世界互联网大会智库合作计划系列成果

亚太地区数据跨境流动机制研究报告

北京邮电大学互联网治理与法律研究中心

2026年4月

世界互联网大会
World Internet
Conference

北京郵電大學
Beijing University of Posts and Telecommunications

互联网治理与法律研究中心
INSTITUTE OF INTERNET GOVERNANCE AND LAW

报告编写组成员

组 长

谢 永 江　　北京邮电大学互联网治理与法律研究中心主任、教授

成 员

徐 运 红　　北京邮电大学互联网治理与法律研究中心兼职研究员

潘 静　　北京邮电大学人文学院副教授

黄 雪 晨　　北京邮电大学互联网治理与法律研究中心兼职研究员

黄 亚 雯　　北京邮电大学互联网治理与法律研究中心研究助理

管 春 凤　　北京邮电大学互联网治理与法律研究中心研究助理

王 喆 鹏　　北京邮电大学互联网治理与法律研究中心研究助理

项 玉 瑶　　北京邮电大学互联网治理与法律研究中心研究助理

康 钰 宁　　北京邮电大学互联网治理与法律研究中心研究助理

目录

一、亚太地区数据跨境流动的重要意义 01

（一）数据跨境流动的意义 01

（二）亚太地区数据跨境流动合作的必要性 01

（三）亚太地区数据跨境流动合作的基础 02

二、亚太地区数据跨境流动机制的比较研究 02

（一）数据跨境流动治理的法律规制方面 02

（二）亚太地区主要经济体数据跨境传输的治理模式 03

（三）亚太地区主要经济体数据跨境流动监管体制与执行机制 05

（四）亚太主要国家数据主权战略部署特征比较 06

三、亚太地区数据跨境流动的主要障碍 08

（一）亟待建立统一的数据跨境流动国际规则 08

（二）数据跨境流动隐私保护问题凸显 10

（三）行业数据跨境流动制度亟待细化 11

四、构建亚太地区数据跨境流动协调机制的建议 11

（一）跨境数据法规的协调发展 11

（二）跨境数据监管的协调合作 13

（三）促进数据跨境流动的制度、机制引领模式生成 14

报告摘要

本报告聚焦亚太数据跨境流动机制，系统分析其必要性、可行性、现存障碍及优化路径。

数据跨境流动作为全球数字经济发展的核心驱动力，在促进贸易增长、技术创新与全球治理中发挥关键作用。亚太地区 GDP 占全球 60% 以上，区域内数字贸易活跃度高，数据跨境流动合作兼具经济贸易发展需求、规则协同与技术创新驱动、安全信任保障及区域战略考量的多重必要性。亚太各国和地区相似的市场需求，为合作奠定了可行基础。

通过对比研究发现，亚太各国在法律规制、治理模式、监管体制与数据主权战略上呈现多元特征，形成了自律主导型、规则互认型、安全优先型等差异化路径。当前数据跨境流动面临三大核心障碍：统一国际规则缺失，现有指导规则效力不足；隐私保护界定与制度环境严格程度不一，信任基础薄弱；行业数据流动标准亟待细化，非敏感商业数据与特殊行业数据监管存在空白。

报告建议从三方面构建协调机制：一是推动跨境数据法规协调，统一保护标准与规则用语；二是强化跨境数据监管合作，完善区域协作与数据交易所、清算中心建设；三是引领制度与机制创新，平衡数据流动与安全、技术发展与主权维护。

一、亚太地区数据跨境流动的重要意义

（一）数据跨境流动的意义

数据跨境流动是指数据在不同国家或地区之间进行传输、存储和处理的过程。企业开展跨国业务、科研机构进行国际合作、云服务提供商为全球用户提供服务等活动，都无法脱离数据跨境流动的范畴，数据跨境流动已成为推动全球一体化进程的关键力量。在商业领域，数据跨境流动使得企业能够整合全球资源，提升市场竞争力，推动国际贸易的繁荣发展。科研领域中，数据跨境流动打破了地域限制，促进了全球科研资源的共享与整合，加速了科技创新的步伐。

数据跨境流动具有重要意义。第一，化解数据本地化风险。数据本地化模式下，企业往往需要投入大量资源在各地建立数据中心以满足要求，而数据跨境流动则能打破这些壁垒，促进全球范围内的知识传播与技术合作。不同国家和地区的企业、研究机构可以更便捷地获取、分析和利用来自世界各地的数据资源，加速新产品、新服务的研发进程，提升整个行业的创新能力和竞争力。第二，促进全球经济的增长。TeleGeography 数据库显示，截至 2025 年 9 月，全球数据跨境流动规模达 1835Tbps，较 2024 全年规模（1479 Tbps）增长 24%[1]。第三，推动全球治理的实现。数据跨境流动突破了传统领土主权管辖范围的限制，在打击国际网络犯罪、应对全球气候变化、基因信息的合作开发等超越一国利益的公共议题中发挥了重要作用，具备实现人类命运共同体理念的工具性价值。

然而，数据跨境流动在带来诸多便利的同时，也引发了一系列不容忽视的问题。首先是数据安全问题，数据传输中的黑客攻击、网络窃密等行为易造成商业秘密、个人隐私和国家敏感信息泄露。其次，不同国家和地区在隐私保护方面的标准和法律法规存在显著差异，企业在进行数据跨境传输时容易陷入合规困境。此外，各国数据监管的主体、范围和力度各不相同，使得跨境数据的监管存在诸多空白和漏洞。

（二）亚太地区数据跨境流动合作的必要性

亚太地区覆盖了中国、东盟等全球最具活力的经济体，其在数据跨境流动方面的合作需求愈发凸显。数据跨境流动合作的必要性不仅体现在弥合制度分歧上，更体现在推动区域经济发展、促进规则互通、推动技术进步、保障安全信任以及提升区域全球影响力的综合需求。

1. 经济与贸易发展需求

跨境电商、金融科技和数字服务的快速扩展，直接依赖于数据的自由流动。如果数据无法自由、安全地跨境传输，这一增长态势将受到严重制约。因此，经济与贸易发展的现实需求成为推动亚太地区加强数据跨境流动合作的重要动力。由于亚太地区经济体间具有高度互补的产业链关系，形成了密切的数字贸易网络，若缺乏统一规则，企业将面临高昂的合规成本，区域协作优势被削弱。

2. 规则协同与技术创新的双重驱动

数据跨境流动不仅仅是经济层面的需求，更是规则与技术双重作用的结果。亚太地区有多种数据跨境流动制度安排，例如 APEC 的《互联网与数字经济路线图》、跨境隐私规则（CBPR）和跨境隐私执法安排（CPEA），全球 CBPR 论坛，可信数据自由流动（DFFT），《东盟数字经济框架协议》（DEFA）等，这些规则呈现对接和互认趋势。综合来看，规

[1] 中国信息通信研究院：《全球数字治理蓝皮书（2025 年）》，第 1 页。

则协同为数据跨境流动提供了“制度模板”和“最低共识”，而隐私增强技术、跨境数据传输安全技术、全链路数据可追溯技术等技术创新则使这种协同从原则层面转化为可操作的能力，两者共同推动亚太地区数据跨境流动合作迈出实质性步伐。

3. 安全与信任保障及区域战略考量

在推动数据跨境流动合作的过程中，安全与信任保障始终是绕不开的关键问题。对于亚太地区而言，若没有协调一致的信任和安全框架，各国和地区间的数字合作将逐渐被各自的监管壁垒割裂，区域内部市场的互联互通将受到严重削弱。更为关键的是，全球数字治理格局面临规则碎片化和制度竞争的挑战，美国、欧盟等主要经济体均在强化自身规则的外溢效应。如果亚太地区不能在区域层面形成最低共识与协调机制，跨国企业将被迫在多套制度之间穿梭，不仅增加合规复杂度与成本，也会削弱区域作为整体的制度竞争力。在这种背景下，亚太地区的非约束性与包容性机制成为战略优势，它可以在高政治敏感度之外推动软协调和能力建设，为区域经济体提供安全与信任框架。

（三）亚太地区数据跨境流动合作的基础

亚太地区各经济体存在数据跨境流动相似的市场需求，成为合作的内在动力。首先，平衡数据安全与开放的需求。亚太地区各经济体普遍面临数据安全与经济发展的双重压力，应在数据安全和开放之间寻求平衡。其次，交易信任的需求。目前各经济体对数据跨境流动的规制呈现出碎片化和分散化的特征，尚未形成统一的数据跨境流动规则，难以满足各经济体之间日益增长的交易信任要求，亟需构建区域协同治理体系与标准化合作框架。最后，数字化转型的需求。数据跨境流动能够汇聚全球数据资源，为企业和科研机构提供更广泛的视角和更丰富的素材，从而激发创新思维；数据跨境流动创新和拓展了传统货物和服务贸易的形式与深度，发展出了新贸易业态，有效地促进了全球产业链变革创新。

二、亚太地区数据跨境流动机制的比较研究

（一）数据跨境流动治理的法律规制方面

亚太地区在数据跨境流动治理的法律规制方面呈现出多元体系化发展路径，既包括“充分性”模式，也包括强调数据主权的“本地化”机制，同时存在大量采用混合体系的区域性制度创新并灵活适应。

美国展现出显著的阶段性演变和制度多元性，其规制模式由高度市场导向转变到国家安全主导，美国国内数据跨境监管转向“安全审查机制”日益明显。

日本《个人信息保护法》兼具美欧数据治理模式的特点，其独特的折中设计使得日本《个人信息保护法》既具备系统性也富有操作性。

韩国虽然同样采用统合式立法，但其高度集中与一致性的制度结构，使得法律适用较为直接，执法效率较高。

澳大利亚作为全球较早构建数据跨境流动法律体系的国家之一，搭建了覆盖政府数据、个人健康数据和个人隐私数据三大核心类别的数据跨境治理框架，为跨境数据的合规管理提供了路径指引。

在东盟经济体中，法律规制水平也存在差异。新加坡政府通过一系列法规构建起了较为成熟的数据跨境法律监管框架。马来西亚在数据跨境流动的法律制度建设方面仍处于相对谨慎而渐进的发展路径。泰国近年来不断完善其个人数据跨境流动治理体系。印尼借鉴欧盟与日、韩建立数据跨境流动的政府许可与合规机制。菲律宾、越南等国多采取混合体

系路径设立数据隐私委员会或网络安全局参与跨境监管。从整体看，东盟各国逐渐呈现出若干共同趋势与典型路径，普遍采用“禁止为原则、例外为条件”的监管模式，且一些国家已开始主动对接国际机制。

加拿大和墨西哥作为北美自由贸易区（USMCA）成员，均在国内法中允许数据自由跨境流动。加拿大规定数据出境须保证等效保护，但未设强制本地化义务。墨西哥则设立数据主体权利与处理者义务，支持国际合作并参与 OECD 和 APEC 多边数据治理机制。

中国近年来已逐步构建起较为系统的法律规范框架，涵盖《网络安全法》《个人信息保护法》《数据安全法》《促进和规范数据跨境流动规定》《数据出境安全评估办法》《个人信息出境认证办法》《个人信息出境标准合同办法》等法律政策文件，根据数据的重要性构建了分类分级、宽严相济的数据跨境流动规则体系。

此外，美国、日本、韩国、澳大利亚、新西兰等国与欧盟就个人数据保护达成“充分性认定”，允许跨境自由流动。

综上，亚太地区在数据跨境流动治理的法律规制方面呈现出多元且动态演化的发展路径。有些经济体以“充分性原则”为主导，有些经济体强调数据主权和本地化控制，还有大量经济体采用混合体系模式。

（二）亚太地区主要经济体数据跨境传输的治理模式

亚太地区各经济体对数据跨境传输的管制措施与治理模式呈现出从自由自律到强规制的广泛谱系。美国围绕“数据跨境自由流动”的战略部署，采取去地域化、去本地化模式来强化制度性权力输出，通过主导地位大力推动自由流动数据政策，同时对特定类型数据出境进行严格管制。中国数据出境管理遵循统筹发展与安全原则，在切实保障数据主权与安全的同时，积极促进数据依法有序自由流动。日本采取“互认 + 企业担责”相结合的治理模式，强调国际协作与制度兼容。韩国体现为“强化合规义务 + 逐步开放”的治理思路，个人数据传输至海外需告知并保证接收方有足够保护能力，要求企业承担更高的信息保护与跨境风险控制义务[2]。澳大利亚和新加坡则体现为“宽监管 + 合规保障”的治理结构，在数据自由流动与隐私权保护之间取得动态平衡。在东盟经济体中，泰国、印尼、马来西亚的数据跨境流动管制日益趋严。值得注意的是，俄罗斯和越南都非常重视数据的本地化存储。

总体来看，亚太地区各经济体在管制措施和治理模式上可大致分为六类：一是“自律主导型”，如美国、新西兰，强调企业自律与契约机制；二是“规则互认型”，如日本、韩国、加拿大，通过国际规则对接和标准合同推动制度兼容；三是“安全优先型”，如中国、俄罗斯、越南，强调国家安全优先与本地化控制；四是“混合协同型”，如新加坡、澳大利亚，兼顾监管框架与市场活力；五是“过渡型”，如泰国、菲律宾、马来西亚，制度逐步向多元责任机制演进；六是“初始型”，如巴布亚新几内亚，暂无独立监管机构。

表 1: 亚太地区部分国家数据跨境传输管制措施与治理模式类型表

经济体	管制措施	主要合规路径	本地化	治理模式类型	监管机构	国际互认机制
美国	合同机制/国家安全管制	自律 / 第三方协议	否	自律主导型	联邦贸易委员会（FTC）	欧盟充分性/CBPR/美墨加
中国	安全评估	安评 / 合同 / 认证	是	安全优先型	国家互联网信息办公室（CAC）	无

[2]See APEC: APEC Privacy Framework (2015).https://www.apec.org/docs/default-source/Publications/2017/8/APEC-Privacy-Framework-%282015%29/217_ECSG_2015-APEC-Privacy-Framework.pdf

日本	等效保护	合同 /BCRs/ 互认	否	规则互认型	个人信息保护委员会（PPC）	欧盟充分性/CBPR
韩国	白名单认证	合同/认证	否	规则互认型	个人信息保护委员会（PIPC）	欧盟充分性/CBPR
新加坡	同等保护	合同/BCRs/ 认 证	否	混合协同型	个人数据保护委员会（PDPC）	欧盟充分性/CBPR
澳大利亚	合理义务	合同 / BCRs/ 认 证	否	混合协同型	澳大利亚信息专员办公室（OAIC）	CBPR/澳新隐私规则（CPRR）
加拿大	合理保障	合同 / BCRs/ 认 证	否	规则互认型	加拿大隐私专员办公室（OPC）	欧盟充分性/CBPR/美墨加
马来西亚	充分保护	合同 / BCRs/ 认 证 /白名单	否	过渡型	马来西亚个人数据保护局（PDPD）	拟加入 CBPR
泰国	充分保障	合同 / BCRs/ 认 证 /白名单	否	过渡型	数字经济和社会部（MDES）	ASEAN
印度尼西亚	政府许可	合同/BCRs/认证 /白名单	是	安全优先型	通讯与信息技术部（DGIA MCIT）	拟加入 CBPR
俄罗斯	本地化法	白名单/许可	是	安全优先型	通信、信息技术和大众传媒监督局（Roskomnadzor）	无
越南	强 制 评 估 + 备案	许可机制	是	安全优先型	公共安全部（MPS）	无

墨西哥	同等保护	合同/BCRs/互认	否	规则互认型	国家透明、信息获取和个人数据保护研究所（INAI）	美墨加/拉美数据保护网络（RIPD）
菲律宾	同等保护	合同/BCRs/认证	否	过渡型	国家隐私委员会（NPC）	CBPR
新西兰	同等保护	合同/BCRs/互认	否	自律主导型	新西兰隐私专员办公室（OPC）	欧盟充分性/澳新隐私规则（CPRR）
文莱	等效保护	评估/合同	是	初始型	信息通信技术行业管理局（AITI）	拟加入 CBPR
巴布亚新几内亚	法制初建	待完善	否	初始型	暂无独立监管机构	无
秘鲁	合同保障	BCRs/合同/互认	否	过渡型	国家个人数据保护局	拉美数据保护网络（RIPD）
智利	合同保障	BCRs/合同/互认	否	过渡型	个人数据保护局（筹建中）	拉美数据保护网络（RIPD）

（三）亚太地区主要经济体数据跨境流动监管体制与执行机制

亚太地区各经济体在监管体制建设方面呈现出显著差异，主要表现为监管机构的组织结构、监管权限的配置方式、监管技术手段的应用程度、行业主体的纳入机制以及制度执行的动态适应能力等方面。

美国的跨境数据监管制度体现出典型的“分散监管 + 行业自治”特征，政府鼓励“行业－监管－标准机构”三位一体的治理生态。中国的数据跨境流动监管制度强调“集中监管 + 多层协同”的体制安排，监管架构依托中央－地方－行业三级协同网络落地。日本的跨境数据监管制度则以“独立监管 + 国际对接”为核心特征，个人信息保护委员会设定了“充分性决定”制度[3]。新加坡的监管制度体现出“轻量监管 + 技术赋能 + 能力引导”的复合性结构，个人数据保护委员会构建了“透明度登记系统”[4]，其“指导型监管 + 数字化监督”模式兼顾效率与风险控制。韩国的跨境数据监管制度突出“集中协调 + 分领域管理”的特征，具备“跨机构协同监管”特点。澳大利亚的数据跨境监管制度则构建在“信息专员 + 弹性框架”之上。

[3]See OAS: Desarrollos en la Protección de Datos Personales: APEC y su Marco de Privacidad (2015), Departamento de Derecho Internacional.
[4]See APEC: Cross-Border Privacy Rules (CBPR) System Documents (2011), APEC Secretariat.

表2: 亚太地区部分国家数据跨境流动治理监管制度对比表

经济体	核心监管机构	是否独立	监管职能覆盖面	跨境监管机制	技术手段支持
美国	联邦贸易委员会（FTC）	否	分散（行业分权）	自律框架 + 认证	合规模型 + 行业标准
中国	国家互联网信息办公室（CAC）	否	集中 + 多级协同	评估 + 备案 + 沙箱	实时审计平台、标签识别
日本	个人信息保护委员会（PPC）	是	全国统一监管	充分性 + 互认系统	报备登记系统
新加坡	个人数据保护委员会（PDPC）	是	全国统一监管	工具箱 + 能力建设	风险评分算法
韩国	个人信息保护委员会（PIPC）	是	分领域 + 协同	许可 + 登记平台	隐私保护技术平台
澳大利亚	信息专员办公室（OAIC）	是	统一协调监管	合理义务 +PIA	评估中心 +AI 审查

（四）亚太主要国家数据主权战略部署特征比较

数据主权问题是国家战略安全、技术竞争与全球治理博弈的核心议题，亚太各国在数据主权的战略部署方面表现出显著的多样化特征。数据跨境流动极大挑战“属地法”原则的适用性，因此各国纷纷尝试建构新的治理秩序，确立“数字疆域”上的主权实践逻辑。

从亚太地区主要国家的战略部署看，不同国家根据自身的安全关切、产业结构、技术自主性和国际战略位置，采取了差异化的数据主权路径。

表3: 亚太地区主要国家数据主权战略部署特征对比表

经济体	战略核心目标	主权边界侧重	国际表述语言	核心文件
中国	数据安全与数据资源化并重	国家安全与数据要素流通双轨	网络主权	《中华人民共和国数据安全法》《国家信息化发展战略纲要》
美国	全球数据获取能力强化	跨境执法权延展	全球数据通用管辖权	《CLOUD 法案》《国家网络战略》
日本	可信数据流动促进贸易自由	信任机制与技术规范	可信数据自由流动（DFFT）	《数字社会构建战略》
新加坡	数字互联互通与监管协同	多边信任与合规机制	DFFT+Trust Framework	《数字经济蓝图 2025》
澳大利亚	数据本地化与国家数字主权	国家控制优先	数字主权	《澳大利亚政府数字战略》
加拿大	保护公民隐私与自主监管	隐私主权优先	数据保护主权	《数字宪章》《隐私法改革法案》
韩国	强化国内数据治理基础	安全与产业平衡	数字主权	《数字新政 2.0》
墨西哥	数据自主权与本地经济保护	地区数据主权强化	主权数据战略	《国家数字发展计划 2022-2026》

在制度建构路径方面，各国对于数据主权的部署呈现出四种主要类型：一是以中国为代表的“法律制度－行政体系－产业政策”一体化模式；二是以美国为代表的“技术标准－市场主导－域外适用”路径；三是以日本、新加坡为代表的“国际协同－治理引领”模式；四是以加拿大、澳大利亚为代表的“隐私优先－国家控制”路径。

各国在国际数据主权战略布局上亦呈现出明显分化。日本、新加坡等主张基于“可信数据自由流动”的多边机制，加强跨境合作协定、数据流通协议和可信认证机制建设。中国、俄罗斯、东盟等经济体则更注重数据主权本位与区域性协同，倡导建立多边互信机制。此外，澳大利亚、加拿大等中等规模经济体则在多边和双边之间寻求平衡，在维护自身主权空间的同时，积极参与区域规则制定。

在具体政策工具方面，数据主权战略部署更强调技术性、可执行性与动态可调整性。主要体现为数据出境备案与审批制度、国家级数据认证体系、企业合规治理平台以及与国家安全、反垄断法规联动的监管体系的组合应用。

从根本的战略逻辑与治理哲学上看，各国在数据主权战略部署中大体呈现出四类范式。一是“国家主权优先”型，以中国、俄罗斯为代表，强调国家安全与公共利益；二是“个人数据中心”型，以加拿大、韩国为代表，强调公民权利是数据主权的核心基础；三是“生态导向共治”型，以日本、新加坡为代表，强调多元主体参与和协同治理；四是“市场驱动与安全并重”型，以美国为代表，形成一种混合式路径。总体来看，亚太各国的数据主权战略部署体现出多样化的路径选择与治理思维，各国正加速完善立法体系、监管框架与国际合作机制，未来，亚太国家的数据主权将持续经历从对抗博弈向制度协调过渡的复杂过程。

三、亚太地区数据跨境流动的主要障碍

相较于传统商品与服务，数据因其无形、高速等特点，在跨境流动中的治理复杂性、主权敏感性和技术不确定性更为显著。尽管亚太地区一直持续推动数据跨境流动机制建设，但各国在制度设计、监管重点、隐私标准等方面存在显著差异，在无强制、统一规则的背景下，数据流动受到法律异构性、安全性壁垒、合规成本增加等因素的共同制约。

（一）亟待建立统一的数据跨境流动国际规则

国际社会在数据跨境流动的法律规制方面尚未形成统一体系，各国普遍面临平衡数据主权、跨境自由流动与数据安全的困境。APEC 长期致力于推动亚太地区数字治理合作，其中《跨境隐私规则体系》（CBPR）作为区域性数据治理机制的重要尝试，被视为数字规则建设的核心内容。然而，CBPR 缺乏强制性约束，成员采纳意愿不一，制度接口设计不清，导致未能形成覆盖广泛、执行有力的统一规则体系，导致数据跨境流动实践中存在大量制度“断点”与政策“灰区”[5]。

1. 现有指导规则效力不足

目前，APEC 内部主要依赖 CBPR 作为基础制度框架。然而，成员经济体整体对 CBPR 体系的参与积极性明显不足。自 2013 年该机制启动以来，仅有美国、墨西哥、日本、加拿大、新加坡、韩国、澳大利亚、中国台北和菲律宾九个经济体陆续加入，自 2021年起再无新增成员。这一现状反映出 APEC 内部对 CBPR 制度的适应性和接受度存在较大分歧。该分歧背后是成员经济体间深层制度的不对称，共识扩大和规则扩散效应极为有限。

[5] 参见史佳颖：《APEC 数字经济合作最新进展与中国的参与策略》，载《东北亚经济研究》2024 年第 8 卷第 5 期。

退出机制同样反映制度松散。低门槛、单边可撤回的退出机制虽体现 APEC“非约束性合作”理念，但削弱了规则的稳定性与权威性。从法理看，CBPR 是一种“非强制性治理工具”，运行依赖参与者意愿与互信，而非硬法的统一适用与强制执行。这意味着，CBPR 虽在理念上推动区域数据流动标准一致性，但受限于执行差异、问责缺失及退出松散，难以构建稳定统一的区域数据治理架构。

表4: APEC 与欧盟数据跨境流动机制对比表

维度	APEC-CBPR	欧盟 GDPR
法律约束力	无强制力，成员自愿加入	具有法律强制力，适用于所有成员
合规对象	企业为主，政府间协同缺失	企业 + 国家制度评估并行
数据类型适用	传统个人数据为主	覆盖个人、敏感、生物、AI 生成数据等
合规路径	第三方认证，标准不一	欧盟评估第三国“充分性”后自动互通
成员覆盖	少数 APEC 成员，参与率低	欧盟与约 17 个国家、地区和国际组织达成充分性协议

2. 难以良好平衡数据保护和跨境数据自由流动

在 APEC 框架下，各成员政治体制、监管理念与法律传统高度多元化，如何在保障隐私与国家安全的同时实现高效可信的数据跨境流动，成为制度设计的核心难点。实践中呈现双重困境：放松管制可能导致数据滥用与风险，过度保护则加重企业合规成本、抑制创新与合作。

不同经济体在数据保护强度与流动便利化方面策略分化。一类强调市场驱动，主张自由流动优先，如美国奉行企业主导路径，鼓励通过合同与行业规范达成合规，但隐私保护依赖企业自律，可能引发公众不信任。另一类强调国家主权与数据安全，如越南强调重要 / 核心数据境内存储，出境需审批并留存副本。第三类尝试建立制度桥梁，推动“可信数据自由流动”（DFFT）为核心的多边机制，但“互信”需制度规则与政策透明支撑，实践中互认机制不完善，如韩日虽同为 CBPR 成员，企业仍需履行双重合规程序。

跨境数据争端缺乏有效多边调解机制是当前关键短板。APEC 未建立系统化、有执行力的数据仲裁平台，争端多依赖双边磋商或本地司法，效率低下且易受政治干扰。现有规则体系难以在隐私权保障与自由流动间建立动态平衡，加剧了制度碎片化，激化了不同路径经济体间的博弈与不信任。各经济体出于安全或保护主义采取的单边措施，正在形成“数据壁垒”替代“数据通道”的趋势，削弱了多边互认机制的可能性。

（二）数据跨境流动隐私保护问题凸显

隐私保护问题的突出与制度环境的差异，成为亚太地区数据跨境流动的关键障碍。各国对隐私的文化认知、法律传统与治理模式存在显著差异，导致数据跨境传输中难以实现标准一致、互认互通与监管协调。

1. 数据隐私保护界定范围不统一

隐私保护中“个人信息”或“个人数据”的定义直接决定法律适用范围与强度。不同国家或地区采用的法律定义存在显著差异，这种差异一方面根植于不同的法系传统和政治文化，另一方面也反映出各国对于数字治理目标的偏重不同[6]。美国采取行业法与州法并行，以市场效率和风险控制为导向，如《加州消费者隐私法》（CCPA）虽接近 GDPR，但适用范围有限。日本《个人信息保护法》近年来向欧盟标准靠拢，加强匿名化信息规范。新加坡 PDPA 定义弹性，依赖企业“合理推定”。韩国对个人数据界定严格，2020 年“数据三法”细化分类标准，增强了法律的精细化程度[7]。中国《个人信息保护法》与相关法规重视个人信息保护，构建了分类分级的个人信息跨境流通规则。

各国的立法差异直接影响数据跨境流动的“识别门槛”与“保护义务”，企业需面对标准不一带来的高昂制度协调成本，严重掣肘亚太地区数字经济发展。

2. 各国对数据跨境流动的制度环境严格程度不一

各国在数据跨境流动的合法性基础、监管路径、执法机制等方面存在显著差异。日本通过“白名单制度”认可部分国家等效保护，要求接收方签署合规义务。韩国获欧盟“充分性认定”，要求数据主体同意或接收方提供相当保护水平。新加坡与澳大利亚采取“中度审查 + 企业责任”模式，侧重事后问责与自愿认证。中国则针对不同类型和数量个人信息设定安全评估、标准合同、保护认证、自由流动等路径，体现数据主权优先逻辑。东南亚多数国家个人信息保护制度处于建设初期，法规落地不足，企业面临“法律存在但执行不佳”困境。

[6]See Graham Greenleaf: Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, Privacy Laws & Business International Report, no. 169 (2021), pp. 10–13.

[7]See In Hwan Park: Korea’s Personal Information Protection Act and Sensitive Data Categories, Asia Data Policy Review, vol. 20, no. 2 (2021), pp. 45–62.

此种制度分化不仅影响企业跨境运营连续性，也限制区域统一数字市场构建。数据隐私与国家安全、主权控制深度绑定，使各国在政策制定中易陷入“保护主义回潮”。

（三）行业数据跨境流动制度亟待细化

在亚太地区各国中，尽管一般性数据流动法律框架逐步建立，但针对特定行业数据的跨境流动标准仍存在空白或分歧，亟需区域层面推进制度细化与协调。行业需求差异显著，缺乏基于异质性的分类规则将导致制度适配性低下，既限制低风险行业自由流动，又未有效防范高风险行业外溢。

1. 对非敏感商业数据的跨境流动标准

非敏感商业数据（如产品规格、供应链信息、物流追踪等）不涉及个人身份或企业核心机密，但目前多数国家未设定明确分类与标准化路径。部分国家出于国家安全敏感，将所有类型数据“一刀切”纳入保护，施加高强度合规义务，导致数据分类失衡、监管低效。一些发达国家如美国、加拿大、澳大利亚分类较为清晰，对非敏感数据受限较少；但东盟多国如越南、菲律宾、印尼将运营数据纳入本地化要求，即便不涉隐私也需本地存储或审批，加重中小企业负担。

2. 对金融、征信等特殊行业数据流动的标准

在数据跨境流动治理的整体结构中，金融、征信等特殊行业数据的流动问题长期处于规制焦点。这些数据高度敏感，与国家经济安全深度耦合，各国普遍采取“本地优先、出境审慎”策略，监管普遍保守。中国对金融数据实施双重规制：通用数据法律与金融行业规范相结合，要求本地存储、分类分级保护，出境限于特定安全评估场景。部分国家也采取类似本地化措施，强调国家对跨境数据的实质控制。对于征信数据，韩国要求严密的精细化管控，要求外国电商满足“同时在五国以上拥有业务”方可境外存储信用卡信息，并动态监管。美国则呈现双重性：鼓励自由流动，但通过国家安全审查对特定外国企业设置访问限制，形成“自由流动表象下的单向收拢”。菲律宾、马来西亚等国要求使用本地数据库，出境需特别许可。日本强调数据可追溯性。

当前亚太地区尚未形成针对金融与征信行业的统一规则，各国治理模式差异根源于数据主权认知、风险容忍度及产业发展阶段的不同，如何在保障安全与推动互联互通间找到制度均衡，将是长期挑战。

四、构建亚太地区数据跨境流动协调机制的建议

（一）跨境数据法规的协调发展

1. 统一数据保护标准，平衡数据保护与自由流动

由于亚太地区各经济体对数据保护的认知与监管重点不同，建议从以下三方面构建区域数据保护的统一框架：

第一，构建核心原则框架。以 APEC《隐私框架》（2015 年版）中的九项核心原则为基础，细化拓展：（1）数据最小化原则：要求企业仅收集实现业务目的所必需的最少数据；（2）目的限制原则：强调数据处理须有明确、合法的

初始目的，后续使用不得偏离该目的；（3）透明度原则：要求企业告知用户数据用途，并公开处理方式、范围及可能的跨境流向；（4）安全保障原则：结合新兴技术场景提出具体合规要求[8]。

依据数据敏感程度与风险等级，建议将数据划分为以下四类：（1）国家安全 / 关键基础设施数据。原则上本地化存储，严格限制跨境传输，仅在为履行国际义务或实现特定合作目的，并经国家层面评估与批准后才能传输。（2）敏感个人信息 / 高度敏感行业数据。实施“更高标准的保护要求”[9]，获取数据主体明确授权要求事前备案或监管审批，可要求数据本地化。（3）一般个人信息。通过认证、标准合同或同意等机制实现跨境流动。（4）非敏感商业数据 / 去标识化统计数据。建立“简化跨境流动机制”，允许企业在履行基本告知义务后自由传输，或通过合同条款明确接收方责任，降低合规成本。

第二，建立差异化实施机制。依发展水平实行差异化标准：发达经济体可率先执行“高标准保护 + 简化审批”模式，并为发展中经济体提供技术援助；发展中经济体可设置“过渡期”与“简化要求”，并通过“数字丝绸之路”技术援助项目，建设数据中心安全防护体系。

第三，完善配套保障体系。可从以下四方面构建多层次支撑机制：

（1）开发标准化合规工具。按行业制定数据出境条件，提供数据敏感度评估示例与认证辅助工具包，并提供多语言版本的免费下载渠道。

（2）建立跨境监管合作机制。搭建各国监管机构间的数据共享系统，实时交换企业合规审计报告、数据泄露事件等信息；组织相关国家开展联合调查与惩戒；设立“数据跨境流动争端调解委员会”。

（3）推动技术创新与应用。推广联邦学习、同态加密等技术；利用区块链实现数据跨境流动的全程可追溯；开发 AI 驱动的数据合规监测工具，自动识别企业数据处理中的高风险行为。

（4）建立动态调整机制。定期发布《亚太地区数据跨境流动实施评估报告》，分析标准执行效果、技术风险与市场需求；建立“提案－专家论证－公开征求意见－多边协商”的规则修订程序，并及时补充针对新兴领域的保护要求。

2. 规范规则用语，构建相互衔接的立法监管体系

规则用语歧义是数据跨境流动的障碍之一。因此，可组织编制《跨境数据治理术语指南》，并建立监管互认机制[10]。

（1）建议对核心术语进行标准化定义

首先，应采取功能主义定义方法，对高频概念进行精准界定，并配套注释说明其外延。围绕个人信息收集告知等基础环节，明确数据处理者基本义务。同时允许各国对敏感数据的范围和保护措施作补充规定，但须透明化。通过“等效性认定”机制，对符合核心标准的规则予以互认[11]。

在实体规则层面确立分层化义务体系：第一层级是所有经济体必须遵守的“硬法”底线，确立最低标准；第二层级是允许各国依国情补充规定的“软法”空间，但须通过强制信息披露确保透明度。

此外应嵌入动态适配机制，通过三大路径实现规则趋同与法律文化差异的平衡：一是建立“等效性认定”程序，对符合核心标准的境外规则予以互认；二是设置定期审查条款，保持规则与技术及国际标准同步演进；三是设计争议解决机制，以协商、调解等非对抗方式化解规则解释分歧。最终在标准化与弹性化间寻求平衡，推动区域数据治理实现帕累托改进。

（2）建议构建术语适用的场景化指引，针对易混淆场景提供判定标准

针对行业特性，建议差异化合规路径。敏感行业可采用主权数据共享架构，在本地化存储前提下实现有限跨境流动；对用户跨境流动显著的行业，应配置动态授权管理系统，根据用户实时位置适配不同经济体规则。该框架还应包含风险预警机制，为企业拓展新市场时自动生成合规路线图。

[8] 参见刘晓春：《欧盟〈通用数据保护条例〉的原则条款及其评析》（2019），载“安全内参”网站。
[9] 数据安全技术数据分类分级规则 (2024)。
[10] See Bradford, Anu, The Brussels Effect: How the European Union Rules the World (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), https://doi.org/10.1093/oso/9780190088583.001.0001, accessed 31 July 2025.
[11] 参见蔡培如：《欧盟法上的个人数据受保护权研究——兼议对中国个人信息权利构建的启示》（2021），载《法学家》。

（3）建议建立动态更新与国内法转化机制

一是设立术语审查委员会，每年对核心概念词典进行迭代，将新兴概念纳入体系，并通过注释明确其与现有术语的逻辑关系。

二是形成可操作的标准化成果，为各国修订国内法提供参考。可参考东盟《数据跨境流动示范合同条款》[12]，制定涵盖安全评估、跨境传输协议等关键环节的立法范本，并配套开发企业合规工具包。

（4）构建“法规衔接清单”的动态管理系统

该系统应包含三个功能模块：一是冲突识别模块，定期扫描并标注与核心原则冲突的条款；二是转换工具模块，自动生成差异分析报告；三是实施监测模块，跟踪清单采纳情况并发布年度合规白皮书。同时设立紧急响应通道，在重大监管冲突发生时，72 小时内启动临时协调机制。

（二）跨境数据监管的协调合作

目前，亚太地区数据监管合作仍以双边协议为主，缺乏多边协调机制，导致监管冲突频发[13]。为改善这一状况，建议设立数据监管合作委员会，由成员国数据保护机构代表组成，负责协调跨境执法行动。该机制可借鉴欧盟 GDPR 第 50 条的国际合作框架，但需适应亚太地区的多样性[14]。

鉴于数据主权的政治化趋势加剧了数据跨境流动的难度，为此，可建设区域性“数据清算中心”，即在特定国家或地区设立中立化数据中心，允许数据在本地存储的同时，通过隐私计算技术实现跨境分析。可借鉴新加坡“可信数据共享框架”（TDMF）的合规经验[15]，并结合中国香港大数据交易所（HKBDE）的区块链技术，确保数据流动的可追溯性，满足各成员的监管审计需求。

1. 完善和促进跨境数据监管的区域性合作

由于亚太各国的数据存储政策呈现出显著分化，政策多元化导致企业难以采用统一的存储策略，因此，企业应采用“区域适配优先”原则，根据目标市场的政策特点将数据分类与存储地点精准匹配，并在跨境传输中严格遵循“目的地合规性验证”原则，通过事前合规审查、协议与技术保障、事中事后动态管理三个层次，确保数据流动全链条符合接收方的法律框架。

为从根本上缓解监管冲突，可设立专门机构，承担监管动态共享、跨境事件联合处置及规则统一解释等职能。在此基础上，建立监管互认机制，对符合标准的监管措施予以互认。在实践中，跨境数据监管的区域性合作需要关注以下 7 个因素：

（1）跨文化精细化设计[16]。各国在用户数据保护上存在文化与法律的双重差异。这要求跨境数据机制超越“技术合规”视角，理解区域文化对用户决策的影响。构建多语言信息平台是促进跨境数据监管交流的关键举措。平台应整合数据保护法规、政策等信息，借助翻译技术与人工校对，保障信息传递的准确性。同时，优化平台界面与搜索功能，开设互动板块以鼓励经验共享。此外，需针对不同市场的语言习惯差异，采用本地化设计。

（2）建立跨境数据治理伦理准则。准则应尊重各国文化差异，以公平、公正、透明为原则，规范数据全生命周期：收集应合法必要，存储须确保安全，传输需确认接收方保护能力，使用应保障用户知情权。同时建立伦理审查机制与跨国委员会，鼓励企业自愿遵守。此举为跨境监管提供道德支撑，避免“统一授权模板”，依文化法律拆分授权场景。

（3）提升数据治理团队专业素养。为有效应对跨境数据监管中的跨文化挑战，须对数据治理团队开展系统培训。培训内容应涵盖文化背景知识，并强化跨文化沟通技巧。此外，通过剖析典型案例，提升团队处理实际问题的敏感性与

[12] 参见杨春白雪：《东盟发布〈跨境数据流动合同范本〉（MCC）》（2021），载 CAICT 互联网法律研究中心。
[13] See Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677 (2015).
[14] See Christopher Kuner: A Global Regulatory Framework for Transborder Data Flows, in Transborder Data Flows and Data Privacy Law (Oxford, 2013; online edn, Oxford Academic, 26 Sept. 2013), https://doi.org/10.1093/acprof:oso/9780199674619.003.0008, accessed 2 Aug. 2025.
[15] 参见徐明月、安小米：《协同理论视角下新加坡可信数据共享框架的案例分析》，载《情报理论与实践》2020 年第 43 卷第 10 期，第 177-182 页。
[16] 参见纬迪资本：《破局印尼数据合规：中国企业出海法规解析与安全导航》，载微信公众号“纬迪资本”，2025 年 3 月 24 日。

能力。可以组织定期专家授课、安排国际交流与实地考察，确保团队精准适应不同文化背景下的监管要求。

（4）强化国际合作与论坛机制。积极借助国际合作项目与专业论坛，为各国搭建沟通协作桥梁。一方面，设立专项合作项目，开展联合研究与标准制定，增进国际互信；另一方面，通过举办高规格国际论坛，邀请多方深入研讨，促进思想碰撞与经验共享。此外，企业可建立“动态授权管理系统”，允许用户根据自身需求随时修改授权范围。

（5）建立数据监管协调机构。该机构应具备三大核心职能：负责协调各国的监管政策；建立统一的执法标准；推动监管互认机制。在实施层面，可借鉴国际有益经验，建立分级分类的监管体系。对于基础性数据保护原则，推动各国达成统一标准；对于敏感数据等特殊领域，允许各国在满足基本要求的前提下制定差异化规则。

（6）构建跨境数据泄露事件分级响应预案。事件分级需以实际影响为导向，除范围与严重程度外，应纳入扩散速度、社会影响等维度。建议划分为四个等级：一级为单一国家内的一般用户数据泄露，未造成实质损失；二级为单一国家内的敏感数据泄露，对企业或用户构成直接风险；三级为跨 2~3 个国家的一般性数据异常，影响有限；四级为跨 3 个以上国家的大规模敏感数据泄露，可能引发区域性监管危机与公众信任崩塌。针对不同等级需匹配差异化的响应流程。

（7）打造智能安全监控网络。亚太地区安全监控网络应以技术赋能为核心，整合现有情报资源，构建覆盖数据全生命周期的动态防护体系。技术架构上，在亚太总部部署中央监控平台，利用 AI 算法建立数据流动基线；在各国节点设置边缘计算终端，对敏感数据进行实时加密校验，异常时触发本地预警并同步中央平台。为提升风险识别精准度，需建立跨境威胁情报共享库，汇总各国高发攻击案例与病毒特征，通过中央平台关联分析识别区域性风险源，并向受影响区域自动推送预警。同时，接入监管沙盒数据，对创新业务进行专项监测。

2. 积极推动国际数据交易所、数据清算中心的建设

在数字经济全球化背景下，亚太地区数据流动规模持续扩大，但面临数据权属模糊、各国标准差异等挑战，亟需构建规范化的流动体系。其核心是依托区域性数据交易所实现交易标准化，并借助第三方数据清算中心保障传输安全，形成“交易－处理－传输”的全链条治理机制。交易所需制定统一规则，明确数据权属与定价机制，同时引入智能合约技术，自动执行数据使用范围与期限的约定。

数据跨境传输前，须由独立清算中心进行脱敏处理。该中心可借鉴“数据信托”模式，对医疗、金融等敏感信息进行匿名化处理。清算中心需接受各国联合监督，并与交易所联动，对不合规数据指导企业二次处理，最终出具包含处理信息的“合规证书”以缩短审批周期。

（三）促进数据跨境流动的制度、机制引领模式生成

亚太地区需要从制度顶层设计和技术治理协同两方面入手，形成“规则－技术－合作”三位一体模式。

1. 兼顾数据流动与安全的制度引领

数据跨境流动的制度设计需在“自由流动”与“安全可控”间寻求平衡，通过构建分级分类管理与合规激励约束并重的体系，为数据跨境提供稳定预期。

分级分类是制度设计的核心。针对高敏感数据，应建立严格的安全评估与审批机制，落实“境内存储 + 授权访问”原则；而对一般商业数据，则采取备案制，允许自由流动以降低企业成本。

合规激励与约束机制是制度落地的关键。一方面通过“白名单”制度给予政策优惠，激励企业提升合规能力，另一

方面强化违规惩戒。同时，制度设计需主动与国际规则衔接，并建立动态调整机制，以应对技术与国际形势变化。

针对跨境电商、远程医疗等特殊场景，需进行规则创新。例如，通过“数据脱敏 + 区块链存证”满足跨境电商的监管需求，或利用“端到端加密 + 权限分级”保障远程医疗数据的安全传输。

2. 技术发展与主权维护相促的治理机制

技术进步是数据跨境流动的核心驱动力，但也可能加剧数据主权冲突。需构建“技术赋能 + 主权护航”的协同机制：一方面通过隐私增强技术降低安全风险；另一方面依托多边合作平台维护数字主权平等。

隐私增强技术是实现“数据可用不可见”的关键工具。联邦学习允许各方联合训练 AI 模型而无需传输原始数据，例如在跨境医疗研究中共享梯度参数而非患者病历[17]；同态加密则支持对加密数据进行计算，使企业仅能获取聚合结果而无法解密细节。这些技术的推广需配套标准认证，对相关技术颁发证书并明确应用参数。

多边技术合作平台是维护数字主权的重要载体。可搭建区域性技术共享平台，开放隐私计算工具包等开源资源，避免技术垄断。同时需建立风险评估机制，对新兴技术进行联合研判，制定应用红线，防止技术霸权对主权的侵蚀。

技术治理规则的动态适配是机制可持续运行的保障。应建立“技术监测－规则迭代”闭环，依托科研机构发布风险预警，并通过“监管沙盒”在特定区域测试新规则，确保治理与前沿技术同步。

[17] 参见刘艺璇、陈红、刘宇涵、李翠平：《联邦学习中的隐私保护技术》，载《软件学报》2022 年第 33 卷第 3 期，第 1057–1092 页。