全球数据跨境流动新规出台背景下企业数据合规管理实施路径的分析

前 言

2025 年下半年以来，全球数据跨境流动监管呈现分化加剧、主权升维态势。一方面，美欧之间在数据隐私框架下维持流动通道，但欧盟通过 TikTok 巨额罚款案展现强硬的数据主权执法姿态；另一方面，俄罗斯加速构建网络隔离体系，哈萨克斯坦以《数字法典》确立充分性认定模式，东盟通过 BCR 和 SCC 机制推进区域流动便利化，巴西和阿根廷对标 GDPR 推进跨境传输法治化。

本报告系统梳理美国、欧盟、俄罗斯、哈萨克斯坦、泰国、东盟及印尼马来西亚、巴西、阿根廷等主要国家和地区自 2025 年下半年以来的数据跨境流动法规政策动态，结合欧盟对 TikTok 处以 5.3 亿欧元罚款、美国商务部发布网联汽车最终规则、俄罗斯强化网络隔离管控等重大执法事件，深入剖析各国监管制度的核心要点、适用范围及政策演变趋势。报告立足中国企业走出去实际需求，针对数字科技、汽车、能源、跨境电商、金融等重点行业提出应对建议，并以典型案例分析为支撑，为企业构建跨境数据合规体系提供参考指引。

目 录

一、核心趋势

（一）总体态势：从流动便利化到主权安全化的范式转换

2025 下半年以来，全球数据跨境流动呈现三大鲜明趋势。

趋势一：数据主权监管从规则构建转向刚性执法。欧盟对 TikTok 处以 5.3 亿欧元罚款，标志着数据主权治理从规则构建阶段正式转入刚性执法阶段。该案的核心要义在于：标准合同条款（SCCs）不再仅具形式合规效力，监管机构已启动对数据传输后实际保护效果的实质性审查。此项执法行动对在欧运营的非欧盟企业，特别是中国背景企业，释放出明确信号——既往签署 SCCs 即视为满足 GDPR 要求的合规路径已难以为继，监管机构转而要求企业举证证明 SCCs 在实际执行层面能够提供与欧盟实质等同的数据保护水平。企业须从形式合规转向实质合规，对数据传输后的全链路保护效果进行持续评估与举证准备。

趋势二：地缘政治因素驱动数据跨境管控持续收紧。美国 BIS 网联汽车最终规则以国家安全为由，实质性地将中俄关联汽车软硬件排除出美国市场。该规则采用组件关联审查机制，单一子模块存在中俄关联即可导致整车被排除出美国市场，其实际影响远超规则字面范围。与此同时，俄罗斯加速构建网络隔离体系，2025 年全年断网时长达 37,166 小时，覆盖 1.46 亿人口，新版《信息安全学说》更将卫星互联网定性为敌对技术。数据跨境流动日益成为大国博弈的关键议题，中国企业走出去面临的地缘政治风险显著上升。

趋势三：新兴市场从规则借鉴转向制度创新。哈萨克斯坦《数字法典》将 GDPR 式充分性认定与关键数据强制本地化相结合，形成具有中亚特色的数据治理模式。泰国率先在东盟内部建立 BCR 认证机制并完成首批审批，审查周期仅 180 天且无政府费用。东盟 DEFA 谈判于 2025 年 10 月达成实质性结论，有望成为全球首个区域级数字经济治理协定，覆盖 6.8 亿人口、目标 2 万亿美元数字经济规模。新兴市场正在探索有别于美欧的差异化路径——在确保数据主权的同时推进流动便利化，这为中国企业优化区域合规布局提供了制度性机遇。

（二）对中国企业走出去的总体影响判断

当前全球数据跨境流动监管对中国企业走出去的影响可从五个维度进行评估。

影响维度	具体表现	风险等级
合规成本攀升	须同时满足多个法域的本地化、传输机制、透明度要求，合规投入显著增加	高
供应链重塑	美国 BIS 规则等迫使企业重构供应链，剔除特定国家关联，影响全球产业布局	极高
执法不确定性	SCCs 效力受实质审查，签了合同不等于合规成为新常态，合规判断难度加大	高
市场准入门槛	数据合规成为市场准入的硬性条件，违规可能导致业务暂停或市场禁入	极高
技术路径调整	数据架构须适配本地化优先趋势，全球统一 IT 系统面临拆分重构压力	中高

上述五个维度的影响并非孤立存在，而是相互叠加、彼此放大。例如，供应链重塑直接导致合规成本攀升和技术路径调整，执法不确定性进一步提高了市场准入门槛的判断难度。对于正在推进国际化战略的中国企业而言，数据合规已不再是运营层面的合规事项，而是关系到市场准入、供应链安全、业务连续性的战略层面核心议题。

二、各国/地区法规政策深度解析

（一）美国：国家安全逻辑下的精准围堵

1. BIS《网联汽车最终规则》——供应链数据封锁

该规则由美国商务部工业与安全局（BIS）于 2025 年 1 月 16 日发布，2025 年 3 月 17 日生效，法律依据为《贸易扩张法》第 232 条款及信息通信技术与服务（ICTS）授权。规则建立了四类禁止交易，从硬件进口、软件搭载、整车销售和关联制造商四个维度，对中国和俄罗斯关联的网联汽车供应链实施系统性封锁。

四类禁止交易的核心内容如下：

—— **VCS 硬件进口禁令：**禁止在知情情况下向美国进口由中国或俄罗斯实体设计、开发、制造或供应的车辆连接系统硬件，包括远程信息控制单元、蓝牙、蜂窝、卫星和 Wi-Fi 模块。

—— **含受限软件整车进口禁令：**禁止进口包含受限软件的整车，该软件由中俄实体设计、开发、制造或供应。

—— **含受限软件整车销售禁令：**禁止在美国境内销售上述整车。

—— **中俄关联制造商全面销售禁令：**由中国或俄罗斯拥有、控制或受其管辖的网联汽车制造商，不得在美国销售包含任何 VCS 硬件或受限软件的整车，无论该硬件或软件是否与中俄存在关联。

关键时间节点：软件相关禁令自 2027 年款车型起生效；硬件相关禁令自 2030 年款车型起生效；中俄关联制造商销售禁令自 2027 年款车型起生效。2026 年 3 月 17 日前设计开发且未被中俄实体维护增强的软件子组件可享受遗留代码豁免。

2. 三个关键设计对中国企业的深层影响

该规则的本质并非单纯的数据传输限制，而是以数据安全为切入点对汽车供应链的系统性重构。其中三个关键设计值得中国企业高度关注。

第一，**组件关联审查机制产生广泛溢出效应**。汽车软件系统通常由数百乃至上千个子组件构成，规则规定只要其中一个子组件涉及中俄实体，整套自动驾驶系统软件即被认定为受限软件。这意味着中国软件供应商即便仅提供单一功能模块，亦将导致整车制造商无法进入美国市场。此项设计促使整车制造商在供应商选择上趋于保守审查，实际影响范围远超规则字面规定。实践中，全球主要整车制造商已着手系统排查其供应链中的中国关联子组件，部分企业要求供应商出具书面承诺，声明其产品不含中俄关联代码。上述趋势对中国汽车软件企业（涵盖智能驾驶算法、车载操作系统、车联网通信模块等领域）的海外市场拓展构成实质性制约。

第二，**关联制造商销售禁令具有域外管辖效力**。即使中国背景车企在美国本土设厂、采购美国零部件、雇佣美国员工，只要其最终控制权归属中俄实体，其在美销售车辆即被全面禁止。该条款实质上阻断了中国车企通过美国本土化进入美国市场的路径。比亚迪、蔚来、长安等中国车企此前探索的美国市场准入策略（包括经墨西哥设厂间接进入美国市场等方案）均受到该条款的实质性影响。

第三，**遗留代码豁免附设限制性条件**。2026 年 3 月 17 日前开发的软件子组件，若此后由中俄实体进行维护、增强或修改，则丧失豁免资格。这意味着中国软件供应商对已有产品的任何版本更新或程序缺陷修复均将触发禁令，客观上迫使整车制造商在 2026 年 3 月前完成供应链替代。中国供应商由此面临双重困境：继续维护现有产品将触发禁令限制，停止维护则将丧失既有客户关系与市场地位。

3. EU-US 数据隐私框架（DPF）与中国企业的关系

2025 年 9 月，欧盟普通法院驳回针对 DPF 的司法挑战，DPF 在法律层面获得阶段性稳固。但特朗普 EO 14179（AI 政策）可能调整美国情报机构数据访问限制度，DPF 仍面临不确定性。需要特别指出的是，DPF 仅适用于美国实体接收欧盟数据，中国企业不能依赖 DPF。在欧运营的中国企业须自行构建 SCCs 加补充措施的合规路径，且须为 DPF 可能失效准备 Plan B——即一旦美欧数据传输通道中断，如何确保企业全球数据协同不受冲击。

4. 对中国企业的专项影响分析

美国的数据管控逻辑与欧俄存在本质差异——欧俄侧重管控数据流向，美国则针对供应链来源实施限制。这意味着中国企业应对美国规则的核心不在于数据传输机制的调整，而在于供应链身份的管理。具体而言，中国汽车产业链企业须在保住美国市场与维持中国身份之间做出战略选择。选择保住美国市场意味着供应链的去中国化，包括设立独立法人实体、独立代码库、独立开发团队；选择维持中国身份则意味着放弃美国市场，将资源集中于欧洲、东南亚、中东、拉美等非美市场。这一选择不仅涉及合规判断，更涉及企业的长期市场战略定位。

（二）欧盟：执法亮剑与制度整合并行

1. TikTok 5.3 亿欧元 GDPR 罚款——数据主权执法的里程碑

2025 年 5 月 2 日，爱尔兰数据保护委员会（DPC）对 TikTok 处以 5.3 亿欧元罚款，其中 4,500 万欧元针对违反透明度义务，4.85 亿欧元针对违反跨境传输保障措施。DPC 同时命令 TikTok 在 6 个月上诉期满后暂停向中国的数据传输。此案是 GDPR 跨境传输执法史上具有分水岭意义的案件。

核心违法事实有两项。其一，SCCs 有效性未能验证。TikTok 使用 SCCs 作为向中国传输 EEA 用户数据的法律基础，但 DPC 认定 TikTok 未能证明 SCCs 和补充措施在实际执行中能够确保传输数据获得与欧盟境内实质等同的保护水平。关键问题在于中国工程师通过远程访问方式处理 EEA 用户数据，而 TikTok 无法证明这种远程访问受到有效约束。其二，透明度义务违反。TikTok 的隐私政策未充分告知用户其数据将被传输至中国。

此案的三大执法突破对中国企业具有直接而深远的影响。

突破一：SCCs 从形式合规走向实质审查。过去企业普遍认为签署 SCCs 即可满足 GDPR 跨境传输要求。TikTok 案彻底打破这一认知：监管机构开始审查 SCCs 在实际执行中的有效性，包括接收国法律环境是否允许 SCCs 条款被真正履行。对于中国企业在欧运营，这意味着仅签 SCCs 已远远不够，必须进行传输影响评估（TIA），并部署可验证的技术和组织补充措施。

突破二：远程访问被认定为数据传输。TikTok 案中，中国工程师通过远程访问方式处理 EEA 用户数据，被 DPC 明确认定为 GDPR 意义上的数据传输。这一认定扩大了跨境传输的适用范围：即使数据物理存储在欧盟服务器上，只要位于第三国的人员可以远程访问，即构成跨境传输。这对采用全球统一 IT 系统、集中式数据管理平台的中国科技企业影响深远——企业总部的 IT 运维人员、数据分析师、产品经理等若远程访问欧盟用户数据，均触发 GDPR 第五章跨境传输规则。

突破三：6 个月暂停令的威慑力远超罚款。DPC 不仅开出罚单，更命令 TikTok 在 6 个月内暂停向中国的数据传输。这种业务暂停处罚的威慑力远超罚款本身——对任何依赖全球数据协同的科技公司而言，被迫切断数据流意味着核心业务功能瘫痪。这要求企业将跨境数据合规从合规成本视角升级为业务连续性视角。

2. 中国法律环境对 SCCs 有效性的影响

TikTok 案中，DPC 在审查 SCCs 有效性时，重点关注了中国法律环境是否影响 SCCs 条款的履行。对于所有将欧盟数据传输至中国或允许中国境内人员访问的企业，以下中国法律条款是 TIA 的核心评估对象：

—— **《数据安全法》第 36 条：**外国司法或执法机构调取存储在境内的数据，须经中华人民共和国主管机关批准。该条款可能被欧盟监管机构解读为中国政府有权阻止企业履行 SCCs 项下的数据提供义务。

—— **《个人信息保护法》第 41 条：**非经中华人民共和国主管机关批准，组织和个人不得向外国司法或执法机构提供存储于境内的个人信息。该条款同样可能被认定为影响 SCCs 的可执行性。

—— **《个人信息保护法》第 38 条：**在中国境内运营中收集和产生的个人信息和重要数据，应当依法在境内存储。确需向境外提供的，须通过安全评估、认证或标准合同等方式。该规定意味着中国境内实体在接收境外数据时，可能面临中国法律对数据再传输的限制。

需要指出的是，上述条款在实操中的适用场景主要针对外国司法或执法机构的调取请求，而非企业间的商业数据传输。但欧盟监管机构在 TIA 中可能采取保守解读，将中国政府有权限制数据流出作为 SCCs 有效性的风险因素。中国企业须在 TIA 中充分论证上述条款的适用范围有限，并部署技术补充措施（如数据加密、密钥由中国境外实体控制、数据脱敏处理）以降低风险。

3. 《欧盟 Data Act 汽车数据指南》——车联网数据权利重塑

2025 年 9 月 12 日，欧盟委员会发布《Data Act 汽车数据指南》，针对汽车行业实施 Data Act 第二章（数据访问与共享）提供专项指引。该指南覆盖车辆数据定义、数据访问权、OEM 义务、第三方访问等关键领域。2026 年 9 月起，OEM 须全面提供车辆数据访问功能，用户有权访问并共享车辆数据给第三方服务商。EU Data Act（Regulation (EU) 2023/2854）的一般适用日期为 2025 年 9 月 12 日，其中关于数据访问权和不公平合同条款已于该日生效。针对汽车 OEM 的 Article 3(1)产品设计义务，适用于 2026 年 9 月 12 日之后投放市场的联网产品，即该日期之后首次在欧盟市场销售的车辆须内置数据访问接口。已上市车辆不强制追溯改造，但 OEM 须确保新车型符合要求。

该指南对中国车企的影响体现在三个层面。产品层面，在欧销售的中国品牌车辆须在 2026 年 9 月前建立标准化的数据访问接口，允许用户和第三方获取车辆数据，涉及车机系统架构调整、数据格式标准化、API 开发等工程投入。商业模式层面，过去车企对车辆数据的控制权被打破，用户可自主将数据共享给第三方，这直接影响车企的数据增值服务收入（如保险、维修保养、远程诊断），同时也为中国背景的出行服务企业打开了市场机会。合规层面，OEM 在提供数据访问的同时须保护商业秘密，Digital Omnibus 提案进一步强化了这一保护，允许企业在存在商业秘密泄露至第三国风险时拒绝提供数据——中国车企可探索利用这一条款保护核心技术数据。

4. Digital Omnibus 立法提案——AI Act 修订与 GDPR 简化

2025 年 11 月 19 日，欧盟委员会发布 Digital Omnibus 立法提案（COM(2025) 836），核心内容是对《人工智能法》（AI Act）的修订和《通用数据保护条例》（GDPR）的简化，旨在降低 AI 系统合规成本、澄清高风险 AI 系统义务、简化 GDPR 中个人数据定义和透明度要求的条款。该提案并非针对数据跨境流动的专门立法，而是对现有 AI 和数据保护规则的修正。2026 年 5 月 7 日，欧洲议会和理事会已就该提案达成临时协议（provisional agreement），预计 2026 年下半年正式通过。

对中国企业的影响主要体现在 AI 合规层面。利好方面，提案降低了 AI 系统的合规门槛，有利于在欧开展 AI 业务的中国企业。风险方面，GDPR 简化条款中关于第三国法律保护较弱的表述可能间接影响中国企业获取欧盟数据的便利性。

须特别注意，Digital Omnibus 并未整合 Data Act、数据治理法等其他立法，Data Act 的适用不受该提案影响。企业在合规评估时须将 Digital Omnibus（AI Act/GDPR 修订）与 Data Act（数据访问权）作为两个独立的法规框架分别应对。

（三）俄罗斯：数字主权走向数字封闭

1. 152-FZ 修正案——个人数据本地化强化

联邦法第 23-FZ 号（修订 152-FZ《个人数据法》）于 2025 年 7 月 1 日生效。该修正案对 152-FZ 第 18 条第 5 款进行了根本性修订，从义务导向转为禁止导向——禁止使用俄罗斯境外数据库进行个人数据的记录、系统化、积累、存储、更新和检索。最高罚款为首次违规 600 万卢布，重复违规 1,800 万卢布。上述罚款金额依据 2025 年 5 月 30 日生效的联邦法第 420-FZ 号，即修订《行政违法法典》确定。此外，2025 年 9 月 1 日生效的联邦法第 156-FZ 号和第 233-FZ 号引入了新的罚则，对将同意条款嵌入其他文件等违规行为的罚款可达 150 万卢布。企业应关注 Roskomnadzor 行政罚款体系的持续调整。

跨境传输的合规路径为：本地化先行（境内数据库初始收集）→ 获得数据主体同意 → 跨境同步（不超过本地处理量）→ 向 Roskomnadzor 通知。需要强调的是，新规并非完全禁止跨境传输，而是要求先本地、后跨境的处理顺序。

这一修正案对在俄运营的中国企业影响深远。所有处理俄罗斯公民个人数据的企业，必须确保数据初始收集和处理使用俄罗斯境内数据库。中国企业在俄运营时，须将俄罗斯用户数据的初始处理与全球系统解耦。任何直接将俄罗斯用户数据写入境外数据库的行为（如全球统一 CRM 系统直接收集俄罗斯用户信息）均构成违规。企业须采用本地收集加跨境同步模式，并确保本地系统具备完全离线运营能力——2025 年俄罗斯断网总时长达 37,166 小时，本地系统不能依赖与全球系统的实时连接。

2. 新版《信息安全学说》——从数字主权到数字封闭

2026 年 1 月公开的新版《信息安全学说》标志着俄罗斯数字政策从主权管控升级为全面封闭。核心内容包括：卫星互联网（Starlink）被定性为敌对技术；移动设备和外国邮件服务列为破坏性影响载体；预计 2028 年过渡到网站白名单制度；对数字系统（含 AI）全生命周期实施国家控制。

俄罗斯正在走一条与中国截然不同的数字主权道路。中国的模式是选择性管控加开放发展——在关键领域实施数据管控的同时保持与全球数字经济的深度整合，中国企业的国际化受益于这一策略。俄罗斯的模式则是控制加隔离——将数字主权等同于信息封闭，趋向土库曼斯坦模式。

对中国企业的影响需要从机遇和风险两个维度评估。机遇方面，俄罗斯对外国技术的排斥为中国 IT 企业在俄市场创造了替代机会，中国云服务、企业软件、网络安全产品在俄市场具备拓展空间。风险方面，俄罗斯持续断网和可能的白名单制度使得在俄业务的数据连通性面临极大不确定性。卫星互联网被定性为敌对技术，可能影响使用卫星通信的物流、能源勘探等行业。中国企业须为断网场景做好本地化运营预案，包括本地数据存储、本地业务处理、离线交易支持等。

（四）哈萨克斯坦：《数字法典》——中亚数据治理新范式

《哈萨克斯坦共和国数字法典》于 2026 年 7 月 1 日生效，是中亚地区最具雄心的数字立法。法典效力优先于其他涉及数字领域的普通法律，其制度设计呈现 GDPR 框架加本地化强化加 AI 治理的复合特征。

核心制度设计包括三个方面。

跨境数据传输方面，采用类 GDPR 的充分性认定机制：数据可自由流向提供可比保护水平的国家；跨境传输须满足保护水平等效条件；运营商可采纳 BCR 或 SCC 作为保障措施。关键数据本地化方面，被归类为关键信息基础设施的系统须将数据存储和处理在哈萨克斯坦境内服务器，哈萨克斯坦公民的个人数据须在境内服务器存储和处理，设立国家数据登记册作为行政信息的单一真相来源。AI 治理方面，AI 系统分为低、中、高

风险等级，高风险系统须满足透明度、可解释性和人工监督要求，生成式 AI 和深度伪造内容须明确标注，禁止潜意识操纵技术和社会评分系统。

对中国企业而言，充分性认定模式意味着中国企业须证明中国提供可比保护水平。在当前中哈数据保护水平认定尚未建立的情况下，企业须依赖 SCCs 或 BCR 作为传输保障措施。在哈萨克斯坦运营能源、通信、金融等关键行业的中资企业须部署本地 IT 基础设施。哈萨克斯坦是一带一路重要节点国家，中资企业在哈能源矿产、基础设施建设、金融服务等领域投资密集，《数字法典》的生效将直接触发这些企业的数据合规调整需求。法典效力优先于其他法律的设计减少了法规冲突风险，为企业提供了相对清晰的合规框架。

（五）泰国：东盟数据传输机制的先行者

1. PDPC《BCR 审查与认证法规》

2025 年 9 月 29 日，泰国个人数据保护委员会办公室（PDPC Office）发布 BCR 审查与认证法规，依据 PDPA 第 29 条建立。BCR 分为 BCR-C（控制者）和 BCR-P（处理者）两类，审查周期最长 180 天，无政府费用，认证无固定到期日。已持有 EU 或 UK BCR 的企业可走加速审批通道，首批两份 BCR 已于 2025 年 9 月 30 日获批。

已持有 EU 或 UK BCR 的中国企业集团（如华为、中兴等在欧已有 BCR 布局的企业），可通过加速通道获得泰国 BCR 认证，显著降低集团内跨境数据传输的合规成本。未持有 EU 或 UK BCR 的企业，首次申请审查周期约 180 天，须提前规划。BCR 审批无政府费用，但准备申请文件（含泰语翻译和公证）须投入实质性资源。在充分性名单公布前，中国企业传输泰国数据须依赖 SCCs 或 BCR。

2. 跨境传输 SCC 体系

泰国 SCC 体系支持三种合同条款模式：东盟模型合同条款（ASEAN MCCs）、欧盟 SCC、PDPC 规定的标准条款。SCC 须包含数据导入方 72 小时内报告数据泄露的义务。充分性名单尚未公布。

泰国的SCC体系设计具有灵活性，允许企业选择最适合的合同条款模式。中国企业在泰运营时，若已使用欧盟SCC与其他法域的关联实体进行数据传输，可在泰国直接沿用，无需另行签订PDPC规定条款，降低了多法域合规的复杂性。72小时数据泄露报告义务要求企业建立快速响应机制，这与欧盟GDPR的72小时通知要求一致，已建立GDPR合规体系的企业可直接复用现有流程。

（六）东盟及印尼、马来西亚：区域一体化与国别管控并行

1. 东盟数字经济框架协议（DEFA）

东盟DEFA谈判于2025年10月达成实质性结论（第14轮谈判），预计2026年底签署。覆盖约6.8亿人口，数字经济规模目标从当前约3,000亿美元增至2030年2万亿美元。DEFA推动区域数据流动便利化，已发布东盟跨境数据流动模型合同条款作为SCC模板，建立数字贸易规则、无纸化贸易、电子商务、网络安全和数字支付的统一框架。

DEFA有望成为全球首个区域级数字经济治理协定。其意义在于：在美欧数据治理模式之外，东盟正在形成以便利化加灵活性为特征的第三条道路。不同于欧盟的充分性认定和俄罗斯的强制本地化，东盟路径强调通过模型合同条款和区域互认机制实现数据流动便利化，同时保留各成员国的国别管控空间。对中国企业而言，DEFA一旦签署，在东盟多国布局的中国企业（特别是在东南亚有密集业务布局的电商、物流、金融科技、智能制造企业）可受益于统一的SCC模板和降低的法规差异，显著降低区域合规成本。

2. 印尼PDP法

2022年第27号法（UU PDP）于2024年10月全面生效，参照GDPR设计，具有域外效力。跨境传输须确保接收国保护水平不低于印尼标准或提供充分保障措施。法律适用任何对印尼数据主体产生法律效果的个人数据处理活动。配套实施细则仍在制定中，监管机构组建进程缓慢，执法尚未全面展开。

印尼是中国企业走出去的重要目的地，特别是在镍矿加工、新能源汽车、电商、数字金融等领域投资密集。PDP 法的域外效力意味着即使中国企业在中国境内处理印尼用户数据（如通过跨境电商平台收集印尼消费者信息），也须遵守 PDP 法。在细则尚未出台的窗口期，中国企业应参照 GDPR 标准提前建立合规体系，避免细则出台后面临合规追赶压力。

3. 马来西亚 NCII 制度

2024 年《网络安全法》（Act 854）于 2024 年 8 月生效，建立国家关键信息基础设施（NCII）制度。NCII 实体须进行网络安全风险评估和审计，涉及关键行业数据出境的安全评估要求。NACSA（国家网络安全局）作为主管机构。

马来西亚是中国企业走出去的重要节点，特别是在半导体、电子信息制造、能源、基础设施建设等领域。中资企业在马运营涉及能源、通信、金融等关键行业的，须关注 NCII 认定标准并满足数据安全评估要求。Act 854 的执行细则仍在完善中，企业应密切跟踪。需要特别关注的是，马来西亚 NCII 制度与中国《网络安全法》下的关键信息基础设施保护制度存在衔接问题——在马运营的中国企业可能同时受到两国 CII/NCII 监管，须建立双重合规机制。

（七）巴西：对标 GDPR 的跨境传输法治化

ANPD 第 19/2024 号决议确立跨境传输规则，合规截止日为 2025 年 8 月 23 日。核心机制包括：ANPD 批准的 SCCs、自定义条款、BCR、充分性认定（尚未发布）。数据泄露须在 3 个工作日内报告，须指定数据保护官（DPO）。ANPD 2025-2026 监管议程将国际数据传输列为优先议题，与 EU 保持充分性认定对接讨论。

巴西是中国企业在拉美地区的最大投资目的地，特别是在基础设施、能源电力、农业、制造业等领域投资密集。ANPD 新规要求中国企业在向巴西提供服务或从巴西接收数据时，须确保合同包含 ANPD 批准的 SCC 条款。3 个工作日的数据泄露报告时限比 GDPR 的 72 小时更短，企业须建立快速响应机制。须指定 DPO 并确保 DPO 具备足够的独立性和资源。

中国企业应特别关注 ANPD 与 EU 的充分性认定对接进展。若巴西获得 EU 充分性认定，将简化巴西至欧盟的数据流，但对中国至巴西的数据流影响有限。中国企业在巴西的合规路径仍以 SCCs 为主。此外，巴西与中国的数据保护合作机制尚未建立，企业须自行构建合规体系，不能依赖政府间的互认安排。

（八）阿根廷：充分性认定的延续与深化

2024 年 1 月，欧盟委员会完成对阿根廷的充分性认定续期审查，确认阿根廷继续提供充分的数据保护水平。阿根廷国会正在审议三项新法案，均对标 GDPR 设计，旨在更新 2016 年的《个人数据保护法》（第 25.326 号法）。

阿根廷作为拉美少数持有 EU 充分性认定的国家，具有作为中国企业拉美区域数据中心的潜力。中国企业可通过在阿根廷设立区域数据中心，利用阿根廷的 EU 充分性地位简化欧盟至拉美的数据流动。但须注意目的限制原则——数据须用于初始收集时声明的目的，不能随意扩大使用范围。须关注阿根廷三项新法案的立法进展，及时调整合规策略。

三、中国企业走出去面临的数据合规挑战分析

（一）中国数据出境法规与外国法规的衔接冲突

中国企业走出去面临的一个独特挑战是：既要遵守中国的数据出境监管要求，又要满足东道国的数据本地化和跨境传输规则，两套规则之间存在衔接冲突。

冲突场景一：数据回流冲突。中国《个人信息保护法》第 38 条规定，向境外提供个人信息须通过安全评估、认证或标准合同等方式。当中国企业将东道国用户数据从中国境内服务器传输回东道国时，须同时满足中国数据出境要求（如安全评估或 SCC 备案）和东道国数据入境要求（如欧盟 SCCs 有效性验证）。两套要求在评估标准、审批流程、技术措施等方面存在差异，企业须建立双重合规机制。

冲突场景二：数据调取冲突。中国《数据安全法》第 36 条和《个人信息保护法》第 41 条规定，外国司法或执法机构调取境内数据须经主管机关批准。这一规定在 TikTok 案中被 DPC 作为评估 SCCs 有效性的风险因素。当中国企业将欧盟用户数据传输

至中国境内时，欧盟监管机构可能基于上述条款认定 SCCs 有效性不足。企业须在 TIA 中充分论证上述条款的适用范围有限（主要针对外国司法/执法调取，而非商业数据传输），并部署技术补充措施降低风险。

冲突场景三：本地化双重要求冲突。中国《网络安全法》要求关键信息基础设施运营者在境内收集和产生的个人信息和重要数据须在境内存储。当中国企业同时在俄罗斯、哈萨克斯坦等要求强制本地化的国家运营时，须同时满足中国数据境内存储和东道国数据本地存储的要求。这意味着企业须在多个国家分别部署数据基础设施，大幅增加 IT 投入和运营复杂度。

（二）中国企业全球数据架构面临的根本性挑战

当前大多数中国企业的全球数据架构采用总部集中管理模式——全球各区域业务数据统一汇聚至中国总部数据中心，由总部进行集中处理和分析。这一模式正面临各国数据本地化要求的根本性挑战。

一是全球统一 IT 系统的拆分压力。中国企业普遍使用全球统一的 CRM、ERP、HR 系统，各区域数据统一存储在中国总部或单一区域数据中心。在各国数据本地化要求下，这种一套系统打天下的模式须拆分为区域模块，每个区域须部署本地数据处理能力。以一家在 20 个国家运营的中国制造企业为例，若每个国家都要求本地化部署，IT 基础设施投入可能增加 50%至 100%。

二是总部远程访问受限。TikTok 案确立远程访问等于跨境传输的先例后，中国总部人员远程访问境外用户数据的行为受到严格限制。这意味着总部的 IT 运维、数据分析、产品管理等职能须重新设计——要么将部分职能本地化到各区域，要么建立严格的数据脱敏和访问控制机制，确保总部人员仅能访问非个人数据或已充分脱敏的数据。

三是数据协同价值的受损。全球数据统一管理的核心价值在于跨区域数据分析和协同——通过整合各区域用户行为数据、市场趋势数据、供应链数据，形成全球统一的商业智能。数据本地化要求打破这一模式，各区域数据成为孤岛，企业丧失全球数据协

同的分析优势。这对依赖数据驱动决策的中国科技企业（如跨境电商、社交媒体、数字金融）影响尤为深远。

（三）不同类型中国企业的差异化合规挑战

中国企业在走出去过程中面临的合规挑战因企业类型不同而存在显著差异，须分类分析。

企业类型	核心合规挑战	优先应对方向	合规成本预估
互联网/科技企业	远程访问被认定为跨境传输；SCCs 实质审查；数据架构去耦合	欧盟数据本地化；TIA 与技术补充措施	高（IT 架构重构）
汽车/智能驾驶企业	BIS 供应链限制；Data Act 数据开放；子组件牵连效应	供应链替代评估；数据访问接口开发	极高（市场准入风险）
能源/基础设施企业	多国 CII/NCII 本地化；断网运营风险；跨境数据交换受限	本地数据设施部署；离线运营预案	中高（设施投入）
跨境电商/贸易企业	多法域 SCC 合规；本地化收集；消费者数据保护	区域数据分区；合同条款标准化	中（合规流程优化）
金融/支付企业	数据本地化与跨境支付冲突；监管审批复杂	牌照合规与数据合规协同；本地化金融数据中心	高（监管合规投入）
制造业/供应链企业	供应链数据交换受限；工业数据分类分级；商业秘密保护	数据分类分级；供应链数据协议	中（流程调整为主）

从上表可以看出，互联网科技企业和汽车智能驾驶企业面临的合规挑战最为严峻——前者受 SCCs 实质审查和远程访问认定影响，须重构全球数据架构；后者受 BIS 供应链限制影响，面临市场准入风险。能源基础设施企业须应对多国 CII/NCII 本地化要求，合规投入主要体现在设施部署层面。跨境电商和金融支付企业的合规挑战集中在多法域合同条款管理和本地化运营方面，合规成本以流程优化为主。制造业和供应链企

业的核心挑战在于供应链数据交换和工业数据保护，可通过数据分类分级和供应链数据协议加以应对。

四、重点行业影响深度分析

（一）数字科技行业

数字科技行业是数据跨境流动监管受影响最深的行业。云服务、SaaS 和数据中心运营商面临各国数据本地化要求和跨境传输合规成本的双重压力。

对在欧运营的中国 SaaS 企业而言，TikTok 案确立的远程访问等同于跨境传输这一原则具有直接冲击。如果欧盟用户数据可被中国总部远程访问，包括 IT 运维访问数据库、数据分析师查询用户数据、产品经理查看用户行为统计等情形，即构成须受 GDPR 管辖的跨境传输，须部署 SCCs 并补充保护措施。这要求中国 SaaS 企业重构其全球数据架构：在欧盟部署独立的数据处理基础设施，切断中国总部的远程访问通道；建立基于角色的访问控制机制，确保总部人员仅能访问聚合后的非个人数据；部署端到端加密，密钥由欧盟本地实体控制。

对云服务企业而言，俄罗斯和哈萨克斯坦的强制本地化要求意味着须在两国部署本地数据中心。中国云服务企业可借此机会拓展俄语区市场，但须应对两个挑战：一是俄罗斯断网风险，本地数据中心须具备完全离线运营能力；二是制裁合规挑战，在俄运营须注意美国和欧盟对俄制裁的溢出效应，避免触发二级制裁。

东盟 DEFA 推进为数字科技企业带来机遇——统一的 SCC 模板和降低的法规差异有助于在东盟多国运营的中国科技企业降低合规成本。中国电商、金融科技、出行服务企业在东南亚布局密集，DEFA 一旦签署将显著简化区域数据合规架构。巴西 ANPD 新规要求中国科技企业在向巴西提供服务时须使用 ANPD 批准的 SCC 条款，3 个工作日数据泄露报告要求须纳入运营流程，并须指定 DPO。

（二）汽车行业

网联汽车已成为全球数据跨境监管的焦点行业。中国车企同时面临美国以供应链限制方式封堵市场准入、欧盟以 Data Act 要求数据开放的双重压力，这对车企的数据架构、商业模式和合规体系提出了复杂要求。

美国 BIS 规则的供应链封锁效应方面，中国汽车软件供应商面临被排除出全球整车供应链的风险。即使是提供一个小模块的中国软件企业，其子组件牵连效应会导致整车厂失去美国市场。全球主要整车厂已开始系统排查供应链中的中国关联子组件，部分企业要求供应商书面承诺不含中俄关联代码。中国车企通过在美设厂、使用美国零部件实现本土化的路径也被关联制造商销售禁令阻断——只要最终控制权在中俄实体手中，在美销售的车辆即被全面禁止。

欧盟 Data Act 汽车指南的数据开放要求方面，在欧销售的中国品牌车辆须在 2026 年 9 月前建立数据访问接口。这既是合规挑战，也是商业模式转型契机。中国车企须从数据控制者向数据服务提供者转变，在产品层面建立标准化数据访问接口，在商业模式层面探索数据服务新业态。同时，Digital Omnibus 的商业秘密保护条款可被用于保护核心技术数据——中国车企可探索在存在商业秘密泄露风险时拒绝提供特定数据。

供应链重构机遇方面，美国 BIS 规则迫使全球车企寻找替代中俄的软硬件供应商，但也为中国汽车零部件企业在非美市场创造了替代机会。日韩欧车企在美国市场须去中俄化，但在非美市场仍可与中国供应商合作。中国车企应加大在东南亚、中东、拉美、非洲等非美市场的投入，以对冲美国市场封锁的影响。同时须关注 2027 年款软件合规和 2030 年款硬件合规的时间节点，在 2026 年 3 月前完成面向美国市场的供应链替代评估。

（三）能源行业

跨境能源基础设施的数据交换面临日益严格的数据主权审查，关键能源基础设施数据本地化要求在多个法域同步强化。

俄罗斯 CII 制度方面，能源行业属于关键信息基础设施范畴，在俄运营的能源企业须满足数据本地化要求。俄罗斯断网风险进一步增加了能源数据通信的脆弱性——油气管道监控、电网调度、油田生产等关键系统的数据通信不能依赖与国际网络的实时连接，须建立本地化的数据采集、处理和存储能力。对于在俄运营的中资能源企业，须部署完全离线的数据运营系统。

马来西亚 NCII 制度方面，Act 854 将能源行业纳入关键信息基础设施范畴，在马运营的中资能源企业须满足数据安全评估和审计要求。中国企业在马的能源投资须建立数据安全评估流程。哈萨克斯坦《数字法典》要求关键系统的公民数据须本地存储处理，能源行业大概率被纳入关键系统范畴。中哈油气管道、中哈铀矿合作等项目须部署本地数据基础设施。

跨境能源数据交换受限方面，智能电网、油气管道监控等跨境能源基础设施的数据交换面临多国数据主权审查。中国与中亚国家的天然气管道、与东南亚国家的电网互联等项目，须建立分区管理、本地化处理的数据架构。能源数据交换协议须明确数据类型、传输范围、安全保障措施，并通过各国数据安全评估。

（四）跨境电商行业

跨境电商是中国企业走出去的重要业态，涉及大量消费者个人数据的跨境处理。全球数据跨境流动新规对跨境电商企业的影响主要体现在三个方面。

多法域 SCC 合规方面，跨境电商平台在多个国家同时运营，须同时满足各国的跨境传输合同要求。以一家同时面向欧盟、泰国、巴西市场的中国跨境电商平台为例，须分别签署符合 GDPR 要求的欧盟 SCC、符合泰国 PDPC 要求的 SCC、符合巴西 ANPD 要求的 SCC。三种 SCC 在条款内容、数据主体权利、数据泄露报告时限等方面存在差异，企业须建立多法域合同管理机制。

本地化收集方面，俄罗斯 152-FZ 修正案要求俄罗斯用户数据须先在俄罗斯境内数据库完成初始收集，再在获得用户同意后同步至全球系统。这意味着跨境电商平台须在

俄罗斯部署本地 CRM 数据库，用户注册信息先写入本地数据库，再按合规路径同步至全球系统。同步数据量不得超过本地处理量，且须向俄相关监管部门通知。

消费者数据保护方面，各国的数据泄露报告时限差异较大——欧盟 GDPR 为 72 小时，巴西 ANPD 为 3 个工作日，泰国 SCC 要求 72 小时。跨境电商平台须建立统一的数据泄露应急响应流程，以巴西 3 个工作日这一最短时限为基准设计报告机制，确保满足所有法域的要求。同时须在各运营国指定数据保护联系人，确保当地监管机构能及时联系到企业。

（五）金融与支付行业

金融与支付行业面临数据本地化与跨境支付业务需求之间的根本冲突。金融交易天然具有跨境属性，但各国数据本地化要求使得金融数据的跨境传输面临严格限制。

中国金融科技企业走出去过程中，如支付宝、微信支付等企业在海外业务拓展时，须在各国部署本地化金融数据中心，将用户交易数据的处理和存储本地化。跨境支付须建立分区的数据交换机制：在欧盟区域内部通过 SCCs 实现数据协同，在俄语区采用本地收集与跨境同步相结合的模式，在东盟通过 MCCs 实现区域数据流动。

此外，金融行业的特殊监管要求，包括反洗钱、反恐融资、跨境资金监控等，可能与数据保护法产生冲突。金融机构须在满足数据保护法要求的同时，确保不违反金融监管的跨境数据报告义务。这要求金融企业建立合规冲突协调机制，在数据保护合规与金融监管合规之间取得平衡。

五、中国企业应对策略建议

（一）战略层面：构建分区治理、本地优先的全球数据合规架构

策略一：全球数据分区治理

鉴于各国数据本地化要求差异巨大，中国企业应放弃全球统一数据架构的理想模式，转向分区治理架构。具体分区方案如下。

分区	覆盖区域	架构特征	数据流向	合规重点
欧盟区	EU/EEA	本地化处理加 SCCs	区内自由流动，区	远程访问控制；

		加 TIA	外须 SCCs	TIA
俄语区	俄罗斯、哈萨克斯坦	强制本地化加有限同步	本地优先，跨境须同意加通知	本地数据库部署；离线运营
东盟区	泰国、印尼、马来西亚等	区域 SCC 加国别合规	区内 MCCs，区外须 BCR 或 SCC	BCR 申请；多国合规协同
美洲区	巴西、阿根廷	SCC 加 ANPD 合规	充分性国家自由流动	ANPD 批准 SCC；DPO 指定
中国区	中国大陆	安全评估加 SCC 加认证	按中国跨境传输规则	数据出境安全评估；SCC 备案

策略二：本地化优先原则

在每个运营所在国优先部署本地数据处理能力。在俄罗斯、哈萨克斯坦等强制本地化国家，必须部署本地数据库，且本地系统须具备完全离线运营能力。在欧盟部署本地化处理能力以减少跨境传输需求——将欧盟用户数据的处理、存储、分析全部在欧盟境内完成，避免触发跨境传输规则。在东盟利用区域 SCC 模板实现多国数据协同，降低逐国合规成本。

本地化部署的成本虽然较高，但相比违规风险（罚款、业务暂停、市场禁入）和远程访问受限带来的业务效率损失，本地化投入具有更高的长期性价比。对于资源有限的中小企业，可优先采用云服务商的本地区域服务，如阿里云法兰克福区域、AWS 莫斯科区域等，而非自建数据中心，以降低初期投入。

（二）合规层面：建立可审计的跨境数据传输体系

策略三：从形式合规到实质合规

TikTok 案的核心教训是：签署 SCCs 不等于合规。中国企业须建立可审计的实质合规体系，包括三个层面。

传输影响评估（TIA）方面，对每条跨境数据传输线路进行 TIA，评估接收国法律环境对 SCCs 有效性的影响。特别关注中国《数据安全法》第 36 条、《个人信息保护法》第 41 条等关于数据调取的规定是否影响 SCCs 的履行。TIA 应包括：接收国数据保

护法律体系评估、政府数据调取权力分析、SCCs 条款可执行性评估、补充措施有效性评估。TIA 应每年更新一次，在接收国法律环境发生重大变化时及时修订。

技术补充措施方面，部署可验证的技术保护措施。具体包括：端到端加密，密钥由数据导出方控制，确保数据导入方无法独立解密；数据假名化或匿名化，降低数据被调取后的风险；最小化访问权限，基于角色的访问控制，确保仅授权人员可访问特定数据；全量访问日志留存和审计，确保所有数据访问行为可追溯。

组织补充措施方面，明确数据导入方和处理方的责任义务，建立数据主体权利响应机制，定期开展合规审计，建立数据泄露应急响应流程。特别是要建立数据访问审批机制——任何位于中国境内的人员访问境外个人数据，须经合规部门审批并记录访问目的、访问范围、访问时间。

策略四：多传输机制并行准备

鉴于各国传输机制要求不同且政策可能变化，企业应为每条关键数据流准备至少两种传输机制。主要机制为 SCCs，适用范围最广，是多数法域的首选合规工具；备用机制为 BCR，适用于集团内传输，一旦获批可覆盖集团内所有跨境传输，或适用充分性认定；应急机制为本地化处理，在传输机制失效时切换至本地处理模式，确保业务连续性。

（三）运营层面：重点行业专项应对

策略五：汽车行业——供应链重构与数据开放并行

应对美国 BIS 规则方面：

1. 全面梳理产品线中所有中俄关联的软件子组件，建立供应链数据关联清单。

2. 对面向美国市场的产品线，提前在 2026 年 3 月前完成供应链替代评估，利用遗留代码豁免窗口。

3. 评估技术隔离方案的可行性——设立独立法人实体、独立代码库、独立开发团队，但须注意子组件牵连规则使此方案操作困难。

4. 加大在非美市场（欧洲、东南亚、中东、拉美）的投入，以对冲美国市场封锁的影响。

5. 关注 BIS 通用授权的后续发布，评估是否有适用的豁免场景。

应对欧盟 Data Act 方面：

1. 2026 年 9 月前完成车辆数据访问接口开发，确保在欧销售车辆符合数据开放要求。

2. 建立数据分类分级体系，区分可开放数据和商业秘密数据，利用商业秘密保护条款保护核心技术数据。

3. 探索数据服务新业态——从数据控制者向数据服务提供者转型，将数据合规要求转化为商业模式创新契机。

策略六：数字科技行业——数据架构去耦合

1. 将全球统一 IT 系统拆分为区域模块，实现数据处理的本地化。

2. 在欧盟部署独立的数据处理基础设施，切断中国总部的远程访问通道，建立基于角色的访问控制机制。

3. 评估 BCR 在东盟的可行性，为集团内数据传输建立高效通道。已持有 EU 或 UK BCR 的企业应优先利用加速审批通道。

4. 在巴西市场，确保合同包含 ANPD 批准的 SCC 条款，建立 3 个工作日数据泄露报告机制，指定 DPO。

5. 在俄罗斯部署本地数据库并确保离线运营能力，采用本地收集加跨境同步模式。

策略七：能源行业——关键基础设施合规

1. 在俄罗斯、哈萨克斯坦、马来西亚等强制本地化国家部署本地数据存储和处理设施。

2. 为俄罗斯断网场景准备离线运营预案，确保油气管道监控、电网调度等关键系统的数据采集和处理不依赖国际网络。

3. 建立跨境能源数据交换的安全评估流程，明确数据类型、传输范围、安全保障措施。

4. 在马来西亚关注 NCII 认定标准，满足 Act 854 项下的数据安全评估和审计要求。

策略八：跨境电商行业——多法域合规协同

1. 建立多法域合同管理机制，针对欧盟、泰国、巴西等不同市场分别签署符合当地要求的 SCC。

2. 在俄罗斯部署本地 CRM 数据库，确保用户数据先本地收集后跨境同步。

3. 建立统一的数据泄露应急响应流程，以最短时限（巴西 3 个工作日）为基准设计报告机制。

4. 在各运营国指定数据保护联系人，确保当地监管机构能及时联系到企业。

（四）组织保障层面

策略九：建立跨境数据合规治理体系

1. 设立全球数据合规官（Global DPO），统筹各区域数据合规工作，直接向高管层汇报。Global DPO 应具备中国数据保护法、GDPR 及主要东道国数据保护法的知识背景。

2. 在欧盟、俄罗斯、东盟、拉美等关键区域配置专职数据合规人员，确保每个关键运营国都有合规对接人。

3. 建立全球数据映射清单，全面梳理企业全球数据流，包括数据类型、传输路径、传输机制、存储位置、访问权限。数据映射清单应每季度更新。

4. 每年至少进行一次跨境数据传输合规审计，重点关注 SCCs 有效性、本地化要求和透明度义务。审计应由独立于业务部门的团队或第三方机构执行。

策略十：建立中外数据法规衔接机制

鉴于中国企业须同时遵守中国数据出境法规和东道国数据保护法规，企业应建立专门的中外数据法规衔接机制。具体措施包括：建立中国数据出境合规流程（安全评

估、SCC 备案、认证），确保境外数据回流中国时满足中国法规要求；建立东道国数据保护合规流程（SCCs 签署、TIA 评估、本地化部署），确保中国数据出境后满足东道国要求；建立合规冲突协调机制，当中国法规与东道国法规产生冲突时，通过法律评估、监管沟通、技术措施等方式寻求解决方案。

六、典型案例分析

案例一：TikTok 5.3 亿欧元罚款案——远程访问等于跨境传输

2025 年 5 月 2 日，爱尔兰数据保护委员会（DPC）对 TikTok 处以 5.3 亿欧元罚款。核心违法事实包括：TikTok 将 EEA 用户数据传输至中国境内服务器并允许中国工程师通过远程访问方式处理，但未能证明 SCCs 和补充措施在实际执行中能提供与欧盟实质等同的保护水平。此外，TikTok 的隐私政策未充分告知用户数据将被传输至中国。

此案对企业跨境数据合规的启示是多维度的。远程访问等于数据传输的认定扩展了跨境传输的适用范围。许多跨国企业允许总部 IT 人员远程访问全球各区域的系统日志、数据库和运维平台。在 TikTok 案后，这种实践若涉及欧盟个人数据，即构成须受 GDPR 第五章管辖的跨境传输。SCCs 有效性验证要求将合规重心从签合同转移到证明合同可执行。企业不能仅仅签署 SCCs 了事，还须评估接收国的法律环境是否允许 SCCs 条款被真正履行。6 个月暂停令的处罚设计创造了合规倒计时效应——企业不仅面临罚款，更面临业务中断风险。

对中国企业的实操启示：第一，立即排查中国境内人员对境外个人数据的远程访问情况，包括 IT 运维访问数据库、数据分析师查询用户数据、产品经理查看用户行为统计等场景。第二，部署数据脱敏和访问控制技术措施，确保总部人员仅能访问非个人数据或已充分脱敏的数据。第三，完成针对中国法律环境的传输影响评估，重点分析《数据安全法》第 36 条和《个人信息保护法》第 41 条的适用范围。第四，更新隐私政策，充分披露数据传输安排，确保透明度义务合规。第五，建立数据访问审批机制，任何位于中国境内的人员访问境外个人数据须经合规部门审批。

案例二：美国 BIS 网联汽车规则对中国智能驾驶企业的影响

以一家中国智能驾驶软件供应商为例，分析 BIS 规则的实际影响。假设该供应商为一家欧洲车企的 ADAS 系统提供感知算法模块（SAE Level 3 及以上 ADS 软件的子组件）。根据 BIS 规则的子组件牵连设计，该供应商参与开发的感知算法模块属于受限软件的子组件，整套 ADAS 软件套件因此被认定为受限软件，使用该 ADAS 软件套件的整车无法进入美国市场（2027 年款车型起）。

该中国供应商面临两个选择。选择一，被排除出面向美国市场的供应链——整车厂为保住美国市场，须替换中国供应商。这意味着该供应商不仅丧失美国市场（直接损失），还可能丧失与该整车厂在全球其他市场的合作机会（间接损失），因为整车厂倾向于采用统一供应商以降低系统整合复杂度。选择二，技术隔离方案——将面向美国市场的产品线与全球其他市场隔离，确保美国市场产品不含中国关联代码。但子组件牵连规则使这种隔离在实践中极为困难，需要设立独立法人实体、独立代码库、独立开发团队，成本高昂且效果不确定。

更深层次的影响在于供应链的寒蝉效应。即使该供应商最终选择技术隔离方案，整车厂也可能因为合规风险的不确定性而主动替换中国供应商。这意味着 BIS 规则的实际影响范围远超规则字面覆盖的中俄关联企业——所有中国背景的汽车软件供应商，无论是否实际面向美国市场，都可能面临被全球整车制造商预防性替换的风险。

应对要点：全面梳理产品线中所有中俄关联的软件子组件，建立供应链数据关联清单；评估技术隔离方案的可行性（独立代码库、独立开发团队、独立法人实体），但须认识到子组件牵连规则使此方案操作困难；加大在非美市场的投入，以对冲美国市场封锁的影响；关注 BIS 通用授权的后续发布，评估是否有适用的豁免场景；探索与非美市场整车制造商的深度合作，建立技术绑定关系，降低被替换风险。

案例三：俄罗斯数据本地化新规对中国跨境电商的冲击

以一家在俄运营的中国跨境电商平台为例。该平台原架构为：俄罗斯用户注册信息直接写入位于德国法兰克福的全球 CRM 数据库，中国总部通过全球系统统一管理所有

用户数据。根据 2025 年 7 月 1 日生效的 152-FZ 修正案，俄罗斯用户数据的初始收集（记录、系统化、积累、存储等）必须使用俄罗斯境内数据库，直接写入德国数据库构成违规。

调整方案为：在俄罗斯部署本地 CRM 数据库（莫斯科或圣彼得堡数据中心），俄罗斯用户注册信息先写入本地数据库；在获得用户明确同意后，将数据同步至全球 CRM 系统；同步数据量不得超过本地处理的个人数据量；向 Roskomnadzor 提交通知。

额外风险考量：俄罗斯 2025 年断网总时长 37,166 小时的现实意味着本地系统须具备完全离线运营能力，不能依赖与全球系统的实时连接。该平台须在俄罗斯本地部署完整的业务处理能力——用户注册、商品浏览、订单处理、支付结算等核心功能均须在本地完成，仅在网络可用时将数据同步至全球系统。这要求 IT 架构从全球集中式转向本地分布式，软件开发和运维成本显著增加。

此外，俄罗斯新版《信息安全学说》可能进一步收紧数据管控——卫星互联网被定性为敌对技术，可能影响使用卫星通信的物流追踪系统；预计 2028 年过渡到网站白名单制度，可能影响该平台的域名可访问性。该平台须为这些极端场景准备应急预案，包括本地域名注册、本地支付通道、本地物流合作等。

案例四：中国金融科技企业在东盟的多法域合规实践

以一家在泰国、印尼、马来西亚三国运营跨境支付业务的中国金融科技企业为例。该企业须同时满足三国的数据保护法规要求：泰国 PDPA（须 SCC 或 BCR，72 小时数据泄露报告）、印尼 PDP 法（须充分保障措施，域外效力）、马来西亚 Act 854（NCII 安全评估）。

合规架构设计：在泰国部署本地数据处理设施，评估 BCR 申请的可行性（审查周期约 180 天）；在印尼参照 GDPR 标准建立合规体系，与全球 SCCs 框架对接；在马来西亚关注 NCII 认定标准，满足数据安全评估和审计要求。利用东盟 MCCs 实现三国间的区域数据协同，降低逐国合规成本。同时关注 DEFA 谈判进展，为 2026 年签署后的区域合规简化做好准备。

该案例展示了东盟区域一体化加国别管控并行模式对中国企业的实际影响——企业既可以从区域统一 SCC 模板中受益，又须应对各成员国的国别管控要求。在 DEFA 签署前，企业须在区域协同和国别合规之间取得平衡，优先确保国别合规到位，再追求区域协同效率。

七、结论与展望

（一）核心结论

1. 全球数据跨境流动已从经济议题升级为安全议题。美国以国家安全为由封锁中俄汽车供应链，欧盟以数据主权为由对 TikTok 开出天价罚单，俄罗斯以信息安全为由构建网络隔离体系——数据跨境流动监管已深度嵌入地缘政治逻辑。中国企业走出去必须将数据合规作为战略层面的核心议题，而非运营层面的合规事项。

2. 本地化优先正在成为全球共识。从俄罗斯的强制本地化到哈萨克斯坦的关键系统本地化，从欧盟的实质审查到东盟的国别管控，各国虽路径不同，但都在强化数据本地处理要求。中国企业应顺应这一趋势，构建本地优先、跨境补充的数据架构，放弃一套系统打天下的传统模式。

3. SCCs 从形式合同走向实质审查是不可逆趋势。TikTok 案确立了 SCCs 有效性须实质验证的先例。这意味着跨境数据传输的合规成本将显著上升，企业须投入更多资源进行传输影响评估和技术补充措施部署。中国企业特别须关注中国《数据安全法》和《个人信息保护法》对 SCCs 有效性的影响评估。

4. 东盟正在形成差异化路径。以 DEFA 和泰国 BCR 机制为代表的东盟路径，在美欧模式之外提供了便利化加灵活性的替代方案。中国企业应充分利用东盟的制度红利，优先在东盟布局区域数据合规架构，探索 BCR 和 MCCs 的协同应用。

5. 中国企业面临中外数据法规衔接冲突的独特挑战。中国数据出境监管要求与东道国数据保护法规之间存在衔接冲突，企业须建立双重合规机制，同时满足中国数据出境要求和东道国数据保护要求。这一挑战是中国企业独有的，须通过专门的合规架构设计加以应对。

（二）未来展望

短期（2026 年）关注重点：

—— 欧盟 Digital Omnibus 立法进程（AI Act 修订与 GDPR 简化，2026 年 5 月已达成临时协议，预计下半年正式通过）

—— 美国 BIS 网联汽车软件禁令执行

—— 东盟 DEFA 签署

—— 哈萨克斯坦《数字法典》生效（2026 年 7 月 1 日）

—— 俄罗斯白名单制度进展

—— 巴西 ANPD 充分性认定进展

中期（2027 至 2028 年）关注重点：

—— 美国 BIS 网联汽车硬件禁令执行（2030 年款车型合规截止）

—— 欧盟 Data Act 汽车数据访问要求全面执行（2026 年 9 月起）

—— Digital Omnibus 正式通过后 AI 合规义务的调整

—— 东盟 DEFA 实施效果评估

—— 俄罗斯数字封闭政策的深化或调整

—— 中欧数据保护对话与合作机制进展

—— 中国与一带一路沿线国家数据保护合作安排

对中国企业的整体建议：在全球数据跨境流动分化加剧、主权升维的大背景下，中国企业应放弃一套系统打天下的思维，构建分区治理、本地优先、多机制并行的全球数据合规架构。同时，应将数据合规从被动应对转变为主动能力建设——良好的数据合规体系不仅是合规成本，更是国际市场准入的竞争壁垒和品牌信任的基础。在全球数据治理格局加速重塑的窗口期，率先建立完善数据合规体系的中国企业，将在国际化竞争中占据先发优势。

附录：各国/地区数据跨境流动法规速查表

国家/地区	核心法规	关键日期	主要传输机制	本地化要求	罚款上限
美国	BIS 网联汽车最终规则	2025.03.17 生效	禁止性规则	不适用	交易禁止
欧盟	GDPR 加 Data Act 加 Digital Omnibus	Data Act 一般适用：2025.09.12；Article 3(1) 汽车义务：2026.09.12	SCCs/BCR/充分性 Digital Omnibus：AI Act/GDPR 修订（非数据流动专门立法）	无强制	营收 4%或 2000 万欧元
俄罗斯	152-FZ 修正案	2025.07.01	本地化加同意加通知	强制（初始收集）	1800 万卢布
哈萨克斯坦	《数字法典》	2026.07.01	充分性/BCR/SCC	关键系统强制	行政至刑事
泰国	PDPA 加 BCR 法规	2025.09.29	BCR/SCC	无强制	民事加行政
东盟	DEFA（谈判中）	预计 2026 签署	ASEAN MCCs	各成员国规定	各成员国规定
印尼	PDP 法	2024.10 生效	充分保障措施	无（细则待定）	营收 2%或 20 亿 IDR
马来西亚	Act 854	2024.08 生效	NCII 安全评估	关键行业评估	罚款及监禁
巴西	LGPD 加 ANPD No.19/2024	2025.08.23 合规	SCC/BCR/充分性	无强制	营收 2%或 5000 万 BRL
阿根廷	第 25.326 号法	EU 充分性 2024.01 续期	充分性/SCC	无强制	待新法案确定