组成部分。同时，公众对隐私保护的高度期待和信息主权意识的增强，进一步推动政策的严格化。

4. 政策机制与工具

(1) 约束限制型的充分性评估

在约束限制型数据跨境流动模式下，充分性评估仍然指通过法律或监管机制对数据接收国的数据保护水平进行审查，但其审查范围会扩展至包括非个人数据在内的更广泛的数据类型，并附加额外要求。例如，俄罗斯《批准确保对个人数据主体权利进行充分保护的外国名单》要求跨境传输前需确认接收国能对数据主体权利提供“同等保护”，强化

公共数据保护要求，并基于国家安全等因素可限制或中止传输。

（2）事前审批

事前审批是一种由监管部门主导的数据跨境流动前置审查政策工具，要求企业在进行跨境数据传输前必须向主管部门提交申请并获得批准，以确保接收方的数据保护能力符合本国法律要求。其与充分性评估的主要区别在于事前审批通常针对具体的跨境申请个案，需要定期更新，核心目标是维护国家安全与数据主权。

事前审批政策工具在全球实践中通常会针对重要数据和核心数据设立。例如，越南的《关于个人数据保护的13/2023/ND-CP号政府法令》规定每次个人资料的跨境转移须向当局提交《贸易影响评估》；巴基斯坦的《信息技术（隐私保护）法案》草案提出对关键个人数据在跨境传输前向监管机构提交安全评估报告及接收方合规承诺。

（3）受管辖国家（地区）限制规则

受管辖国家（地区）限制规则主要强调限制特定国家或实体获取数据，通过单独立法或行政命令，明确禁止或限制特定交易。限制规则通常会明确“受限国家（地区）”范围，界定具体的受限领域，主要侧重对国家或地区的区别化限制。

美国《“应对外国对手获取美国公民敏感个人数据”的最终规则》对受限国家有着明确禁止数据自由跨境流动的规定，并在规定中强调例外的交易

类型需通过相关主管部门事前审批批准。韩国《信息与通信网络利用促进法》、印度《数字个人信息保护法》、希腊《数据保护法》则对侵害国家安全和公民隐私的国家或地区进行限制。

（四）趋势分析

1. 数据跨境流动政策范式分布及趋势

报告涉及的相关政策按范式类型区分，结果如图1所示：审慎弹性型政策占主流，在所有数据跨境政策中占比约为59.28%，框架内便利型政策占比约为26.29%，而约束限制型政策占比约为14.43%，为三种政策范式中占比最少的一类。

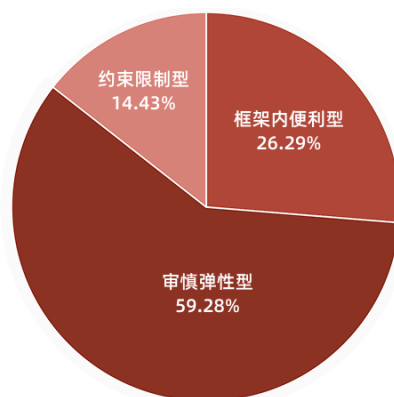


图1：全球数据跨境流动政策范式分布

全球数据跨境流动政策从时间趋势上来看（如图2），2005年之后审慎弹性型政策开始集中出台，其中2018年达到峰值，约有28个属于审慎弹性型的政策发布，基本与GDPR的出台有关。框架内便利型政策分别在2010年和2018年左右有增加，此后常会有更多审慎弹性型政策跟随发布，但2014到2024年间的平均发布频次较2010年前后有明显下降。约束限制型政策在2016年之前较少被考虑，2016年前后逐渐成为一种选择。

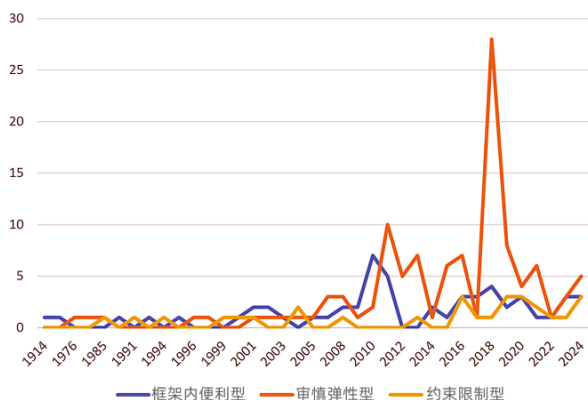


图2：全球数据跨境流动政策范式的时间趋势

从各国随时间的政策发布上来看，少数中小国家在近几年频繁出台一系列针对数据跨境流动的政策，但基本上都属于同一个范式。美国、俄罗斯、巴西等经济体在2018年后普遍加强安全导向的监管措施，其中俄罗斯2020年发布的《关于批准确保对个人数据主体权利进行充分保护的外国名单》与美国2024年发布的《“应对外国对手获取美国公民敏感个人数据”的最终规则》都属于约束限制性政策；中国则在近两年的政策调整中适度放松了数据出境的事前审批要求，出台了审慎弹性型的政策。

2. 政策机制及工具的分布与趋势

全球数据跨境流动政策从政策工具的使用上来看（如图3所示），数据主体知情权作为一个通用的条件，71.79%的政策中均有涉及。事前审批和受管辖国家（地区）限制规则在政策中的采用比例分别为8.72%和6.15%，表明该类限制性政策工具在过去的跨境数据政策中并不属于主流。在兼顾安全与发展的政策目标下，使用充分性评估的政策占比45.64%，采用企业合同条款的占38.46%，而标准合同条款的应用率则为30.26%，很多政策会同时允许上述三种机制和工具生效。此外，事后问责制、企业负责制也在政策中被广泛使用，所涉政策占比分别为35.38%、28.72%。交易类型受限/豁免清单、约束性企业规则被政策采纳的比例则相对较低，均在5%以下。整体而言，注重安全偏向限制的政策工具应用较少，为促进数据流动或兼顾安全设计的标准化工具和免责程序则被广泛地组合使用。

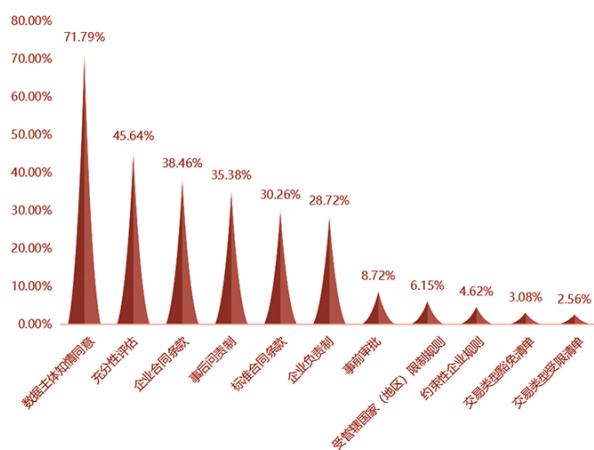


图3：数据跨境流动政策中的政策机制及工具使用分布

从政策机制及工具的时间演变来看（如图4所示），数据主体知情同意在每个政策发布较多的年份均会被大量引用。企业负责制、事后问责制和企业合同条款在2008年之后，各年频次波动较为平缓，是比较成熟的政策机制及工具。2018年，大量政策采用了充分性评估、标准合同条款，应该与GDPR的发布有关。特别需要注意的是，在2016年之前，仅有个别政策会考虑采用事前审批或受管辖国家（地区）限制规则，而在2016年之后，加入事前审批的政策增多，2024年对国家（地区）的限制则到达了新的高峰。

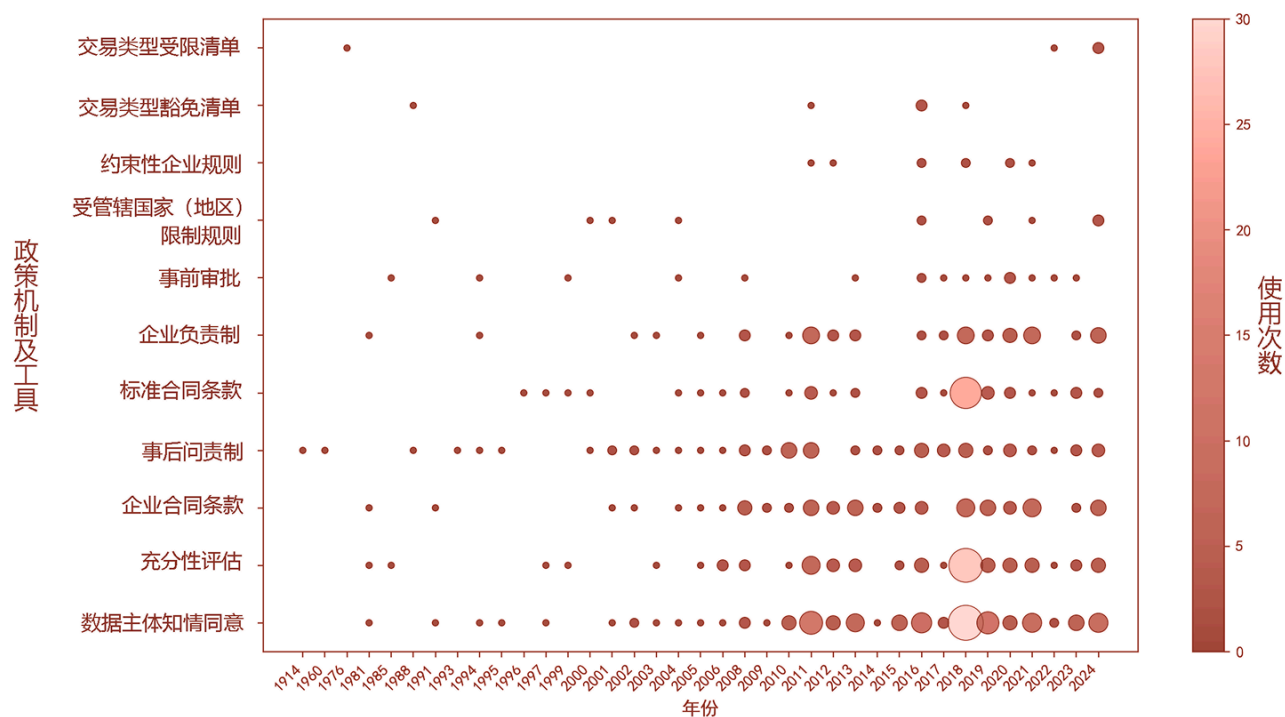


图4: 数据跨境流动政策中各政策机制及工具使用趋势

针对不同的数据类型和交易对象，在不同时间出台的相关政策所对应范式也会有所不同。整体而言，一些政策机制或工具会被针对不同领域的政策采纳：企业负责制和事后问责制通常针对企业数据的跨境流动，并且要求相关企业建立内部评估；数据主体知情同意通常是个人信息保护政策的基本条件；充分性评估也更多针对个人数据传输，但不同政策要求的评估标准存在明显的异质性；合同条款和受限/豁免清单的规定相对清晰，可操作性较强；受管辖国家（地区）限制规则开始逐渐被纳入数据监管的政策工具箱。



03

数据持有及使用环节的政策比较

政策对数据持有及使用环节的相关规定，可视作针对数据跨境流动政策的关联性要求。在所统计的政策文件中，涉及数据持有环节的规定约占24%，涉及数据使用环节的规定则约占70%。不同政策并不一定同时包含数据持有及使用环节的规范，但若设置了相关要求，则其政策条款往往在同一政策范式内呈现出趋同特征。

(一)

数据持有环节的政策比较

1. 框架内便利型政策

框架内便利型范式在数据持有环节的主要特点，是一般不强制要求数据进行分类分级或实施本

地化存储。此类政策最多会参照数据跨境流动前置政策中的分类条件，将数据划分为**重要数据及非重要数据**，对重要数据（如涉及国家安全和重要技术数据、金融数据、地理数据、健康数据、自然资源数据等）作出明确的行业规范，要求进行本地化存储并限制跨境流动。而对于非重要数据，则主要依靠市场机制和企业自主分类处理，不设定强制的本地化存储要求。

2. 审慎弹性型政策

审慎弹性型范式一般在持有环节会根据数据的**重要性、价值、使用目的、潜在风险**进行分类，同时作相应的数据本地化存储及跨境流动前的处理规定。对于具体的行业数据往往视具体情况而定，通常会从存储技术、加密要求、本地化阈值等方面进行判断。

3. 约束限制型政策

约束限制型范式在数据持有环节通常对数据分级分类、处理方式的定义较为模糊，政府的自由裁量权较大。同时，该范式通常要求数据必须本地化存储，一些政策中也会要求必须将数据处理的计算设施设置在境内。在特殊情况下，经过境外接收方处理后的数据也必须返回境内进行存储。

（二）数据使用环节的政策比较

当前，不同数据跨境流动政策范式在针对使用方的要求趋同，主要体现在两个方面：

1. 使用原则共通

不同政策范式均倡导目的限制、数据最小化使用及数据定期销毁原则。

（1）目的限制原则

要求收集和处理个人数据必须是出于特定、明确和合法的目的，且不得将数据用于超出原定目的的任何用途。欧盟《通用数据保护条例》明确规定数据处理必须基于“特定、明确、合法目的”，禁止后续处理与原始目的的不兼容。中国《个人信息保护法》要求数据处理必须与“处理目的直接相关”，且不得通过“捆绑授权”等变相扩大使用范围。也存在一些例外情形，例如美国《外国情报监视法》允许情报机构在国家安全名义下突破目的限制，但需通过法院命令或国会授权的紧急程序。

（2）数据最小化使用原则

强调在收集数据时应仅获取完成任务所必需的最少量数据，避免过度收集与处理，从而降低泄露和滥用的风险。例如，韩国《个人信息保护法》要求企业通过“数据必要性评估”证明收集字段与业务功能的直接关联性。印度《个人数据保护法案》将数据分为“关键数据”与“敏感数据”，仅允许在用户明确同意的前提下收集后者。其中也有一些实践冲突，例如墨西哥《联邦数据保护法》允许企业为反洗钱目的强制收集生物识别数据，形成最小化原则的例外。

（3）数据定期销毁原则

数据定期销毁原则强调一旦数据不再需要或达到存储期限，应被及时销毁，以防止不必要的数据长期存储，降低数据泄露风险。例如，加拿大《个人信息保护与电子文件法》规定数据保留周期不得超过“履行合同或法定义务所需时间”，销毁需采用不可逆技术（如物理粉碎存储介质）；新加坡《个人数据保护条例》要求企业制定数据生命周期管理政策，并定期向监管机构提交销毁记录。

2. 域外监管要求趋同

不同政策范式均主张数据出境国享有对域外数据审查、公民访问和一般性权利保留的管控权。

（1）域外数据审查

主张数据出境国保留对域外数据的审查权，包括但不限于对境外存储或处理数据的合法性、合规性进行审查，确保这些数据的处理不违反本国的法

律法规。例如，美国《云法案》要求境内企业提供海外服务器数据。

(2) 公民访问权

主张数据出境国公民有权依照隐私权和其他法定权利访问在其他国家存储的个人数据。凭此要求，数据出境国得以确保其公民能够随时访问、修改或删除他们在其他国家所存储的数据，以保障个人隐私和信息安全。例如，巴西《通用数据保护法》赋予公民“数据可移植权”，要求企业以结构化格式提供完整数据副本（包括境外存储部分）。澳大利亚《隐私法规定》公民可要求企业披露数据跨境传输路径及接收方身份，企业需在30日内响应。

(3) 一般性权利保留

一般性权利保留指的是数据出境国保留对跨境数据流的一般性监管权，包括要求其他国家遵守本国的法律、确保数据处理标准的一致性以及在必要时采取措施保护公民和组织的权益。

(三) 小结

关于持有及使用环节的政策工具，如图5所示，在2018年达到顶峰，与GDPR的出台有一定关联。此外，2008年之后常以销毁原则和目的限制原则为主流，透明度原则在2011年被最多的政策使用，此后就很少被关注，直到2018年再被重视。数据本地化（存储）要求整体上很少被提及。

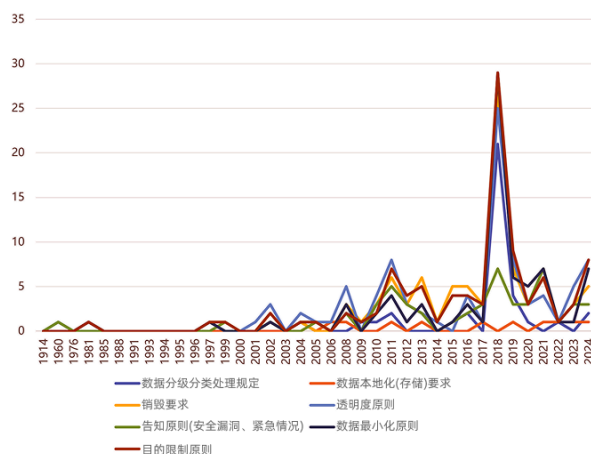


图5：持有及使用环节的政策工具使用趋势

针对数据持有及使用环节的政策差异主要体现在对数据分级分类处理及本地化存储的要求上，共同之处在于个人信息处理要求及数据跨境后的使用方监管要求上。

1. 个人信息处理要求

各国政策在个人信息的处理方面体现出共同的高度重视，主要集中在数据主体的同意原则、合法性、透明性和安全性保障等方面。具体包括：

(1) 数据主体同意

要求数据处理方在收集、存储和使用个人信息前，必须获得数据主体的明确同意。

(2) 合法性与必要性

数据处理必须基于合法目的，且遵循最小化原则，确保数据收集和处理的范围仅限于必要的信息。

（3）透明性与告知义务

数据处理方需向数据主体清楚说明数据的用途、处理方式和潜在风险，保障其知情权和控制权。

（4）安全性与保护措施

要求企业或机构采取严格的数据安全保护措施，包括加密、访问控制等，防止数据泄露、滥用或未经授权的访问。

2. 域外数据管辖权

域外数据管辖权主要体现在各国对其数据跨境后处理的延伸管辖权和监管要求上，政策核心是确保数据在跨境流动后依然符合本国的数据安全标准。具体包括：

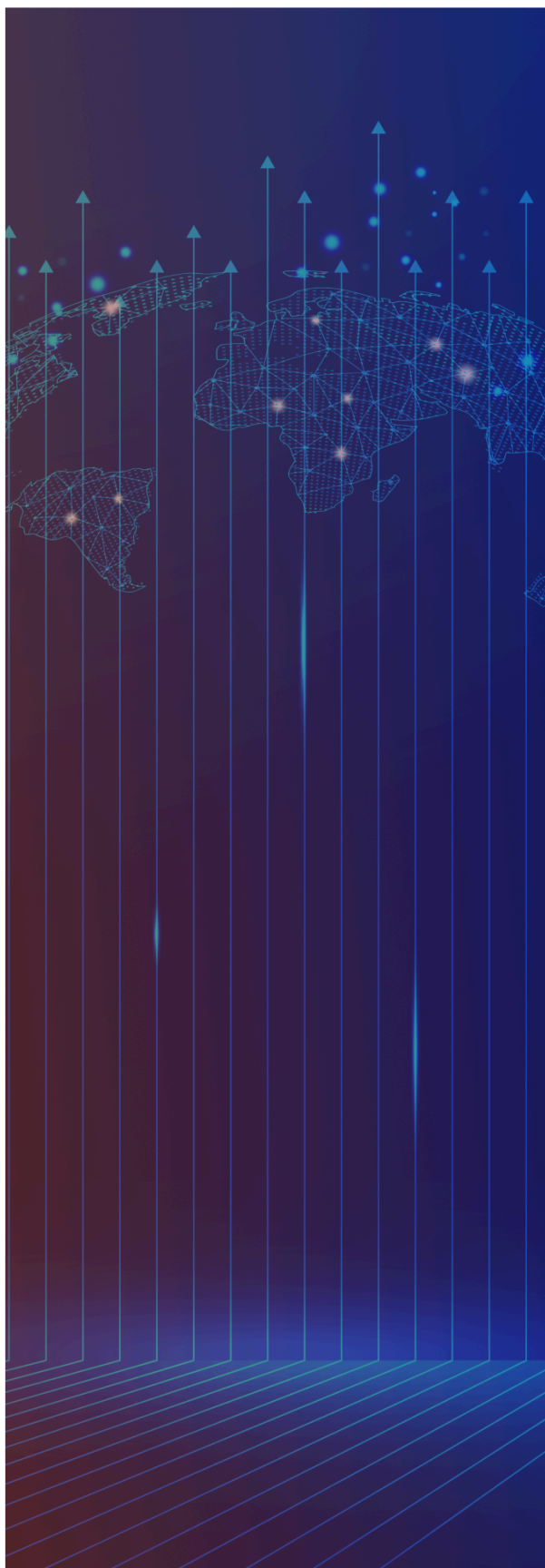
（1）数据跨境后的合规要求

该规则要求数据接收方（如境外企业或机构）必须符合数据输出国的数据保护标准，保证数据使用的合法性和安全性。

（2）数据使用限制

部分政策对数据出境后的处理作出明确限制，要求数据接收方不得将数据用于未经授权的目的或向第三方转移，确保数据跨境后的使用符合原始数据主体的授权和保护标准。

整体而言，各类政策对行业数据、关键数据的区分逐步明确，以金融、医疗、地理信息、政府政务等为代表的重要数据基本均被要求本地存储，相关政策对定义较为广泛的个人数据、公共数据和企业运营数据则存在不同程度的审慎评估态度。





04

数据跨境流动国际合作中的政策比较

各国对数据跨境流动从持有、交换、使用等多个环节存在多样化的单边要求，使得全球数据跨境流动的政策环境变得日益复杂。在此背景下，国际社会呼吁在现存的单边政策机制下，寻求多样性的合作及冲突协调框架，以促进数据开放、共享、流动。为此，本章对当前多、双边国际合作机制中形成的政策文本进行分析。

总的来看，与数据跨境流动国际合作有关的政策文件主要出现在多边安排（Plurilateral Arrangements）与贸易协定（Trade Agreement）中。其中，多边安排中的政策通常是由三个以上的国家或地区共同参与的国际性合作工具，旨在通过制定规则或在基本原则达成共识，规范特定类型数据的跨境传输¹⁹。针对数据跨境流

动的贸易协定是现代贸易协定中的一个新兴组成部分，主要是为了规范数据在不同国家贸易往来中的安全流动²⁰。

（一）

不同政策范式在多边安排中的体现

针对数据跨境流动的多边安排通常以隐私和数据保护为主要议题，其目标是推动国家（地区）间数据跨境流动的协调与互操作。从约束效力上看，可分为强制性安排及非强制性安排，从政策范式上看，主要由框架内便利型和审慎弹性型构成。因而，目前可将多边安排的政策区分为：**（1）非强制性框架内便利型（2）非强制性审慎弹性型（3）强制性审慎弹性型。**

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

²⁰ 同上

1. 非强制性框架内便利型

非强制性安排基于“软法”原则，鼓励各方采纳数据保护原则，并促进隐私保护制度间的互操作性，以实现数据的跨境流动。在以联合国为代表的多边安排中，相关政策文件多遵循框架内便利型范式，侧重原则性和制度性共识，未对具体政策工具作出硬性规定。例如，联合国通过《全球数字契约》提出可信数据流动、数据保护与数字赋权等核心目标，倡导建立多层次、具备互操作性的数据治理标准，并鼓励发展中国家积极参与全球在数据主权与数字安全方面的规则制定；经合组织（OECD）则通过《隐私和跨境个人数据流动保护指南》确立包括目的限定、透明性、安全保障等在内的基本原则，同时构建以互信机制、法律政策协调与跨国执法合作为支撑的三重治理路径，力求在推动数据自由流动的同时，实现对个人隐私与国家利益的有效保护。

案例1：联合国（UN）《全球数字契约》

2023年5月，联合国发布《全球数字契约》（Global Digital Compact），旨在为构建一个开放、自由、安全且以人为本的数字未来确立共同的原则、目标与行动路径，推动全球数字领域的包容性和可持续发展。

契约将可信数据流动（Data Free Flow with Trust）确立为核心目标之一，强调必须在保障个人隐私和数据主权的基础上，实现数据的自由、安全和高效跨境流动。为此，契约提出应建立多层次、可互操作的数据治理标准体系，通过制度协调、标准衔接以及能力建设，增强各国间数据治理制度的兼容性。

在数据治理理念方面，契约特别关注发展中国家的参与权与话语权，主张通过多边对话平台推动全球数据规则的共建共享，避免“数据鸿沟”进一步扩大。同时，契约倡导在数据保护与使用之间建立动态平衡，既提出促进数据创新应用的主张，也强调保障数据主体权益。

2. 非强制性审慎弹性型

在区域性多边安排的政策文件，通常遵循着审慎弹性型的政策范式，对数据处理、存储、流通、使用等多个方面，有着原则性的政策工具要求。其中部分文件仅有共识性意义，对签署国不具有直接的法律约束力。

例如，东盟在2016年通过《东盟个人数据保护框架》（ASEAN PDP Framework），确立了知情同意、目的限制、安全保障等核心原则，并通过东盟数字治理框架和东盟数字经济蓝图2025，进一步推动数据跨境流动与区域数字经济发展。西非国家经济共同体（ECOWAS）于2010年通过《个人数据保护附加法案》，要求成员国对接收国进行充分性评估，并建立独立数据保护机构，以加强跨境数据治理的合规监管。此外，伊比利亚美洲国家组织（Ibero-American States）在2017年制定《伊比利亚美洲国家数据保护标准》，引入充分性评估和标准合同条款，以确保数据跨境传输符合统一的合规标准。

案例2：东盟《个人数据保护框架》 (ASEAN PDP Framework)

2016年，东盟通过《个人数据保护框架》，旨在加强区域内个人数据保护领域的合作与标准化，确保在促进数据高效流动的同时保障隐私安全。该框架确立了知情同意、目的限制、安全保障、访问与更正、责任保全等核心原则，虽无法律约束力，但为成员国国内立法提供了政策指导，并倡导通过协议合作与信息共享提升治理能力。

在此基础上，东盟陆续出台多项配套政策以推动跨境数据流动和数字经济发展。2018年发布的《东盟数字治理框架》提出战略优先事项，引导成员国在数据流通、隐私保护与监管协调方面形成统一路径；2021年通过的《东盟数字经济蓝图2025》则提出八项重点成果目标，构建更具可持续性、包容性的区域数字经济格局。

3. 强制性审慎弹性型

强制性多边安排是指由多个国家或地区通过国际条约、协议或其他具有法律约束力的机制建立的数据治理框架。这些安排通过明确的法律规则和执行机制，规范数据跨境流动中的隐私保护和数据安全，确保参与国在共同遵守规则的基础上实现数据的自由流动。目前，针对数据跨境流动的强制性多边安排通常遵循着审慎弹性型的政策范式。

例如，欧洲委员会在2018年修订并通过《第108号公约+》（Convention 108+），要求成员国实施充分性评估、合同条款和风险评估机制，以确保数据跨境流动的安全性，并设立独立的数据保护

监管机构，强化执法与合作。亚太经合组织（APEC）则通过《隐私框架》及CBPR跨境隐私规则体系，为亚太地区的数据流动建立具有法律约束力的隐私保护认证机制，并在数据处理者隐私识别（PRP）体系下确立分级认证和监管流程，以提升跨境数据流动的合规性和安全性。

案例3：亚太经合组织（APEC）《隐私框架》

2005年，亚太经合组织（APEC）发布《隐私框架》，确立包括避免伤害、收集限制、个人信息合理使用等在内的九项核心原则，旨在协调区域隐私标准、促进跨境数据流动。该框架于2015年修订，以应对数字技术发展带来的新挑战。

为落实该框架，APEC于2011年建立跨境隐私规则体系（CBPR），构建由政府支持、企业参与、可执行的隐私认证机制。成员经济体须具备独立隐私执法能力并通过CPEA机制审核，方可加入。该机制确保企业合规性和执法效力，为区域内隐私政策协调奠定基础。

此外，APEC还设立了面向数据处理者的隐私认证体系（Privacy Recognition for Processors），基于问责、透明、安全、完整性四项核心原则，配套26项要求和121项措施，采用“自评—第三方评估—持续监督”三阶段流程，通过差异化评估机制提升了隐私治理的包容性与灵活性。

多边安排政策	约束性程度	政策范式	适用范围	争端解决机制	遵守与执行的监督机制	违反后果与制裁	成员国的义务与权利	成员国自主性与灵活性
联合国《全球数字契约》	非强制	框架内便利型	全球	无正式机制	无监督机制	无制裁	推动数据流动和隐私保护的基本原则	高灵活性
OECD《隐私和跨境个人数据流动保护指南》	非强制	框架内便利型	OECD成员国	无正式机制	无监督机制	无制裁	自愿遵循，促进隐私保护	高灵活性
东盟《个人数据保护框架》	非强制	审慎弹性型	东南亚地区特别是东盟成员国	无正式机制	无监督机制	无制裁	鼓励各国落实保护原则	高灵活性
西非国家经济共同体《个人数据保护附加法案》	非强制	审慎弹性型	西非地区特别是ECOWAS成员国	区域协调机制	数据保护机构监督	无制裁	仅供参考，鼓励成员国采纳	高灵活性
伊比利亚美洲国家组织《伊比利亚美洲国家数据保护标准》	非强制	审慎弹性型	拉美地区特别是伊比利亚美洲国家	无正式机制	无监督机制	无制裁	仅供参考，鼓励成员国采纳	高灵活性
欧洲委员会《第108号公约+》	强制	审慎弹性型	欧洲委员会成员国、欧盟成员及其他签署国	法院审理和跨国合作	强制性监督	经济或政治制裁	必须遵守公约的要求	低灵活性
APEC《隐私框架》	强制	审慎弹性型	亚太地区尤其是APEC成员	CPEA（跨境隐私执法安排）	第三方认证和监督	失去CBPR认证、贸易制裁	成员国需落实隐私保护要求	低灵活性

表2: 多边安排中的数据跨境流动政策比较

(二)

不同政策范式在贸易协定中的体现

贸易协定虽然主要针对商品和服务贸易，但日益增长的数据交易需求愈发需要通过在贸易协定中专门设置相关条款来进行协调、评估。由于贸易协定往往建立在各方的信任基础上，目的是促进各方贸易合作，因此与数据跨境流动相关的贸易协定通常以框架内便利型范式呈现。同时，可根据贸易协定的约束程度区分为**（1）非约束性框架内便利型贸易协定**；及**（2）约束性框架内便利型贸易协定**。

1. 非约束性框架内便利型贸易协定

非约束性框架内便利型贸易协定虽未形成强制性约束力，但通过规则协调、政策对话和合作机制，为数据流动提供便利性安排。这类协定通常纳入电子商务章节，确立数据自由流动原则，同时兼顾数据隐私保护、监管合作与例外机制，以在促进跨境数据流动的同时维护国家公共政策目标与安全。其核心特征在于以开放市场为导向，允许各国在灵活性与监管要求之间寻求平衡，并通过定期磋商、附加协议和联合审查等机制不断优化规则体系。

例如，韩国 - 秘鲁自由贸易协定通过设立电子商务对话机制，确立了数据自由流动、非本地化要求及源代码保护等核心条款，推动了双边对相关数据本地化要求的调整。中美洲 - 墨西哥自由贸易协定在电子商务章节中确立数据自由流动与禁止本地化义务，同时设立电子商务工作小组推动规则实施，并在2020年的修订中引入人工智能数据治理条款，以适应技术发展趋势。欧盟-日本经济伙伴关系协定则通过数据自由流动、个人信息保护及网络安全合作机制，确保双方数据保护标准的对等性，并设立联合审查机制，以保障跨境数据流动的安全性与合规性。

案例4：欧盟-日本经济伙伴关系协定（EPA）

欧盟与日本于2019年签署生效了《经济伙伴关系协定》（EPA），协议的第8章（电子商务）和第16章（数据保护）均包含数据跨境流动的条款。

协议明确了数据跨境流动的三项核心条款。**一是数据自由流动原则**（第8.71条）。禁止缔约方对跨境数据流动施加限制，除非为实现合法公共政策目标实行的非歧视性、必要性的措施。同时，该条款还明确非本地化要求，即不得以数据本地化存储作为市场准入条件。**二是个人信息保护条款**（第16.4条）。协议确认了欧盟《通用数据保护条例》（GDPR）与日本《个人信息保护法》（APPI）的对等性，要求缔约方维持“高水平保护标准”，并设立联合审查机制（每两年一次）确保标准持续等效。**三是网络安全合作机制条款**（第8.76条）。协议要求双方建立网络安全事件联合响应框架，包括跨境数据泄露72小时通报机制、关键基础设施攻击的信息共享机制、网络安全标准的互认程序。

2.约束性框架内便利型贸易协定

约束性贸易协定制定了对成员国国内法具有约束力的数据流动规则，通常配套有明确的条款执行机制及监督方式，以确保成员国履行其义务。

例如，《区域全面经济伙伴关系协定》（RCEP）通过电子商务章节确立数据跨境自由流动原则，强调减少非关税壁垒，并要求成员国提升数据保护标准，同时建立电子商务对话和争端解决机制，以协调数据治理问题。《全面与进步跨太平洋伙伴关系协定》（CPTPP）则在个人信息保护、跨境数据流动和计算设施本地化要求方面确立严格规则，同时允许基于公共政策目标的例外，以确保成员国在数据治理中的灵活性。《数字经济伙伴关系协定》（DEPA）强调个人信息保护的国际化、数据跨境流动的自由化以及计算设施非本地化的要求，同时鼓励成员国建立监管互认和可信认证机制，以促进数字经济合作。

案例5：《数字经济伙伴关系协定》（DEPA）

《数字经济伙伴关系协定》（DEPA）是全球首个专注于数字经济和数字贸易的多边安排，由新加坡、新西兰和智利于2020年6月签署，并于2021年1月7日生效。中国于2021年申请加入，并于2022年启动正式谈判。

在数据跨境流动方面，DEPA确立了三项关键政策安排：一是个人信息保护，要求成员国建立符合国际标准的法律框架，并推动监管与认证机制的互认；二是数据自由流动，鼓励减少不必要的数据流动限制，同时保留公共政策例外条款；三是反对计算设施本地化，禁止强制要求企业将数据中心设在本地，以促进数字贸易便利化。

贸易协定名称政策	约束性程度	数据自由流动要求	数据本地化要求	数据保护机制	执行与争议解决机制	安全性措施	例外条款
韩国-秘鲁自由贸易协定	非强制	是	否	是	电子商务对话机制	无特别强调	有，基于公共政策
中美洲-墨西哥自由贸易协定	非强制	是	否	是	电子商务工作小组，修订议定书	网络安全合作机制	有，基于公共政策
欧盟-日本经济伙伴关系协定（EPA）	非强制	是	否	是	联合审查机制	跨境数据泄露通报机制，网络安全标准互认	有，基于公共政策
区域全面经济伙伴关系协定（RCEP）	强制	是	否	是	电子商务对话机制，联合委员会	安全性要求，加强能力建设，信息共享机制	有，基于公共政策
跨太平洋伙伴关系协定（CPTPP）	强制	是	否	是	鼓励通过对话解决争端	非歧视性要求，网络安全合作	有，基于公共政策
数字经济伙伴关系协定（DEPA）	强制	是	否	是	无特别提及	监管互认，数据保护可信标志互认	有，基于公共政策

表3: 贸易协定中关于数据跨境流动规则的比较

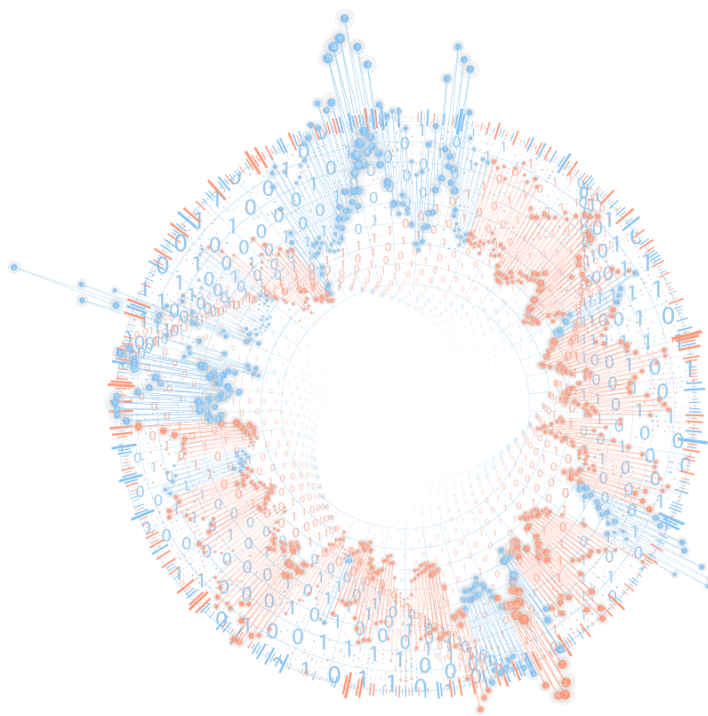
(三) 小结

在数据跨境流动的国际合作中，多边安排与贸易协定普遍采用框架内便利型和审慎弹性型政策范式，较少涉及强约束性措施，体现出对数字经济全球化背景下政策灵活性与适应性的要求。

在工具设计上，多边安排侧重引入标准合同条款、分级分类管理、豁免清单、知情同意机制及公共政策例外条款，并强调非本地化存储以保障数据自由流动；而贸易协定则更聚焦于数据自由流动与反对本地化要求，但较少规定具体操作工具。

政策的约束性强弱主要受成员国范围与发展水平以及合作类型影响。成员国覆盖范围广、发展差异大的多边安排通常采用非强制性机制，强调共识建立与制度协调，保留成员国自主调整空间。反之，成员国发展水平相似的多边安排及多边贸易协定因规则统一需求更高，普遍具备较强法律约束力与执行机制。

总体来看，当前国际合作呈现出“软法为基、弹性治理、原则趋同”的特征，在增强制度兼容性的同时，逐步构建自主和规范并重的全球数据治理体系。





05 促进全球数据跨境流动的建议

(一) 降低政策壁垒，促进数据跨境流动

数据跨境流动是推动全球数字经济可持续发展的重要支撑。然而，不同国家和地区的政策差异直接导致了数据跨境流动过程中合规成本增加、运营复杂度和不确定性提升。建议国际社会积极推进政策协调，逐步降低政策壁垒，形成更加统一的跨境数据流动规则体系。

具体而言，各国应建立灵活的跨境数据流动规则框架，避免复杂及不确定性的审批流程，尤其是要减少政策中的前置性审查和行政许可要求。同时，应鼓励通过多边和双边合作机制，推动充分性审查、数据保护与隐私标准的国际互认，实现不同

数据治理体系间的相互衔接。为此，可积极推动主要国家和地区间的政策兼容与标准对接，构建跨制度的互信机制。此外，建议设立数据跨境流动争端解决机制，为各国间或企业间在数据流动与合规过程中出现的法律冲突、标准分歧等问题提供协商、调解与仲裁的制度性路径。该机制可作为现有合作平台的延伸，推动争端高效解决，增强政策安排的稳定性和预期性。

为强化政策落地，各国监管机构还可推动数据跨境监管协作机制建设，包括建立联合审查平台、互派监管联络官、共享合规案例数据库等，提升政策执行过程中的透明度与协调性。同时，也可鼓励制定通用的数据分类分级指引和标准合同条款模板，供跨国企业不同法域之间复用，降低重复合规成本。通过上述措施，各国将共同打造更加开放、透明、协调的数据跨境流动环境，释放全球数字经济发展潜能。

(二)

明确施策条件，适应不同跨境需求

针对数据及交易类型的多样性，可针对不同场景采用不同范式的数据跨境流动政策。例如，针对高频非重要数据，可以采用框架内便利型政策以降低数据流动的行政成本，促进流动效率；针对重要高价值数据，可以采用审慎弹性型政策，形成对数据安全和隐私保障的同时，确保跨境流动不受过多限制，充分发挥数据的利用价值；针对涉及国家安全或公共利益的重要数据（比如军事数据、生物识别数据等），可以采用约束限制型政策，最大限度地保证数据不被外泄或滥用。

鉴于不同国家和地区在产业发展、法律制度、数据保护理念上的差异，建议根据具体国情采用差异化的政策范式以提升数据跨境流动规则的适应性与可接受度。对于数字经济较为发达、数据应用广泛、同时注重数据隐私和个人权利保护的国家或地区，宜采用审慎弹性型政策范式，在保障数据安全与合规基础上，灵活设置风险评估、合规认证、事中审查等机制，确保重要高价值数据在控制风险的前提下实现有序流动。对于数据流动需求强烈、以提升效率和降低制度成本为优先目标、同时具备较为成熟的技术治理能力的地区，可采用框架内便利型政策范式，通过建立数据分类分级管理体系、简化审批程序、推行备案制等方式，优化高频非重要数据的跨境流动路径，实现高效与安全的平衡。而对于数据安全风险突出、关键数据资源集中或数字基础设施较为脆弱、优先关注风险防控或数据治理能力不足的国家或地区，则更适合采用约束限制型政策范式，通过设置更为严格的数据出境审批机制、数据本地化要求和负面清单管理，最大限度保

障国家安全与公共利益。上述分类施策不仅有助于尊重各国自身的政策选择空间，也为构建全球范围内多元共存、互信互认的数据治理体系提供现实路径。

(三)

强化主体权益，培育流动信任环境

全球数据跨境流动的顺利推进依赖于数据主体权益的有效保护。国际社会应进一步明确和强化数据主体的权利保护要求，包括知情权、自主决定权、访问删除权、投诉救济权等。

建议各国在跨境数据处理过程中建立明确的信息披露机制，确保数据主体能够充分了解数据处理目的、传输目的地、潜在风险及救济途径，保障数据主体的自主性。同时，各国应构建透明、高效的国际数据主体权益救济和申诉机制，设立跨境投诉平台或仲裁中心，确保数据主体在发生数据权益侵害时能够迅速获得有效的救济。此外，还应加强跨国企业内部的合规管理，提升企业数据治理的透明度和责任意识，进一步增强公众对数据跨境流动的信任与接受程度，为全球数字经济可持续发展营造良好的国际合作环境。

(四)

推动技术创新，强化治理保障能力

技术创新是提升数据跨境流动政策监管效率的重要手段。各国应积极开发和部署相应的数据跨境流动数字化平台，通过引入大数据分析、人工智能、区块链技术等，建立更为智能化、自动化的数据监管系统，提高数据跨境流动审批流程的效率和透明度。

具体而言，在数据跨境流动申请与审批过程中，可以构建跨境数据流动在线审批备案平台，利用“自动化流程管理系统”处理企业提交的跨境数据申请，实现资料提交、审批流程流转、结果反馈等环节的自动化，减少人为因素干扰，提高审批效率与可追溯性。在数据合规性审核中，可部署人工智能（AI）和大数据分析技术，对企业上传的数据类别、传输路径、接收方性质等进行自动分类和风险识别，结合历史案例进行合规性智能比对，通过动态监管与实时分析，构建智能化预警机制。在数据全生命周期监控场景中，可引入数据标识技术、区块链技术等，构建全流程可追溯的防篡改数据流动日志，对数据的出境、传输、使用等环节进行时间戳记录和链上备案，实现全生命周期透明管理，提升数据审计能力。

同时，各国应积极推动监管技术标准的互认，如共同制定跨境数据流动的接口标准、构建合规规则建模语言、开发风险评估算法模型等，通过标准的协同制定与实施，促进不同国家和地区间监管平台的互联互通，降低数据跨境流动中的合规壁垒。



附件：相关政策清单

序号	政策名称	政策范式	发布主体	颁布时间
国际组织及区域性政策				
1	全球数字契约	框架内便利型	联合国	2024年9月
2	隐私和跨境个人数据流动保护指南	框架内便利型	OECD	2013年11月
3	个人数据保护框架	审慎弹性型	东盟	2016年11月
4	个人数据保护附加法案	审慎弹性型	西非国家经济共同体	2010年2月
5	伊比利亚美洲国家数据保护标准	审慎弹性型	伊比利亚美洲国家组织	2017年10月
6	第108号公约+	审慎弹性型	欧洲委员会	2018年5月
7	隐私框架	审慎弹性型	APEC	2015年11月
8	欧盟 - 美国数据隐私框架	审慎弹性型	欧盟 - 美国	2023年7月
9	韩国 - 秘鲁自由贸易协定	框架内便利型	韩国、秘鲁	2011年3月
10	中美洲 - 墨西哥自由贸易协定	框架内便利型	中美洲、墨西哥	2011年11月
11	欧盟-日本经济伙伴关系协定	框架内便利型	欧盟、日本	2019年2月
12	区域全面经济伙伴关系协定	框架内便利型	RCEP成员国	2020年11月
13	跨太平洋伙伴关系协定	框架内便利型	CPTPP成员国	2018年12月
14	数字经济伙伴关系协定	框架内便利型	DEPA成员国	2021年1月
国家及地区政策				
15	数据保护法	审慎弹性型	阿尔巴尼亚	2024年12月
16	关于个人数据保护的18-07号法律	审慎弹性型	阿尔及利亚	2018年6月
17	个人数据保护法	审慎弹性型	阿根廷	2016年4月
18	第60-E/2016号规定（个人数据保护）	审慎弹性型	阿根廷	2006年7月
19	ADGM数据保护条例	审慎弹性型	阿联酋	2021年2月
20	第5号数据保护法	审慎弹性型	阿联酋	2020年7月
21	个人信息法	框架内便利型	阿塞拜疆	2010年5月
22	个人数据保护法2020年第151号	约束限制型	埃及	2020年7月
23	埃塞俄比亚联邦民主共和国宪法	框架内便利型	埃塞俄比亚	1995年8月
24	埃塞俄比亚联邦民主共和国刑法	框架内便利型	埃塞俄比亚	2005年5月
25	民法典第958/2016号计算机犯罪公告	框架内便利型	埃塞俄比亚	1960年6月
26	文件认证和登记公告第922/2015号	框架内便利型	埃塞俄比亚	2016年2月

序号	政策名称	政策范式	发布主体	颁布时间
27	电子签名公告第1072/2018号	框架内便利型	埃塞俄比亚	2023年9月
28	爱尔兰数据保护法	审慎弹性型	爱尔兰	2018年5月
29	个人数据保护法	审慎弹性型	爱沙尼亚	2018年12月
30	数据保护法	审慎弹性型	安哥拉	2011年6月
31	联邦隐私法	框架内便利型	澳大利亚	1988年12月
32	国防贸易控制法	审慎弹性型	澳大利亚	2012年11月
33	数据保护法	审慎弹性型	巴巴多斯	2019年8月
34	预防电子犯罪法	框架内便利型	巴基斯坦	2016年8月
35	个人数据保护法案（草案）	审慎弹性型	巴基斯坦	2023年6月
36	信息技术（隐私保护）法案	审慎弹性型	巴基斯坦	2023年草案
37	个人数据保护的2018年第30号法律	审慎弹性型	巴林	2018年12月
38	数据保护法	审慎弹性型	巴拿马	2021年5月
39	互联网民事框架	框架内便利型	巴西	2014年4月
40	个人数据保护法	框架内便利型	巴西	2011年10月
41	一般个人数据保护法	审慎弹性型	巴西	2020年9月
42	数据跨境传输条例	审慎弹性型	巴西	2024年8月
43	个人信息保护法	约束限制型	百慕大	2016年7月
44	个人数据保护法	审慎弹性型	保加利亚	2002年1月
45	关于个人身份信息保护的2009-09号法律	审慎弹性型	贝宁	2009年5月
46	数据保护法	审慎弹性型	比利时	2018年7月
47	关于数据保护和个人数据处理的第90/2018号法	审慎弹性型	冰岛	2018年5月
48	个人数据保护法	审慎弹性型	波兰	1997年8月
49	个人数据保护法	审慎弹性型	波斯尼亚和黑塞哥维那	2011年1月
50	多民族玻利维亚国政治宪法第130条	框架内便利型	玻利维亚	2009年2月
51	数据保护法	约束限制型	博茨瓦纳	2024年8月
52	数据保护法	审慎弹性型	布基纳法索	2013年11月
53	第1号个人数据保护法	审慎弹性型	赤道几内亚	2016年7月

序号	政策名称	政策范式	发布主体	颁布时间
54	丹麦数据保护法	审慎弹性型	丹麦	2018年5月
55	德国联邦数据保护法	审慎弹性型	德国	2018年5月
56	多米尼加宪法第44条	框架内便利型	多米尼加共和国	2010年1月
57	行政违犯法典第195-FZ号	框架内便利型	俄罗斯	2001年12月
58	个人数据法	审慎弹性型	俄罗斯	2006年7月
59	关于批准确保对个人数据主体权利进行充分保护的外国名单	约束限制型	俄罗斯	2020年10月
60	个人数据保护组织法	审慎弹性型	厄瓜多尔	2021年5月
61	欧盟通用数据保护条例	审慎弹性型	法国	2018年5月
62	数据隐私法	审慎弹性型	菲律宾	2012年9月
63	芬兰数据保护法	审慎弹性型	芬兰	2019年1月
64	第132/V/2001号法律	审慎弹性型	佛得角	2001年1月
65	制定数字代码N°23-010的法律	框架内便利型	刚果民主共和国	2023年3月
66	宪法第15条和第20条	约束限制型	哥伦比亚	1991年7月
67	处理个人数据的保护	审慎弹性型	哥斯达黎加	2011年3月
68	格恩西岛辖区数据保护法	审慎弹性型	格恩西岛	2018年5月
69	第94-V号法律“关于个人数据及其保护”	约束限制型	哈萨克斯坦	2013年5月
70	个人信息保护法（PIPA）	框架内便利型	韩国	2011年9月
71	信息与通信网络利用促进法（网络法）	约束限制型	韩国	2001年7月
72	海外经营者个人信息保护法指南	审慎弹性型	韩国	2024年4月
73	荷兰欧盟数据保护法实施法案	审慎弹性型	荷兰	2018年5月
74	透明度和获取公共信息法	框架内便利型	洪都拉斯	2006年12月
75	吉尔吉斯共和国个人数据法	审慎弹性型	吉尔吉斯斯坦	2008年4月
76	关于几内亚共和国网络安全和个人数据保护的 L/2016/037/AN号法律	约束限制型	几内亚	2016年7月
77	阿尔伯塔省个人信息保护法	框架内便利型	加拿大	2003年12月
78	关于公共机构所持文件的获取及个人信息保护法	审慎弹性型	加拿大	1985年7月
79	加拿大联邦法律（个人信息保护与电子文件法）	审慎弹性型	加拿大	2004年1月

序号	政策名称	政策范式	发布主体	颁布时间
80	魁北克省私人部门个人数据保护法	约束限制型	加拿大	1994年12月
81	信息自由与隐私保护修正案	约束限制型	加拿大	1985年7月
82	数据保护法	审慎弹性型	加纳	2012年5月
83	数据保护法	审慎弹性型	加蓬	2011年10月
84	关于个人数据处理的第110/2019 Coll.号法案	审慎弹性型	捷克共和国	2019年4月
85	网络和数据保护法	审慎弹性型	津巴布韦	2020年11月
86	关于喀麦隆电子通信的第2010/013号法律	框架内便利型	喀麦隆	2010年12月
87	关于喀麦隆网络安全和网络犯罪的第2010/012号法律	框架内便利型	喀麦隆	2010年12月
88	关于刑法的第N°2016/007号法律	框架内便利型	喀麦隆	2016年7月
89	关于喀麦隆电子商务的第2010/021号法律	框架内便利型	喀麦隆	2010年12月
90	关于喀麦隆消费者保护的2011/012号框架法	框架内便利型	喀麦隆	2011年5月
91	关于国家信息和通信技术局（ANTIC）的组织和运作的第2019/150号法令	框架内便利型	喀麦隆	2019年3月
92	关于支付系统、手段和事件的第03/16-CEMAC-UMAC-CMAC-CM号条例	框架内便利型	喀麦隆	2016年12月
93	关于保护个人数据的第2024/017号法	框架内便利型	喀麦隆	2024年12月
94	数据保护法	审慎弹性型	卡塔尔	2016年11月
95	数据保护法	审慎弹性型	开曼群岛	2019年9月
96	第06/L-082号个人数据保护法	约束限制型	科索沃	2019年2月
97	第2024-532号法（可再生能源设备税收豁免）	审慎弹性型	科特迪瓦	2024年6月
98	关于电子交易的2013-546号	审慎弹性型	科特迪瓦	2013年7月
99	关于打击网络犯罪的第2013-451号法	审慎弹性型	科特迪瓦	2013年6月
100	关于保护个人数据的2013-450号	审慎弹性型	科特迪瓦	2013年6月
101	关于电信和信息通信技术的第2012-293号命令	审慎弹性型	科特迪瓦	2012年3月
102	关于打击和贩卖人口行为的第2015-79号法令	审慎弹性型	科特迪瓦	2015年2月
103	关于电子交易的第20号法律	框架内便利型	科威特	2014年4月
104	欧盟通用数据保护条例	审慎弹性型	克罗地亚	2018年5月

序号	政策名称	政策范式	发布主体	颁布时间
105	数据保护法	审慎弹性型	肯尼亚	2019年11月
106	个人数据处理法	审慎弹性型	拉脱维亚	2018年7月
107	数据保护法	审慎弹性型	莱索托	2012年2月
108	电子数据保护法	约束限制型	老挝	2017年7月
109	欧盟通用数据保护条例	审慎弹性型	立陶宛	2018年7月
110	欧盟通用数据保护条例	审慎弹性型	卢森堡	2018年5月
111	关于保护个人数据和隐私的第058/2021号法律	约束限制型	卢旺达	2021年10月
112	第190/2018号法律：关于执行欧盟通用数据保护条例的补充措施	审慎弹性型	罗马尼亚	2018年7月
113	数据保护法	审慎弹性型	马达加斯加	2024年12月
114	2018年数据保护法	审慎弹性型	马耳他	2018年5月
115	数据保护法	审慎弹性型	毛里求斯	2018年1月
116	联邦贸易委员会法案	框架内便利型	美国	1914年9月
117	加州消费者隐私法案	框架内便利型	美国	2018年6月
118	关于防止受关注国家获取美国人敏感个人数据和美国政府相关数据的行政命令	约束限制型	美国	2024年2月
119	“应对外国对手获取美国公民敏感个人数据”的最终规则	约束限制型	美国	2024年12月
120	美国云法案	约束限制型	美国	2018年3月
121	网络安全法案	框架内便利型	孟加拉国	2023年2月
122	个人数据保护法	审慎弹性型	秘鲁	2011年6月
123	个人数据保护法	审慎弹性型	摩尔多瓦	2011年7月
124	第1.565号数据保护法	审慎弹性型	摩纳哥	2024年12月
125	联邦个人数据保护法	框架内便利型	墨西哥	2010年4月
126	联邦个人数据保护法实施条例	审慎弹性型	墨西哥	2011年12月
127	保护私人持有的个人数据联邦法	审慎弹性型	墨西哥	2010年7月
128	个人信息保护法	审慎弹性型	南非	2013年11月
129	第787号法第787号个人数据保护法	审慎弹性型	尼加拉瓜	2012年3月

序号	政策名称	政策范式	发布主体	颁布时间
130	国家刑法典	框架内便利型	尼泊尔	2017年8月
131	个人隐私法	约束限制型	尼泊尔	2018年9月
132	个人隐私条例	约束限制型	尼泊尔	2020年10月
133	欧盟通用数据保护条例	审慎弹性型	挪威	2018年7月
134	通用数据保护条例	审慎弹性型	欧盟	2016年4月
135	欧盟通用数据保护条例	审慎弹性型	葡萄牙	2018年5月
136	个人信息保护法下根据充分性认定从欧盟与英国境内接收的个人数据的处理补充规则	审慎弹性型	日本	2003年5月
137	个人信息保护法	审慎弹性型	日本	2015年9月
138	数据保护法	审慎弹性型	瑞典	2018年5月
139	联邦数据保护法	审慎弹性型	瑞士	2020年9月
140	个人数据保护法	审慎弹性型	萨尔瓦多	2021年4月
141	数据保护法	审慎弹性型	塞尔维亚	2019年8月
142	关于电子交易的第2008-08号法	框架内便利型	塞内加尔	2008年1月
143	关于个人数据保护的第2008-12法	审慎弹性型	塞内加尔	2008年1月
144	第2016-29号法	约束限制型	塞内加尔	2016年11月
145	保护自然人免受个人数据处理和此类数据自由流动的第125 (I) /2018号法律	审慎弹性型	塞浦路斯	2018年7月
146	个人数据保护法	约束限制型	沙特阿拉伯	2021年9月
147	个人数据跨境传输条例	审慎弹性型	沙特阿拉伯	2024年9月
148	欧盟通用数据保护条例	审慎弹性型	斯洛伐克共和国	2018年5月
149	欧盟通用数据保护条例	审慎弹性型	斯洛文尼亚	2018年5月
150	信息化法	框架内便利型	塔吉克斯坦	2001年8月
151	信息法	框架内便利型	塔吉克斯坦	2002年5月
152	个人数据保护法	审慎弹性型	塔吉克斯坦	2018年8月
153	信息安全设施认证、信息对象认证及其国家登记程序条例	约束限制型	塔吉克斯坦	2004年10月
154	国家认证的信息安全设施名单	约束限制型	塔吉克斯坦	2008年2月

序号	政策名称	政策范式	发布主体	颁布时间
155	个人数据保护法	审慎弹性型	泰国	2019年5月
156	个人资料保护法	审慎弹性型	坦桑尼亚	2023年5月
157	数据保护法	审慎弹性型	特立尼达和多巴哥	2011年6月
158	电子商务条例	审慎弹性型	土耳其	2006年7月
159	数据保护法	审慎弹性型	土耳其	2016年4月
160	第519-V号《关于私人生活及其保护的信息法》	框架内便利型	土库曼斯坦	2017年3月
161	数据保护和隐私法	约束限制型	乌干达	2019年3月
162	个人数据保护法	框架内便利型	乌克兰	2010年6月
163	第414/009号法令	框架内便利型	乌拉圭	2009年8月
164	第19.670号法令	框架内便利型	乌拉圭	2018年10月
165	第64/2020号法令	框架内便利型	乌拉圭	2020年2月
166	第20.075号法令	框架内便利型	乌拉圭	2022年10月
167	第18.331号数据保护法	审慎弹性型	乌拉圭	2008年8月
168	第ZRU-547号《个人数据法》	审慎弹性型	乌兹别克斯坦	2019年7月
169	西班牙数据保护和数字权利保障基本法	审慎弹性型	西班牙	2018年12月
170	希腊数据保护法	约束限制型	希腊	2019年8月
171	个人数据保护法	审慎弹性型	新加坡	2012年9月
172	关于信息自决权和信息自由的第CXII号法案	审慎弹性型	匈牙利	2011年7月
173	个人数据保护法	审慎弹性型	亚美尼亚	2015年5月
174	隐私保护法	审慎弹性型	以色列	1981年5月
175	第101/2018号法令：关于GDPR实施和国内数据保护法规的调整	审慎弹性型	意大利	2018年9月
176	信息技术法	框架内便利型	印度	2000年10月
177	个人数据保护法案	审慎弹性型	印度	2018年7月
178	关于个人数据保护的2022年第27号法律《个人数据保护法》	审慎弹性型	印度尼西亚	2022年10月
179	数据保护和数字信息法案	审慎弹性型	英国	2018年5月
180	英属维尔京群岛2021年数据保护法	审慎弹性型	英属维尔京群岛	2021年7月

序号	政策名称	政策范式	发布主体	颁布时间
181	关于个人数据保护的13/2023/ND-CP号政府法令	约束限制型	越南	2023年4月
182	第3号数据保护法	审慎弹性型	赞比亚	2021年3月
183	关于个人数据保护的007/PR/2015号法案	审慎弹性型	乍得	2015年2月
184	关于电子交易的008/PR/2015号法	审慎弹性型	乍得	2015年2月
185	数据保护法	审慎弹性型	直布罗陀	2004年1月
186	第19,628/1999号法律	约束限制型	智利	1999年9月
187	中华人民共和国网络安全法	框架内便利型	中国	2016年11月
188	中华人民共和国消费者权益保护法	框架内便利型	中国	1993年10月
189	促进和规范数据跨境流动规定	审慎弹性型	中国	2024年3月
190	数据出境安全评估办法	约束限制型	中国	2022年7月
191	网络数据安全条例	约束限制型	中国	2024年9月
192	个人资料（私隐）条例（第486章）	审慎弹性型	中国香港	1996年12月
193	澳门个人资料保护法	审慎弹性型	中国澳门	2005年8月
194	台湾个人资料保护法	审慎弹性型	中国台湾	2023年5月

注：本报告的政策范式分类依据“二、全球数据跨境流动政策的基本范式”中所述判断。