财经法学 No. 3，2026
pp. 189 - 208

TikTok 案视角下欧盟个人数据跨境传输监管扩张及中国企业的应对

张　彤*

内容提要：在全球数字化与地缘政治博弈交织的背景下，个人数据跨境传输已成为国际经贸往来与涉外法治的核心议题。2025 年爱尔兰数据保护委员会（DPC）对中国企业 TikTok 作出巨额处罚。通过该案可发现 GDPR 框架下个人数据跨境传输规则的适用逻辑、扩张路径及其背后的数字主权博弈本质，揭示欧盟凭借 GDPR 构建以“实质等同”保护为内核的严格跨境数据监管体系，并通过司法实践不断扩张其规则影响力。这种扩张不是单一维度，而是从地域、行为、审查深度到补充措施的全面进化。这些规则的扩张适用不仅对全球数字企业运营与国际数据流动秩序产生深远影响，也给中国企业带来一系列数据跨境传输的合规困境，应从制度、机制和技术层面，为中国企业数据跨境传输合规提供纾解之道。

关键词：TikTok　数据跨境传输　“实质等同”保护　数据主权　监管扩张

一、问题的提出：TikTok 案何以成为数据跨境传输的“风暴眼”

数据在数字全球化发展的当下，已成为驱动经济增长、社会创新与国家竞争的核心战略资源。在数字经济时代，数据不再是简单的数字化表达，已是经济资源，更是国家战略资源。〔1〕不同于传统资源，数据的价值不仅在于蕴藏的信息本身，更在于其流通和共享所带来的倍增效应。它不仅是跨国公司日常运营、提供全球服务的技术前提，更交织着个人隐私保护、国家数据主权

* 张彤，中国政法大学比较法学院教授。

本文为“中国政法大学新兴学科培育与建设计划”项目的阶段性研究成果。

〔1〕 参见李海舰、赵丽：《数据成为生产要素：特征、机制与价值形态演进》，载《上海经济研究》2021 年第 8 期，第 48 页。

维护、数字经济发展与国际规则竞争等复杂博弈。

全球主要经济体纷纷构建自身的数字治理规则，其中欧盟凭借《通用数据保护条例》(General Data Protection Regulation，以下简称 GDPR)〔2〕率先塑造了一套以个人数据基本权利保护为目的、以实质等同保护为核心原则的跨境数据流动监管范式，并借助“布鲁塞尔效应”，使其规则效力延伸至欧盟境外，对全球数据治理产生了巨大影响。

GDPR 高标准的治理范式在实践中引发了较多国家间的规则冲突与合规困境。特别是对于像中国这样拥有庞大数字市场与活跃出海企业的国家而言，欧盟规则的单边扩张与严苛标准，对我国企业的跨境数据处理构成了较大现实挑战。例如，短视频社交平台 TikTok（及其中国国内版本抖音）的全球崛起与随之而来的监管风暴，将个人数据跨境传输这一复杂议题推至国际舆论与法律博弈的前沿。〔3〕TikTok 作为字节跳动集团面向全球用户的短视频分享平台，自 2018 年 GDPR 生效后迅速在欧洲风靡。为了更好地服务欧洲用户，中国字节跳动集团在爱尔兰注册了 TikTok Technology Limited（以下简称 TikTok Ireland），该公司是其在欧盟境内的核心实体公司；此外，其还在英国注册了 TikTok Information Technologies UK Limited（以下简称 TikTok UK）。

2021 年，爱尔兰数据保护委员会（Data Protection Commission，以下简称 DPC）发起了针对 TikTok Ireland 的合法性审查。根据字节跳动集团自身的说明以及 DPC 的认定，TikTok Ireland 与 TikTok UK 共同作为字节跳动在欧洲经济区（The European Economic Area，以下简称 EEA）用户数据的控制者。TikTok Ireland 于 2021 年 3 月向 DPC 提交了关于向中国进行数据转移的评估报告及其他支持性文件并在后续调查中承认：为支持平台运营，包括与软件工程、维护和开发有关的职能，位于中国的特定人员确实可以远程访问存储于爱尔兰境内服务器上的 EEA 用户数据。2025 年 4 月 30 日，DPC 对 TikTok Ireland 作出了一项对欧盟用户数据跨境具有深远意义的裁决，认定 TikTok Ireland 主要存在两项违规：一是违反 GDPR 第 46 条第 1 款的适当保障措施，未能确保传输至中国的欧盟个人数据获得与欧盟“实质等同”的保护水平；二是违反 GDPR 第 13 条第 1 款的透明度义务，未能清晰告知用户数据将被中国母公司的员工访问。基于以上两项违法行为，TikTok Ireland 被处以 5.3 亿欧元的罚款，同时 DPC 下达了要求其暂停数据传输的暂停令（Suspension Order）和进行整改的纠正令（Corrective Order）。〔4〕

该案件的法律问题在于 TikTok Ireland 作为 EEA 的数据控制者，通过远程访问等方式将用户数据系统性地传输至中国母公司，是否履行了 GDPR 第五章关于跨境数据传输的合规义务。这场争议的核心触及了数字经济的基础性问题：个人数据能否以及如何进行跨越国界流动；当个人数据承载了个人隐私、企业资产与国家安全三重利益时，传统以领土为基点的法律管辖权如何应

〔2〕 See Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC. 该条例于 2016 年 5 月 4 日发布在《欧盟官方公报》上。

〔3〕 例如，以美国为首的多个国家，近几年以“国家安全”为由，对 TikTok 的数据处理实践展开调查，并试图通过行政命令或立法强制其进行业务剥离或数据本地化。例如，美国通过《保护美国人免受外国对手控制应用侵害法》等立法动议，直指 TikTok 的中国背景可能使其用户数据面临被中国政府“非法获取”的风险。

〔4〕 See Decision of the Data Protection Commission, In the matter of TikTok Technology Limited (Case Reference: IN-21-9-2), 30 April 2025.

对。TikTok 案恰好成为一个绝佳的观察窗口，它集中暴露了现行国际规则在数据跨境问题上的碎片化与失灵，迫使我们对相关法律框架进行深刻反思。在数字经济全球化与数据主权意识觉醒的双重背景下，探讨欧盟个人数据跨境监管的扩张逻辑，不仅是法律解释学的任务，更是关乎中国数字企业海外核心资产安全与竞争力的重大经济命题。因此，深入剖析 TikTok 案所折射的欧盟个人数据跨境监管规则逻辑、扩张路径及其战略本质，对于理解全球数据治理格局演变、应对中国企业面临的现实挑战，以及构建中国自身跨境数据治理方案，都具有重要的现实意义。

本文将结合 TikTok 案件事实，综合运用法释义学、比较法学及法经济学的方法深入剖析本案的三项核心法律争议，一是 TikTok Ireland 数据传输行为是否构成 GDPR 意义上的“跨境传输”，二是 TikTok Ireland 是否履行了充分的“风险评估义务”，三是 TikTok Ireland 采取的补充措施与透明度措施是否足以达到 GDPR 要求的“实质等同”的保护水平，目的在于揭示欧盟数据跨境传输监管扩张的本质及中国企业合规的突围路径。

二、规制原点：欧盟个人数据跨境传输的规制模式

（一）数据跨境传输的标准

随着数字经济的蓬勃发展，数据流动的无国界性与法律管辖的地域性之间的张力愈发凸显。对“跨境传输”的准确界定是研究数据跨境传输的重要前提。20 个世纪 70 年代，“跨境数据传输”就已经被提出。〔5〕但至目前，“跨境”的“境”是否为国境尚无定论。从国际法角度看，“境”一般指一个主权国家行使主权的物理空间，即陆、海、空、驻外使馆、船舶以及航空器等。〔6〕欧盟 GDPR 第五章将“跨境传输”解释为“个人数据向第三国或国际组织传输”（transfer of personal data to a third country or to an international organisation）的行为，“第三国”是指欧盟成员国和欧盟经济区国家（除冰岛、列支敦士登、挪威外）以外的国家。“国际组织”是指依照国际公法设立的组织及其下属机构，或依据两个或更多国家之间达成的协议建立的其他机构。综上，数据跨境传输一般情况下可以定义为数据进行跨越国境的传输活动。

欧盟 GDPR 第五章确立了严格的跨境传输限制，旨在确保个人数据流出 EEA 后，其保护水平“实质等同”于欧盟境内。但 GDPR 第五章并未明确界定“向第三国或国际组织传输个人数据”，这给法律适用带来了解释空间。直至欧洲数据保护委员会（以下简称为 EDPB）发布了《关于 GDPR 第三条适用与第五章跨境传输规定之间相互作用的第 05/2021 号指南》〔7〕（以下简称《第 05/2021 号指南》），方才厘清 GDPR 第三条（地域管辖）与第五章（跨境传输）之间的复杂关系。《第 05/2021 号指南》确立了认定数据跨境传输的三个要件：

---

〔5〕 See G. Russell Pipe, *International Information Policy: Evolution of Transborder Data Flow Issues*, 1 Telematics and Informatics 409, 409－418 (1984).

〔6〕 参见沈俊翔：《数字经济时代个人信息跨境保护的机制研究——兼论 CPTPP 视野下人民法院参与全球数据治理的新型路径》，载《法律适用》2022 年第 6 期，第 175 页。

〔7〕 See Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

第一，数据输出方的该项数据处理活动受 GDPR 的约束。〔8〕根据 GDPR 第 3 条的规定，管辖范围包括在欧盟境内设立的控制者或处理者（设立机构原则），以及虽未设立但向欧盟数据主体提供商品或服务或监控其行为的控制者或处理者（目标指向原则）。需要注意的是，是否受 GDPR 约束是以“数据处理活动”而非“实体”为维度，关注的是某实体的特定数据处理活动是否适用 GDPR，而非该实体是否受 GDPR 管辖。换句话说，一个公司的某些数据处理活动受 GDPR 约束，不代表该公司的所有数据处理活动都必然适用 GDPR。

第二，数据的传输。〔9〕数据输出方必须通过传输或其他方式，将个人数据提供给另一数据控制者、共同控制者或处理者（即数据输入方，importer）。该传输行为除了传统的物理传输之外，还包括广泛的使个人数据为数据接收方“可用”（make available）的方式：通过创建账户、授予对现有账户的访问权限，“确认”或者“接受”有效的远程访问请求，嵌入硬盘驱动器或向文件提交密码从第三国进行的远程访问，存储在服务提供商提供的位于 EEA 以外的云。因此，当欧盟的处理者将来自欧盟外控制者的数据回传给控制者时，构成跨境传输。作为某一企业一部分的实体可能会构成单独的控制者或处理者，数据在同一集团的关联公司间交换的，构成跨境传输。如位于爱尔兰的子公司将其雇员数据传输给位于第三国的总公司，由总公司将数据存储在第三国的人力资源中央数据库中，爱尔兰的子公司以雇主身份披露员工数据，是控制者，位于第三国的总公司是处理者，因此符合该条规定，应适用 GDPR 第五章的规定。值得注意的是，《第 05/2021 号指南》明确排除了同一法律实体内部的数据流动构成“传输”的可能性。其一，内部处理不属于传输，即数据未通过传输、披露或以其他方式提供给其他控制者或处理者。构成传输的，必须有一个披露数据的控制者或处理者（输出方）和另一个接收或获得数据访问权的控制者或处理者（输入方）。如果发送者和接收者属于同一个控制者/处理者，则个人数据的披露不应被视为 GDPR 第五章规定的传输。比如公司雇员在履行工作职责情况下一般不属于独立于公司的数据控制者或数据处理者，因此在诸如因差旅至欧盟区域外而远程访问欧盟境内数据时，此行为不会被视为传输。〔10〕其二，直接收集个人数据的行为不构成传输，比如某法国公民在服务器部署在中国境内的电商网站上注册账号时输入个人数据，由于注册账号的个人数据是由该个人直接提供给中国的电商网站，是数据主体直接主动向接收方披露数据的，由于没有控制者或者处理者（输出方）发送或提供数据，即使该行为涉及跨境，却不属于传输行为。〔11〕

第三，数据接收方位于第三国或国际组织。〔12〕若数据处理是代表控制者进行的，当欧盟的控制者在欧盟使用受第三国立法约束的处理者时，处理者有可能收到该国政府的访问请求，因

〔8〕 See EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, p. 7.

〔9〕 See Section 2.2 of the EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

〔10〕 See EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, p. 11.

〔11〕 Ibid., p. 9.

〔12〕 See Section 2.3 of the EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

此，如果处理者对这种访问请求进行响应，就会发生个人数据的转移。在这种情况下，根据 GDPR 第 28（1）条和序言第 81 条，控制者只能使用那些仅能提供充分保证采取符合 GDPR 要求的技术和组织措施的处理者，以使数据处理达到 GDPR 的要求。处理者是否提供了足够的保证的问题也涉及处理的合法性，以及对完整性和保密性原则的尊重，根据 GDPR 第 5 条第 2 款，控制者应对此负责。〔13〕

正是基于以上三个标准，EDPB 强调，无论输出方是否位于欧盟，只要其处理活动落入 GDPR 管辖范围，即可触发传输规则的适用。TikTok Ireland 在欧盟境内注册成立，并作为 TikTok 在 EEA 的主要数据控制者，显然满足该标准。DPC 认定 TikTok Ireland 向中国字节跳动集团公司提供数据的行为构成 GDPR 意义上的“跨境数据传输”，因此必须遵守 GDPR 第五章规定的传输规则。〔14〕

（二）数据跨境传输的路径

随着对个人数据跨境流动认识的不断深入，欧盟的数据跨境流动规制越来越细化，保护力度不断增强。在具体实践方面，GDPR 确立了以“充分性保护”为主，“适当保障措施”和“例外情况”为补充的个人数据跨境流动的路径。

1. 充分性保护评估

GDPR 第 45 条第 1 款规定：“当欧盟委员会决定第三国、第三国境内一个或多个特定行业或国际组织能确保充分的保护水平时，个人数据可以转移向该第三国或国际组织传输。该传输不需要特定的授权。”这就是个人数据跨境传输保护水平的“充分性认定”（adequacy decision）。

对于充分性保护的认定，GDPR 第 45 条第 2 款规定的考虑因素包含：第一，法律规则和相关立法，前者基于对人权与基本自由的尊重，后者包括关于公共安全、国防、国家安全、刑法和公共机构访问个人数据的一般性与部门性立法，以及此类立法的实施、数据保护规则、职业规则和安全措施；第二，第三国或国际组织的一个或多个独立的监管机构的有效运作，保证数据保护规则得以充分实施，在数据主体行使其权利时和与成员国的监管机构合作时提供帮助和建议；第三，第三国或国际组织许下国际性承诺，或者承诺愿意承担有法律约束力的条约或法律文件所规定的其他责任，以及参加多边或地区性体系而产生的义务，特别是其和个人数据保护相关。

GDPR 第 45 条第 3 款还规定，在评估了充分性保护水平（adequate level of protection）之后，欧盟委员会可以通过制定实施性法案的方式决定，本条第 2 款内的第三国、第三国境内领域或一个或多个特定行业或一个国际组织是否具有充分的保护水平。被认定达到充分保护水平的国家，仍需定期接受欧盟委员会对其是否持续具有充分保护个人数据水平的审查评估。当第三国符合其审查标准后，就可以自由接收欧盟境内的个人数据。

目前，欧盟对域外国家或国际组织数据保护水平的充分性认定，是将与欧盟具有同等保护水平的国家或地区列入一份正面名单，即所谓的“白名单”，进而允许个人数据向进入“白名单”

〔13〕 See EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR, p. 12.

〔14〕 See Decision of the Data Protection Commission, In the matter of TikTok Technology Limited (Case Reference: IN-21-9-2), 30 April 2025, para. 129.

的国家或国际组织传输。“白名单”意味着欧盟委员会认定某个国家、地区或国际组织能提供与欧盟同等水平的个人数据保护，数据可以像在欧盟内部一样自由流动，无须额外授权。截至目前仅有英国、日本、韩国等 15 个国家和地区通过评估，进入了欧盟数据流动的“白名单”。〔15〕

2. 适当性保障措施

由于充分性保护标准要求高、审核周期长，满足条件的国家很少，而个人数据跨境流动是连接全球数字经济的纽带，欧盟的高规格管制使其境内数据不能在全球范围内有效流转，不利于成员国数据跨境业务发展。因此，为了能在数字经济市场取得优势，享受数字红利，汲取数字经济价值，GDPR 第 46 条提出了一项替代性措施，即“适当性保障措施”。其适用前提是，如果缺少根据第 45 条第 3 款做出的欧盟委员会的充分性决定，数据控制者或处理者只有在提供适当保障措施，以及为数据主体提供可执行的权利与有效的法律救济措施的情况下，才能将个人数据传输到第三国或某个国际组织。此处的“适当性保障措施”可以通过以下几种方式提供：

第一，订立标准合同条款（standard contractual clauses，以下简称 SCCs）。它是欧盟委员会发布的标准格式合同模板，主要用于在未获得“白名单”认定的第三国传输个人数据时，通过签订该合同来满足 GDPR 的合规要求。欧盟在 SCCs 中将个人数据传输情形分为四类进行规制，包括个人数据从控制者到控制者、从控制者到处理者、从处理者到子处理者及从处理者到控制者的跨境传输，传输者可根据自身需求选择签订合适种类的合同条款。通常情况下，一旦订立标准合同，便能实现数据自由流动，因此 SCCs 制度是不能满足充分性保护标准的传输者常用的方式之一。换言之，SCCs 是为个人数据传输双方提供的数据处理合同范本，将 GDPR 义务转换为合同义务，通过合同义务来保护数据主体权利，具有极强的示范性。

第二，约束性公司规则（binding corporate rules，以下简称 BCRs）。GDPR 第 47 条第 1 款对此进行了规定，主要解决的是跨国公司或其分支机构所在国的个人数据保护水平未达充分性保护标准时，其跨境接收个人数据的问题。一方面跨国公司在运营发展中，可能涉及与欧盟成员国内多方企业进行贸易往来，若一律订立 SCCs，可能过于烦冗，从而降低商事效率。另一方面在跨国公司内部之间因人力资源管理需要，大量、持续性跨境传输个人数据时，若每次都订立 SCCs 既不利于公司及时管控也会增加运营成本，因此可以采用约束性公司规则。跨国公司和关联企业可以依据 GDPR 第 47 条第 2 款的规定，并结合自身实际情况制定一套完整有效的个人数据跨境传输自我约束规则，明确跨境个人数据的类型、级别、出境目的，个人数据主体在跨境活动中可行使的权利以及受侵害后可采取的救济途径。跨国公司内部制定的个人数据处理规则在经过欧盟数据监管与保护机构审核认可后，即可以实现集团间个人数据的自由跨境传输。

第三，行为准则（codes of conduct）。随着数字经济的日益发展，欧盟也意识到了市场自我管理的重要性，在 GDPR 第四章第五部分（第 40—43 条）专门对“行为准则”作了规定，代表不同种类的控制者、处理者的行业协会或其他机构可以自行制定、修改、扩充行为准则，使

〔15〕 截至目前，获得欧盟充分性认定的“白名单”包括以下国家和地区：获得全面认定的有安道尔、阿根廷、加拿大（仅限商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、韩国、瑞士、英国、乌拉圭、巴西（最新加入），获得部分认定的有美国（仅限加入“欧盟-美国数据隐私框架”的特定公司）。需要注意的是，这份名单是动态更新的。例如，巴西在 2026 年 2 月刚刚获得认定，而俄罗斯、中国等主要经济体目前均不在名单内。

GDPR 得以具体应用于实践。行为准则起草完成后交由监管机构审核，获得欧盟监管机构批准后，经由欧盟委员会通过实施法案的方式确定其在欧盟境内产生约束力。因此，对于那些不符合充分性保护认证的个人数据处理者或控制者，根据行为准则的规定，在通过合同或其他具有法律强制力的措施作出有约束力且可执行的承诺后，可以将个人数据传输至第三国。

3. 例外情形

针对既不属于欧盟委员会认定的“白名单”国家，也不适用“适当性保障措施”的个人数据传输方，GDPR 第 49 条规定了许可个人数据跨境流动的例外情形，包括：数据主体明知传输者保护力度不足仍明确同意个人数据跨境流动；为履行数据主体与控制者之间的合同所需要；为了实现公共利益，如预防犯罪、保护国家安全；为了保护数据主体利益以及行使诉讼权利需要等。如果上述条件都不满足，在已对个人数据跨境流动进行过安全评估并依此评估采取了保障措施，跨境传输不会重复进行且仅涉及少部分数据主体时，传输者也可将欧盟公民的个人数据转移至境外。

综上，GDPR 和《第 05/2021 号指南》共同确定了欧盟个人数据跨境传输的标准。一旦某一数据处理活动被认定为“跨境传输”，在遵守 GDPR 第五章的情况下，可通过上述三条合法性路径进行传输。〔16〕GDPR 确立了数据跨境传输的宏观框架，而 EDPB《第 05/2021 号指南》则通过三要件，赋予了该框架以具体的执行力，体现出欧盟数据传输架构从“形式合规”向“实质合规”的深刻转型。

三、制度演进：从 Schrems 系列案到 TikTok 案的监管逻辑嬗变

（一）Schrems 系列案从“安全港”到“隐私盾”再到“数据隐私框架”：司法挑战推动制度升级

GDPR 出台前，欧盟《1995 年指令》就已经规定，为确保高水平个人数据保护，只有在第三国能够确保足够保护水平的情况下，个人数据才被允许传输至欧盟/EEA 之外。此类充分性水平的确定应根据数据传输操作相关情况以及所涉第三国现行的法律进行评估。评估合格后，欧盟委员会可以通过决定的法律形式来确认第三国能够提供足够保护水平。据此，欧盟委员会发布了《根据欧洲议会和理事会第 95/46/EC 号指令，关于美国商务部发布的“安全港隐私原则”及相关常见问题解答所提供的保护充分性的委员会第 2000/520/EC 决定》（以下简称《2000/520 充分性决定》），该决定的核心是确立了欧盟—美国安全港框架（U. S. - EU Safe Harbor Framework），允许获得安全港认证的美国公司在没有其他保障措施的情况下从欧盟接收个人数据。该框架确立了以企业自律为核心的安全港机制，认为美国商务部制定的安全港个人数据保护规则是充分的，并允许向符合规定的美国公司传输个人数据。但是 2013 年 6 月奥地利公民施雷姆斯（Schrems）向爱尔兰数据保护专员投诉，要求禁止 Facebook Ireland 将其个人数据传输到美国。他认为，斯诺登对美国情报部门活动的揭露事件表明，美国现行法律无法确保充分保护其境内的个人数据免受公共当局进行的监视活

〔16〕 See Section 3 of the EDPB Guidelines 05/2021 on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR.

动。2015 年 10 月 6 日，欧盟法院宣布安全港认定无效，理由是它无法有效防止美国情报当局大规模获取从欧洲传输至美国的个人数据，未能提供符合欧盟《1995 年指令》所要求的充分保护水平。个人数据保护机制依赖企业自律，无法约束公权力的监控，且欧盟公民在美国无司法救济权利。〔17〕法院认为，这一要求应根据《欧盟基本权利宪章》来解读，该宪章保护隐私权、数据受保护权和有效司法救济权，并赋予成员国数据监管机构监督权。这也意味着欧盟对第三国在保障方面的规则和做法进行持续评估，并以此作为数据传输的条件。〔18〕

欧盟法院在 Schrems Ⅰ案中裁定安全港无效表明，仅靠企业自律，不能约束美国情报机构的大规模监控。因此，需要制定限制、保障措施和司法控制机制，以确保欧盟的个人数据得到持续保护，其中包括当公共当局出于国家安全、公共利益或执法目的访问和使用数据时。〔19〕

Schrems Ⅰ案后，欧盟委员会仍然致力于为跨大西洋个人数据传输建立新框架，以确保新安排完全符合法院强调的标准。〔20〕2016 年 2 月 2 日，欧盟和美国达成《隐私盾保护框架》（EU-U. S. Privacy Shield Framework）。这项新安排主要引入新的保障措施，强化对美国情报机构访问个人数据的限制，如设立了隐私盾监察员（privacy shield ombudsman）机制，明确数据主体权利保障措施要求美国企业承诺更强义务，增加美国商务部对参与企业的合规审查。然而施雷姆斯再次向爱尔兰监管机构申诉，认为 SCCs 同样无法阻止美国政府随意的数据访问。2020 年 7 月 16 日欧盟法院在 Schrems Ⅱ案中裁定欧盟委员会的《隐私护盾决定》无效，但确认了 SCCs 的有效性，同时对基于 SCCs 的传输提出了更严格的要求。理由是：SCCs 仅属合同性质，无法约束第三国政府（尤其是情报机构）的数据调取权。因此，个人数据输出方负有评估义务，即必须开展“传输影响评估”（tranfer impact assessment，简称 TIA），以审视第三国的法律环境是否会减损 SCCs 提供的保护。若评估结果显示存在风险，则必须采取“补充措施”（supplementary measures），包括技术措施（如加密）、合同措施及组织措施。〔21〕美国法律对公权力访问数据的限制不能满足欧盟法的要求，如美国《外国情报监视法》第 702 条等仍允许大规模监控，不符合比例性和严格必要性原则。隐私盾监察员机制也不符合《欧盟基本权利宪章》第 47 条意义上的“法庭”要求，该机制不独立且无法作出有约束力的决定，无法为欧盟公民提供有效的司法救济，未能提供与欧盟基本权利宪章“实质等同”（essentially equivalent）的保护。

为回应 Schrems Ⅱ判决，2023 年欧美之间达成新的《欧盟—美国数据隐私框架》（EU-US Data Privacy Framework），欧盟委员会于 2023 年 7 月通过该框架的充分性认定。这项新安排引

〔17〕 See Maximillian Schrems *v*. Data Protection Commissioner, Case C－362/14, Judgment of the Court (Grand Chamber) of 6 October 2015, para. 26.

〔18〕 See *The CJEU's Schrems Ruling on the Safe Harbour Decision*, (October 2015), https://www.europarl.europa.eu/RegData/etudes/ATAG/2015/569050/EPRS_ATA(2015)569050_EN.pdf, visited on 20 December 2025.

〔19〕 See *Transatlantic Data Flows: Restoring Trust through Strong Safeguards*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2016%3A117%3AFIN, visited on 20 December 2025.

〔20〕 See *On the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C－362/14 (Schrems)*, https://eur-lex.europa.eu/legal-content/EN/TXT/? uri=CELEX%3A52015DC0566, visited on 20 December 2025.

〔21〕 See Data Protection Commissioner *v*. Facebook Ireland Ltd, Maximillian Schrems, C－311/18, EU: C: 2020: 559, para. 135.

入了新的保障措施，如引入具有约束力的比例原则约束政府部门的情报收集，设立数据保护审查法院（Data Protection Review Court，DPRC），可对情报活动进行事后司法审查，提供独立的司法救济。此外，拜登政府发布第 14086 号《关于加强美国信号情报活动保障措施的行政命令》，明确要求优先采用有针对性的情报收集方式，为例外情形设置严格条件。采用上述保障措施保证对欧盟公民基本权利的高水平保护，旨在为大西洋两岸共同开展业务的公司提供必要的法律确定性。

2015 年的 Schrems Ⅰ案终结了安全港机制，2020 年的 Schrems Ⅱ案终结了隐私盾机制，迫使美国为保护个人数据跨境传输进行更深层次的法律改革，实现对个人数据保护从“行政救济”到“司法救济”的质变。首先，Schrems Ⅰ案打破了对“充分性决定”的迷信，欧盟法院首次认定，美国国内法对公共权力获取数据的限制不符合欧盟基本权利标准，特别是《欧盟基本权利宪章》第 7 条（尊重私人和家庭生活）和第 8 条（个人数据保护）。但是也遗留了一个未决问题，即法院未直接否定 SCCs，导致企业转向标准合同条款进行数据的跨境传输，但缺乏系统性风险评估要求。Schrems Ⅱ案建立了“实质等同”测试机制，带来了三重革命性变化：一是 SCCs 不再是“勾选框”，法院明确要求，数据出口商必须逐案评估目的地国法律是否提供“实质等同”于欧盟的保护水平，引入传输影响评估（TIA）强制义务，要求记录目的地国监控法律、数据主体权利救济途径等；二是补充措施成为必选项，当目的地国法律可能破坏 SCCs 保护效果时，企业必须实施技术、合同或组织层面的补充措施，如客户管理的端到端加密（数据进口方无法解密），严格访问控制与审计日志；三是明确企业暂停义务，若补充措施仍无法确保保护水平，企业必须暂停或终止传输数据。因此，Schrems 系列案确立了一个重要原则：即便存在 SCCs 等保障措施，数据出口方仍需逐案评估接收国的法律环境，必要时采取补充保障措施。

基于 Schrems 系列里程碑案件，欧盟个人数据跨境流动从“安全港”到“隐私盾”的变化，是欧盟法院对美国数据保护水平的两次否定。从“安全港”到“隐私盾”再到“数据隐私框架”的演变过程表明，欧盟始终坚持其个人数据保护的基本权利标准，要求数据接收地不断调整其国内法律框架以寻求与欧盟对于个人数据的“实质等同”保护水平。欧盟个人数据跨境传输的制度演进，本质上是一部通过司法判例不断强化保护标准的历史。这一演进的核心线索，是欧盟对“实质等同”保护水平的坚持与具体化。

（二）从 Schrems 案到 TikTok 案：“实质等同”的全球化扩展

本案的一个关键事实是，TikTok Ireland 并未将欧盟用户数据物理传输至中国，而是中国员工通过远程方式访问存储在爱尔兰/新加坡的数据。DPC 认定 TikTok 中国员工远程访问欧洲用户数据的行为构成数据跨境传输，且 TikTok Ireland 未能证明中国的法律实践能够提供“实质等同”保护。TikTok Ireland 坚持辩称，数据仅存储在新加坡和美国服务器上，中国员工只是“远程访问”而非“接收”数据，因此不构成法律意义上的跨境传输。〔22〕2025 年 5 月 2 日，DPC 作

〔22〕 2025 年 4 月 TikTok Ireland 承认此前陈述不完全准确。自 2025 年 2 月发现，在部分情况下，确有 EEA 用户数据被存储在中国的两个数据库中。由于该问题披露较晚（在第 60 条机制四周时限届满后才确认），DPC 强调：本案裁定范围仅限于远程访问情形，不包括实际存储于中国服务器的情况；但 DPC 对 TikTok Ireland 提交虚假或不准确信息表示严重关切，后续将结合 EU 监管体系继续调查。参见《重罚 5.3 亿欧元后，爱尔兰又对 TikTok 展开新调查》，载腾讯网，https://news.qq.com/rain/a/20250711A02KVU00，2025 年 7 月 11 日访问；In the matter of the General Data Protection Regulation，DPC Case Reference：IN-21－9－2，30 April 2025.

出了对其处以 5.3 亿欧元巨额罚款的决定，并责令其在六个月内停止向中国传输欧盟用户数据。〔23〕本次处罚主要针对 TikTok Ireland 的以下两项核心违规行为：

第一，跨境数据传输缺乏合法性基础（违反 GDPR 第 46 条第 1 款）。DPC 认定，TikTok Ireland 在长达近三年的时间里，允许其中国员工远程访问存储于新加坡和美国服务器上的欧盟用户数据，这构成了数据向中国境内的传输。尽管 TikTok Ireland 采用了 SCCs 的方式并实施了加密等技术措施（例如其“三叶草项目”中的安全措施），但其未能充分评估并证明，在中国法律框架下，这些数据在实际处理时能获得与欧盟标准“实质等同”的保护水平。由于未能履行这一关键的评估义务，此违规行为被处以 4.85 亿欧元的罚款。

第二，未履行透明性义务、侵犯用户知情权（违反 GDPR 第 13 条第 1 款 f 项）。DPC 调查发现，在 2020 年 7 月至 2022 年 12 月期间，TikTok Ireland 的隐私政策存在重大瑕疵。它既未明确告知欧盟用户其个人数据可能被传输至中国，也未清晰说明位于中国的员工能够远程访问存储于境外服务器上的数据。直到 2022 年 12 月更新隐私政策后，TikTok Ireland 才增加了相关披露。DPC 评估认为此后的隐私政策已符合透明度要求，但针对此前的透明度缺失问题，DPC 处以了 0.45 亿欧元的罚款。〔24〕

DPC 对 TikTok Ireland 上述两种违规行为的处罚，涉及了本案需要解决的三个核心问题：〔25〕TikTok Ireland 是否履行了根据 GDPR 46 条第 1 款的义务，评估中国法律与实践是否能提供等效保护水平；TikTok Ireland 及中国字节跳动集团公司实施的技术、合同、组织措施是否足以确保“实质等同”的保障；TikTok Ireland 是否违反 GDPR 第 13 条第 1 款（f）项透明度的要求，即未充分告知 EEA 用户数据被远程访问或传输至中国的情况。上述问题将在接下来论文的第四部分得到解答。

Schrems 系列判例奠定了欧盟数据跨境传输的基本逻辑。在 2015 年的 Schrems Ⅰ案中，欧盟法院否定了安全港框架的有效性，确立了欧盟数据保护标准不可因跨境传输而被削弱的基本原则。在 2020 年的 Schrems Ⅱ案中，欧盟法院进一步明确，即使采用 SCCs，数据出口方也必须逐案评估第三国的法律实践，确保数据主体获得与欧盟“实质等同”的保护水平。这一判决的核心贡献在于，它将合规关注点从合同文本转向了目的地国的法律环境与实践。TikTok 案仍是这一演进路径的延伸，首次将 Schrems Ⅱ的逻辑系统性地应用于中国，确立了“远程访问＝数据传输”原则。但仅从 DPC 对 TikTok Ireland 两种违法行为的认定和涉及的三个核心合规问题来看，欧盟以 GDPR 为核心构建的跨境传输机制，在“数据主权”理念强化与地缘政治博弈加深的背景下，正从注重“充分性保护”的技术合规，转向强调“实质等同”的监管权力延伸。

〔23〕 See In the matter of the General Data Protection Regulation, DPC Case Reference: IN-21－9－2, 30 April 2025.

〔24〕 参见王珂盈、张天悦、刘祉良：《Tiktok 因“违反”欧盟 GDPR 被爱尔兰重罚 5.3 亿欧元》，载微信公众号“欧盟中国商会 CCCEU”2025 年 5 月 3 日。

〔25〕 See In the matter of the General Data Protection Regulation, DPC Case Reference: IN-21－9－2, 30 April 2025.

四、监管扩张：TikTok 案中的法律发现与规则重构

TikTok 全球运营引发的数据跨境传输争议，是数字经济时代个人数据保护与国家主权、国际贸易规则激烈碰撞的典型案例。本案折射出数据作为新型生产要素在跨境流动中的法律困境，即各国数据保护主义政策与全球数字贸易自由化需求之间的深层矛盾。结合 DPC 对 TikTok Ireland 的个人数据跨境传输审查，我们得以透视欧盟对数据跨境传输监管扩张的具体维度，即在本案中提出的“新标准”是什么。

（一）管辖范围的扩张：从“存储地”到“访问地”

GDPR 第 4 条第 2 款对“处理”进行了概念界定，〔26〕处理是针对个人数据的任何一项或一系列操作，如收集、记录、组织、建构、存储、修改、检索、咨询、使用、披露、传播或其他方式利用、排列、组合、限制、删除或销毁，无论该等操作是否采用自动化方式。从这个条款可以看出，GDPR 对“处理”的定义具有以下几个关键特点：第一，定义宽泛。该定义采用了“任何一项操作或一系列操作”的表述，并紧接着用“例如”列举了 15 种具体操作。这种“总括＋非穷尽列举”的结构意味着，任何对个人数据施加影响的行为，几乎都可以被认定为“处理”。这确保了 GDPR 的适用范围能够跟上技术发展的步伐，覆盖未来可能出现的新型数据处理方式。第二，技术中立。定义明确指出“无论是否通过自动化方式”。这意味着，无论是通过计算机系统自动完成的处理（如算法推荐、大数据分析），还是通过人工手动进行的操作（如纸质档案的查阅、整理），都属于 GDPR 规制的范围。第三，覆盖数据全生命周期。从定义中列举的操作可以看出，“处理”涵盖了个人数据的整个生命周期——从初始阶段到终结阶段。

TikTok Ireland 从存储位置和访问链路上对欧盟个人数据进行了隔离措施。（1）存储位置。如前所述，TikTok Ireland 在法律上主要是依赖 SCCs 的官方合同模板，作为其将欧洲用户数据合法转移到中国进行处理的法律途径。在 2010 版 SCCs 下，EEA 用户个人数据不在中国境内存储，相关服务器位于新加坡和美国。在实施 2021 版 SCCs 后，EEA 用户个人数据的服务器存储地继续不在中国境内存储，在既有存储地美国、新加坡的基础上，自 2023 年 5 月 1 日起引入马来西亚的托管/数据中心以承载相关处理（第三方服务商机房）。（2）访问链路。使用 2010 版 SCCs 规则时，TikTok Ireland 直接与多达 26 家中国关联公司签约，允许它们的员工远程登录到新加坡、美国等地的服务器，以处理欧洲用户的个人数据。为了防止数据被随意查看，TikTok Ireland 设置了严格的管理措施：第一，限人，只有经过审批的特定员工才能访问；第二，限时，每次访问权限的有效期最长不超过 12 个月；第三，限权，遵循“最小权限”原则，即员工只能访问其工作绝对需要的数据。升级为 2021 版 SCCs 规则后，TikTok Ireland 不再直接与所有中国公司签约，而是只指定一家主要的中国公司（北京字节跳动）作为总负责。欧洲数据先传给这家

〔26〕 GDPR 第 4 条第 2 款的原文为：‘processing’ means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction。

公司，再由它分派给其他 15 家中国关联公司去处理。之前设置的严格访问控制措施（如限人、限时、限权）保持不变，但对审批流程中的一些具体职责分工做了微调。

因此，TikTok Ireland 在本案中主张，欧洲用户数据存储在新加坡、美国等地的服务器上，中国员工仅是“远程访问”，并未将数据存储于中国境内，因此不构成跨境传输。DPC 则明确驳斥了这一观点：只要位于第三国的人员在访问过程中于本地设备上形成数据副本（包括缓存），就构成 GDPR 第 4 条所定义的“数据处理”，进而构成跨境传输。这一认定的深远影响在于，它将合规的关注点从“数据存储在哪里”转向了“谁能在哪里访问数据”，数据服务器的物理位置不再是决定性因素，能够访问数据的人员所在地才是。

当中国员工在其位于中国境内的电脑上登录系统，查看、分析、使用欧洲用户的个人数据时，这个“咨询”（consultation）行为就构成了在中国境内对个人数据的“处理”。因此，DPC 认定，这构成了欧盟数据向中国的跨境传输，必须遵守 GDPR 第五章关于数据跨境传输的规定。且通过本案，远程访问并形成本地缓存即构成“跨境传输”。DPC 将 GDPR 第 4 条关于“处理”的定义进行了扩大化解释。这一解释对全球化的 IT 架构（如离岸研发、全球运维中心）的根本性冲击在于，数据服务器的物理位置不再是“避风港”，人员的地理位置成为新的监管锚点。

（二）审查深度的扩张：从“合同约束”到“国家权力审查”

GDPR 第 44 条为一般原则性规定，只有在符合该条例其他条款的前提下，且数据控制者和处理者遵守 GDPR 第五章规定的条件时，才可向第三国传输个人数据。〔27〕GDPR 第 45 条规定了基于充分性决定上的跨境传输，当第三国被欧盟委员会认定为存在充分保护水平时，即在“白名单上”的国家，可向该第三国自由传输个人数据。当然，对那些未能确保达到该条所规定的充分保护水平的国家，并非绝对禁止将数据传输到境外。根据 GDPR 第 46 条第 1 款的规定，当不存在充分性决定时，在提供适当保障措施的情况下，可向第三国传输个人数据。〔28〕措施之一便是该条第 2 款（c）项的规定，欧盟委员会根据 GDPR 第 93 条第 2 款所述审查程序通过的 SCCs。

TikTok Ireland 选择了 SCCs 作为跨境数据的传输途径，因此还需要符合 GDPR 第 46 条采用“适当保障措施”的要求。〔29〕在“Schrems Ⅱ”案中，〔30〕欧盟法院确定了一个原则，即通过 SCCs 进行数据跨境传输的，控制者或处理者仍需要确保目的地国家能够提供充分的保护水平。〔31〕欧盟委员会负责判定非欧盟国家是否具备充分的数据保护水平，即该国的数据保护框架

〔27〕 See Mahsa Shabani, *The Data Governance Act and the EU's Move towards Facilitating Data Sharing*, 17 Mol Syst Biol 1, 1 (2021).

〔28〕 参见〔波兰〕马里厄斯·克里奇斯托弗克：《欧盟个人数据保护制度：〈一般数据保护条例〉》，张韬略译，商务印书馆 2023 年版，第 347 页。

〔29〕 See Frances G. Burwell & Kenneth Propp, *Digital Sovereignty in Practice: The EU's Push to Shape the New Global Economy*, Atlantic Council (2022), https://www.jstor.org/stable/resrep44035.4, visited on 20 December 2025.

〔30〕 See Maximillian Schrems *v.* Data Protection Commissioner, Case C-362/14, Judgment of 6 October 2015 (ECLI: EU: C: 2015: 650)

〔31〕 See In the matter of the General Data Protection Regulation DPC Case Reference: IN-21-9-2 In the matter of TikTok Technology Limited (30 April 2025), para. 265.

是否与欧盟“实质等同”。〔32〕也就是说，TikTok Ireland 作为数据传输者，需要“核实”中国的法律和实践水平是否能给予 EEA 用户数据充分的保护水平。TikTok Ireland 提出，应由 DPC 而非企业承担评估第三国法律的责任。DPC 明确拒绝这一主张，强调数据出口方必须主动履行传输影响评估义务，这是数据跨境传输的前提而非后果。这一立场将举证责任牢固地置于企业一方，显示评估责任的不可转移性。

在评估过程中，涉及的一个核心法律问题是对公共机关获取个人数据的监管（regulation of public authority access）。为了让控制者或处理者评估是否提供了适当的保障措施，控制者或处理者必须首先评估（assess）第三国在传输方面的法律和保障措施，特别是关于公共当局获取数据的法律和措施。〔33〕TikTok Ireland 在对中国法律的评估结论中承认，中国法律对个人数据的保护水平与欧盟在事实上确实存在差异。TikTok Ireland 主要提供给 DPC 非官方英文翻译的中国《刑法》《刑事诉讼法》《国家情报法》《反间谍法》《反恐怖主义法》《网络安全法》《数据安全法》《个人信息保护法》等法律。TikTok Ireland 指出，中国《反恐怖主义法》第 18 条规定，电信业务经营者、互联网服务提供者应当为公安机关、国家安全机关依法防范、调查恐怖活动提供技术接口和解密等技术支持和协助。TikTok Ireland 对中国公共权力机构获取个人数据方面评估后得出的总体结论是，虽然中国法律规定的监控措施是有限制的，但中国政府对数据访问的控制并不像欧盟标准所要求的那样规范和明确。〔34〕但基于属地原则，TikTok Ireland 对此进行了辩解，认为法律中的重大差异不会削弱 SCCs 的有效性，因为“中国政府在法律上无权强迫组织和个人提供非存储在中国境内的数据”〔35〕。为此 TikTok Ireland 向欧盟提交了三份关键材料，包括中国学者专家意见以及律师事务所的研究报告，以证明在属地原则下，中国政府无法获取存储在中国境外的数据，并说明该抗辩具有中国国内法和国际法基础。〔36〕

而 DPC 对于 TikTok Ireland 对其履行的评估义务并不认可。DPC 在决定中将此类法律称为“有问题的法律”（the problematic laws）。〔37〕DPC 主要依据法治清晰性、必要性、独立监督、有效救济四个维度评估中国法律。DPC 认为，本案中的个人数据传输的现实情形是由位于中国管辖境内的人员远程访问，任何此类远程访问的必然后果是 EEA 用户数据会在中国境内的计算机信息系统/设备上被处理（即使原始存储在境外）。也就是说，虽然 TikTok Ireland 提供的证据能够说明中国无法获取到储存在境外的数据，但事实上，中国计算机可以“远程访问”EEA 用户数据。TikTok Ireland 没有说明在远程访问的背景下，中国“有问题的法律”是否适用以及适用程度，从而导致存在着中国公共机构获取 EEA 用户数据的风险。因此，TikTok Ireland 违反了 GDPR 第 46 条第 1 款提供适当保障措施的要求。

---

〔32〕 See Neha Mishra, *International Trade Law and Global Data Governance Aligning Perspectives and Practices*, Bloomsbury Publishing Plc, 2024, p. 32.

〔33〕 See In the matter of the General Data Protection Regulation DPC Case Reference: IN-21-9-2 In the matter of TikTok Technology Limited (30 April 2025), p. 44, para. 256.

〔34〕 Ibid., p. 44, para. 305.

〔35〕 Ibid., p. 44, para. 311.

〔36〕 Ibid., p. 44, para. 372.

〔37〕 Ibid., p. 44, para. 311.

这充分说明，通过 TikTok 案，欧盟将个人数据跨境传输的审查深度从“合同约束”到“国家权力审查”进行了扩张，传输影响评估必须延伸至对目的法律与实际执行情况的审查，企业作为私法主体需承担“举证责任倒置”的义务，被要求承担证明本国公权力运行模式的合规性。企业合规评估的重点已从约束合同相对方扩展到审查目的地国的公权力访问制度。

（三）措施标准的扩张：从“技术加密”到“权限隔离”

Schrems Ⅱ判决说明，依据 GDPR 第 46 条第 2 款规定，SCCs 途径可构成向第三国数据传输时的一种适当保障措施的形式。但欧洲法院也指出，SCCs 仅对欧盟内的控制者与第三国接收方有约束力，并不能约束第三国公共机关。〔38〕因此，是否仅凭 SCCs 即可实际确保有效保护，取决于接收国的法律与实践。存在如第三国法律允许其公共机关干预数据主体权利的情形，仅凭 SCCs 并不足以在实践中确保有效保护。〔39〕于是，若 SCCs 无法提供所需保护、无法弥补第三国的保护不足，就必须考虑是否存在可弥补该不足的补充措施。补充措施必须真正“弥补”第三国法律保护的不足，不能只是“减轻”“降低风险”，而是要达到与欧盟“实质等同”的保护水准。〔40〕

针对这一问题，TikTok Ireland 实施了技术、合同、组织等补充措施以确保“实质等同”的保护水平。第一，远程访问链路采取的技术措施。在系统进入控制方面，对与本案远程访问 EEA 用户数据相关的系统，设置了若干入网/进入控制。在加密方面，传输中与内部访问对在途的 EEA 用户数据进行加密，用于内部系统访问以及远程访问内部 IT 系统亦采用了相应的加密/通道防护机制，存储/数据要素层面对若干数据要素使用加密，远程访问时的数据形态存在“加密/伪匿名/明文”三种形态。在访问控制方面，对中国字节跳动集团的远程访问实行分层审批与最小权限原则，并通过日志机制进行访问认证/追踪。数据按敏感度分级，级别越高审批越严；授权逐案授予，基于已证明的业务必要性。相关审批与权限管理政策文件已提交并区分 2010 版与 2021 版 SCCs 阶段。第二，合同措施。对于 2020 年集团内协议（对应 2010 版 SCCs），TikTok Ireland 认为仅靠 2010 版 SCCs 不能确保“实质等同”，因此在集团内协议中加入了若干补充合同条款（例如明确 SCCs 优先条款以强化 2010 版 SCCs 第 10 条的效力），并辅以外部云厂商合同义务与员工保密义务，此等合同上的措施被认为与技术/组织措施合并后可以达到保护目标。第三，组织措施。通过内部审计与风控团队对若干与本案相关政策进行审计，同时企业重申不向中国其他字节系公司（含今日头条、抖音）共享 EEA 用户数据以供其产品使用。企业设置执法响应团队（LERT），对各法域的公权力请求进行合法性与内控合规性审查；同时就 LERT 流程开展内部培训，并与 Europol/Interpol 等外部机构保持沟通。当然，不存在其他组织措施。

DPC 需要判断 TikTok Ireland 是否已经验证并能够证明，其与中国的集团公司为支持远程访问所实施的补充措施，连同 2010 版与 2021 版 SCCs，一并足以确保 EEA 用户获得 GDPR 第 46 条第 1 款与第 46 条第 2 款（c）项所要求的适当保障、可执行权利与有效法律救济，使其个人

〔38〕 See Data Protection Commissioner *v*. Facebook Ireland Ltd and Maximillian Schrems, Case C－311/18, judgment of 16 July 2020 (ECLI: EU: C: 2020: 559), para. 125.

〔39〕 Ibid., para. 126.

〔40〕 See European Data Protection Board (EDPB), Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (18 June 2021), p. 21.

数据获得与欧盟境内实质等同的保护水平。如前所述，DPC 已认定 TikTok Ireland 未能充分评估中国法律与实践对所涉 EEA 用户数据保护水平的影响。这一缺陷不仅直接影响其选择恰当保障与补充措施的能力，也阻断了其验证、保证与证明“实质等同”保护的可能。

在作出上述前提性判断后，DPC 谨慎审查了 TikTok Ireland 已实施的全部补充措施（技术、合同与组织）。DPC 认为，合同性补充措施不能用来对抗第三国公共机关在“问题性法律”支撑下对个人数据的可能访问，组织性措施同样无法克服此类在“问题性法律”支持下发生的公共机关访问。换言之，这类措施不能弥补因第三国存在“问题性法律”而导致的保护缺口。

尽管 TikTok Ireland 采取了加密、访问控制、合同承诺等技术性和组织性措施，但是 DPC 认定这些措施无效，理由是中国员工为履行工作职责需要访问明文数据，一旦数据以明文形式出现在中国境内，就完全暴露于当地法律的风险之下；而合同措施对政府权力没有约束力。这表明，如果访问权限本身存在风险，技术加密便形同虚设。欧盟监管要求的是从物理和逻辑上将高风险国家的人员与数据彻底隔离，这直接触及了企业的核心运营架构。这一认定传递的信息是补充措施需达到实质性要求。补充措施必须能够从根本上解决访问权限问题，仅仅在既有架构上添加保护层是不够的。这一措施标准的扩张，实质上是从“技术加密”到“权限隔离”的扩张。

（四）透明义务的扩张：从“知情权”到“关键程序义务”

在跨境数据传输已成为企业运营常态的情况下，如何在促进数据自由流动与保护个人隐私之间取得平衡，成为各国立法者面临的重大挑战。GDPR 第 13 条第 1 款（f）项正是欧盟在这一背景下的制度创新，该条款要求数据控制者在直接从数据主体处收集与其相关的个人数据时，必须明确告知数据主体其向第三国或国际组织传输个人数据的意图，并披露是否存在欧盟委员会出具的关于该第三国或国际组织的数据保护水平充分性的决定。若涉及第 46 条、第 47 条或第 49 条第 1 款（b）项所述的传输情形，则应说明所采取的适当或合理保障措施，并向数据主体提供这些保障措施相关文件副本的获取方式或查询渠道。该条款确立了数据控制者在跨境数据传输中向数据主体提供其个人数据流向信息的义务，实质是保障数据主体的知情权。

GDPR 第 13 条第 1 款（f）项作为欧盟数据保护法律框架中的核心条款，在整个 GDPR 知情权保障体系中居于基础性地位。它通过强化透明度要求，确保数据主体能够在数据处理的最开始阶段充分了解其个人数据的跨境流向，从而实现对自身数据的有效控制。同时确保数据主体在数据处理的各阶段都能获得必要的信息，提升其对于数据跨境流动风险的认知和判断能力并有效行使数据保护权利。该条款项下的透明度义务具有特定适用条件：首先，数据控制者必须在“获得个人数据时”向数据主体提供相关信息，即不能在数据收集完成后再行告知，必须同步完成信息披露，这种即时性要求确保数据主体从一开始就知晓数据跨境流动的相关安排，能够在充分知情的基础上作出是否提供数据的决定。其次，该透明度要求仅适用于数据控制者直接从数据主体处收集数据的情形，如果数据是从其他来源（如公开渠道或第三方）获得的，则应适用第 14 条而非第 13 条的规定，即数据控制者应在获得数据后一个月内向数据主体提供信息。最后，义务主体是数据控制者，即决定处理目的和方式的实体。当存在联合控制者时，所有控制者都可能承担相应的告知义务，具体情况取决于他们在数据处理中的角色和责任。

在本案中，TikTok Ireland 提交声明称其已通过 SCCs 作为保障措施来进行对未列入白名单

国家的数据传输，而且 EEA 用户可以获得这些 SCCs 副本的查看途径，认为这些信息保障了 EEA 用户了解他们的个人数据是否被跨境传输、怎样被跨境传输。但 DPC 提出了相反意见并认定 TikTok Ireland 在 2021 年 10 月适用的隐私政策存在严重欠缺，〔41〕违反了该条款关于透明度义务的规定：一方面，隐私政策未明确接收国，在提及数据可能被共享到欧盟以外时，没有具体列明包括中国在内的关联第三国；另一方面，该政策未说明传输性质，未提及远程访问这一事实，EEA 用户不清楚数据共享包括中国员工远程访问其个人数据的情形。DPC 认定，这种不严谨的披露方式严重损害了 EEA 用户作为数据主体的知情权，针对该违法行为单独施加了 4500 万欧元罚款。DPC 强调，类似“数据可能传输至欧洲经济区以外”的含糊表述已不敷使用，必须指明具体国家、访问方式和原因。企业不能使用模糊措辞以逃避在数据跨境流动中应承担的责任，必须主动、具体地解释数据将如何传输以及传输至何处。

这一透明度的具体标准表明，GDPR 第 13 条第 1 款（f）项下的透明度义务的重要性将随着数字经济的深入发展和数据跨境流动的日益频繁而进一步凸显，只有在充分保障数据主体知情权的基础上，才能实现数据保护与数据流动的平衡，从而推动数字经济的健康发展。通过 TikTok 案，透明义务已成为一项关键程序义务，表明了欧盟监管机构对于极致透明度的立场：必须清晰、明确地告知用户数据将传至中国及远程访问的性质，模糊表述构成违规。

五、困境纾解：数字主权博弈下的中国企业合规之困

（一）中国企业的数据跨境传输合规困境

1. 数字主权博弈下的规则扩张

从管辖权域外延伸，到跨境传输机制的单边设定，欧盟通过 GDPR 体系持续推进其数据治理模式的全球化。这一过程表面上是法律技术的输出与合规争议，实质则映射出数字时代的主权博弈。欧盟以基本权利保护为旗帜，通过“充分性认定”等工具，将他国数据治理体系置于其标准审查之下，从而在规则层面争夺数字空间的主导权。〔42〕TikTok 等一系列案件表明，企业合规困境背后往往是欧盟与第三国在数据主权上的根本冲突。TikTok 处罚案并非孤立事件，而是欧盟将其凭借 GDPR 所构建的个人数据监管体系和治理模式推向全球、争夺数字时代规则制定主导权的一个缩影。

其一，价值观与标准输出。欧盟将源于自身历史文化的“人格尊严”观念注入个人数据保护

〔41〕 TikTok Ireland 在调查期间更新了隐私政策，并于 2022 年 12 月向 DPC 提交了新版 EEA 隐私政策。该政策明确指出了 EEA 用户数据传输的目的地国家，并告知 EEA 用户其个人数据存储在美国和新加坡的服务器上，并可能被位于巴西、中国、马来西亚、菲律宾、新加坡和美国的 TikTok 集团实体通过远程方式访问。DPC 评估认为 TikTok Ireland 2022 年 12 月版 EEA 隐私政策符合 GDPR 第 13 条第 1 款（f）项的要求，因此认定 TikTok Ireland 违反该条款的时间范围为 2020 年 7 月 29 日至 2022 年 12 月 1 日。参见：《TikTok 因向中国传输个人数据被处以 5.3 亿欧元罚款》，载安全内参，https://www.secrss.com/articles/78361，2025 年 12 月 26 日访问。

〔42〕 参见史丹、聂新伟、齐飞：《数字经济全球化：技术竞争、规则博弈与中国选择》，载《管理世界》2023 年第 9 期，第 9－10 页；叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察》，载《法学评论》2020 年第 1 期，第 115 页。

制度，并将其包装为具有普遍意义的“基本权利”。〔43〕通过 GDPR 的域外适用和跨境传输机制，欧盟实际上是在全球推行一套以欧洲价值观为基础的数据治理“文明标准”，并演变为在数字时代以“数据保护水平”作为衡量他国是否值得信赖、能否进行数据往来的标尺。欧盟更借助于长臂管辖机制，不仅强化了其域内数据保护标准，而且通过制度输出将“欧盟标准”逐步塑造为全球数据治理的“黄金标准”。〔44〕2022 年《欧盟标准化战略：制定全球标准，支持一个有弹性、绿色和数字化的欧洲单一市场》更明确将自身定位为“全球标准制定者”，意图通过标准设定塑造符合其价值观的国际数字秩序。〔45〕

其二，经济秩序与规则主导权争夺。数据是数字经济的核心生产要素。谁掌握了数据流动的规则制定权，谁就能塑造全球数字经济的运行秩序。〔46〕欧盟通过 GDPR，实质上建立了一个以欧洲市场准入为筹码、以合规要求为手段的规则权力体系。它迫使跨国企业调整其全球数据处理流程，并影响着第三国为获得“充分性认定”或便利企业合规而向欧盟标准靠拢。这使欧盟得以在产业实力不占优的情况下，依然占据全球数据治理的关键地位。

其三，安全自主性保障。GDPR 的严格限制，特别是对未获充分性认定国家数据跨境传输的严苛审查（如 Schrems Ⅱ案所确立的原则〔47〕），直接回应了第三国监控带来的安全威胁。这不仅是保护个人隐私，更是捍卫欧盟的“数字主权”与战略自主性，减少在数据层面对他国的依赖。TikTok 案中对数据可能流向中国并受其法律管辖的担忧，以及 Schrems 案中对防范美国政府访问个人数据及对个人的监控，正是这一安全逻辑在司法和执法层面的直接体现，核心目的是保障欧盟的自主性。

总之，欧盟个人数据跨境传输规则的扩张，不仅是法律规范的延伸，更是其构建数字主权、影响全球数字秩序的战略体现。在日益激烈的国际数据竞争中，这种以规则为载体的主权争夺，将继续深刻塑造全球数据流动的路径与边界，也为全球性企业的跨境数据流动带来合规方面的巨大压力。

2. 中国企业的合规问题

从 TikTok 案可以清晰地看到，欧盟个人数据流动监管正经历一场深刻的扩张。这种扩张不是单一维度的，而是从地域、行为、审查深度到补充措施的全面进化。对中国企业而言，这种扩张直接转化为一系列具体的合规困境。

第一，在地域管辖的扩张下，TikTok 案确立了一个核心规则：即便数据存储在欧洲或第三地，只要位于中国的人员通过远程访问在欧洲以外的设备上形成了数据副本，就构成数据跨境传

〔43〕 参见叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟 GDPR 的原旨主义考察》，载《法学评论》2020 年第 1 期，第 115 页。

〔44〕 参见高戈：《个人数据跨境流动的欧盟立场：不可谈判的人权议题?》，载《人权研究（辑刊）》2024 年第 2 期，第 188 页。

〔45〕 See European Commission, An EU Strategy on Standardisation Setting Global Standards in Support of a Resilient, Green and Digital EU Single Market, COM (2022) 31 final, Feb., 02, 2022, pp. 5 - 7.

〔46〕 参见孙方江：《跨境数据流动：数字经济下的全球博弈与中国选择》，载《西南金融》2021 年第 1 期，第 6 页。

〔47〕 See Data Protection Commissioner *v.* Facebook Ireland and Maximillian Schrems (Schrems Ⅱ), Court of Justice of the European Union, CJEU Case C - 311/18, Judgment, Jul., 16, 2020, para. 192.

输。从“存储地”到“访问地”的转变意味着，合规焦点从“数据存在哪”转向了“谁能访问它”。监管的触角因此延伸至任何能访问欧盟数据的角落。

第二，在行为认定的扩张下，TikTok 案则将“远程访问”明确纳入传输范畴。以往，跨境传输主要指主动的数据发送。从“主动传输”到“被动访问”的转变，对依赖全球研发或运维团队的中国企业冲击巨大，因为访问行为本身，就成了监管对象。另外，TikTok 案表明，欧盟监管机构对透明度的要求极高，数据传输者必须指明数据传输的具体国家（如中国）、访问原因和方式。但对中国企业而言，过于具体的披露可能引发舆论或政治风险；若不披露，则直接面临巨额罚款。这种“过载”的透明度要求，也让企业背上沉重的负担。

第三，在审查维度的扩张下，监管审查已超越双方合同，深入到目的地国的公权力法律环境。在 TikTok 案中，DPC 依据法治清晰性、必要性与比例性、独立监督、有效救济四个维度，对中国法律进行了严格评估。从“合同约束”到“国家权力”的转变，意味着企业不仅要约束自己和合作伙伴，还要承担证明本国法律环境“安全”的重任。企业需要证明目的地国法律能提供“实质等同”保护。但作为一个企业，要论证中国《反恐怖主义法》《网络安全法》《数据出境安全评估办法》等公权力调取数据的制度，是否符合欧盟“清晰、必要、可救济”的标准，难度极高。

第四，在措施标准的扩张下，DPC 认定 TikTok 的技术措施无效，因为员工为履职必须访问明文数据。如果访问权限本身存在风险，技术加密便形同虚设。从“技术加密”到“权限隔离”的转变表明，欧盟监管要求的是从物理和逻辑上将高风险国家的人员与数据彻底隔离，这直接触及了企业的核心运营架构。访问权限往往与业务运营发生冲突，为了实现“权限隔离”，最直接的方式是不让中国员工访问欧盟数据。但这意味着如果将欧盟业务的研发、运维支持完全剥离，可能导致效率下降和成本上升。如何在不牺牲核心运营能力的前提下满足监管要求，也是一个难题。

（二）中国企业的合规应对

从 Schrems 案到 TikTok 案，欧盟个人数据跨境传输制度正经历深刻演进。这一演进的核心逻辑始终如一：无论数据流向何方，欧盟公民的数据保护权利必须得到“实质等同”的保障。TikTok 案的意义不仅在于其对中国企业的警示，更在于它完整呈现了欧盟监管机构的审查逻辑和证明标准，未来任何涉及向“高风险”第三国传输数据的企业，都必须以此为镜，重新审视自身的合规架构。中国企业应在充分理解欧盟规则深层逻辑的基础上，结合自身发展阶段与数字经济发展阶段，在制度、机制和技术方面入手，主动建立合规与风险防范框架，形成兼具韧性与主动性的应对体系。

第一，在制度层面，企业需重点关注欧盟数据跨境传输的法律基础与合规要求。TikTok 案对中国企业的启示是多维度的，每一项数据传输都必须在事实准确、论证充分的基础上构建合规体系。其一，企业必须清晰识别所有数据跨境传输场景，包括“远程访问”这类容易被忽视的情形，技术细节如本地缓存、访问日志等都可能成为监管审查的重点。数据本地化不足以隔离风险。将数据存储于欧洲或新加坡而将访问权限保留在中国境内，这一模式已被证明存在根本性风险。真正的数据本地化要求本地化的运营控制，以及通过技术手段将访问权限与高风险第三国人

员有效隔离。对于核心的欧盟用户数据，可考虑建立真正独立的运营体系。例如，在欧盟本地组建独立的管理与技术支持团队，将数据访问权限与包括中国在内的其他地区进行物理和逻辑上的双重隔离，从根本上消除“远程访问”风险。其二，传输影响评估必须深入具体。TIA 不能流于形式，必须结合具体传输场景评估目的地国法律实践，识别风险并针对性地设计补充措施。特别需要关注公权力访问制度的清晰性、独立监督和救济途径。评估应尽可能获取目的地国法律专家的独立意见，因为 DPC 在 TikTok 案中明确将中国法律作为“事实问题”对待，对当地专家的意见给予更高权重。其三，补充措施必须针对性解决识别出的风险。如果评估发现风险，须设计能够实际应对这些风险的措施。对于涉及中国员工访问的场景，可能需要考虑“零知识”架构、由欧盟实体独家持有解密密钥等技术安排，尽管这可能与需要明文访问的业务操作存在冲突。其四，透明度必须具体明确。隐私政策必须具体指明数据传输的目的地国、访问方式和原因，含糊其词的表述将面临处罚风险。其五，主动与欧盟监管机构对话。例如在进行充分性认定时，如果传输影响评估揭示出无法自行解决的高风险，企业应依据 GDPR 第 36 条启动事前咨询，向欧盟监管机构寻求共同解决方案的可行性。

第二，在机制层面，需完善企业内部数据合规控制体系。企业可以在内部设立专门的数据保护部门，负责对包括数据跨境流动在内的所有数据处理活动进行监督管理，例如 GDPR 数据保护官（data protection officer，DPO）的要求。欧盟的监管实践表明，数据保护已不仅是法律问题，更是涉及市场准入、商业信誉和全球化运营的核心战略问题。中国企业可借鉴“约束性公司规则”（BCRs）等机制，建立集团内部统一且经欧盟监管机构认可的数据保护标准，将合规优势转化为市场竞争优势。此外，构建中国法律环境的“专家证据链”也是合规机制的重中之重。例如，面对 DPC 在 TikTok 案中强调中国法律是“问题性法律”，企业应当联合中国法学专家、涉外律师，就具体数据传输场景下的法律风险出具权威、翔实的法律意见书，构建有效的抗辩证据链，以完成企业举证本国法律环境的任务。

第三，在技术层面，需强化技术性投入与本地化运营。欧盟对违规跨境数据流动的处罚高昂，企业可将此预期成本纳入合规预算，通过加大技术投入、推进数据运营本地化等方式提升合规能力。例如，为增强隐私保护，探讨“可用不可见”技术（如隐私计算、联邦学习、同态加密）用来解决“访问权限”与“数据保护”冲突问题的可能性。当技术能够确保访问者“看见的是密文、算不出明文”时，即可将“高风险的人员访问”转化为“低风险的数据处理”，从而在技术上实现“隔离”效果，满足监管的“有效性”要求。

六、结　论

在数字经济背景下，个人数据跨境传输已成为涉外法治领域的重要议题。欧盟通过 GDPR 构建了以“实质等同”保护为核心的跨境数据监管体系，并借助严格的合规要求与高额处罚机制，对全球数字平台企业产生了显著的规则外溢效应。TikTok 案作为欧盟首次系统性审查涉中国法律环境下数据跨境传输合规性的典型案例，集中体现了这一制度运行逻辑。

通过对 TikTok 案的分析可以发现，欧盟监管机构在适用 GDPR 第五章时，已明确将远程访

问型数据处理纳入“跨境传输”的规制范围，并强调数据在第三国法律与实践环境中是否能够持续获得与欧盟“实质等同”的保护水平。SCCs 不再具有当然的合规效力，而是必须辅以充分的传输影响评估与有效的补充性措施。

从更宏观的视角看，欧盟个人数据跨境传输制度不仅是个人权利保护的法律工具，也承载着规则输出与数字主权维护的战略功能。其设定高标准的数据保护门槛，意在重塑全球企业的数据治理结构，并在数字时代的规则竞争中占据重要位置。对我国而言，TikTok 案揭示了我国企业在参与欧盟市场时面临的合规挑战。欧盟以“实质等同”保护为法律工具，将跨境数据流动问题从商业合规提升至基本人权与制度审查层面，迫使企业为第三国法律风险承担责任，反映了“布鲁塞尔效应”下规则单边外溢与地缘博弈的实质。从企业微观角度看，合规的实质在于中国企业如何寻求合法的博弈空间和应对策略，在现有法律框架下如何通过制度、机制和技术等层面的改进来寻找“求生之道”。

Abstract: Against the backdrop of global digitization and geopolitical competition, cross-border transmission of personal data has become a core issue in international economic and trade exchanges and foreign-related rule of law. In 2025, the Irish Data Protection Commission (DPC) imposed a huge penalty on Chinese company TikTok. It is necessary to analyze the application logic, expansion path, and the essence of digital sovereignty game behind the personal data cross-border transfer rules under the GDPR framework, revealing that the EU has built a strict cross-border data governance system with “essentially equivalent protection” as its core through GDPR, and continuously expands its rule influence through judicial practice. This expansion is not a single dimension, but a comprehensive evolution from geography, behavior, censorship depth to supplementary measures. The expansion and application of these rules not only have a profound impact on the operation of global digital enterprises and the international data flow order, but also bring a series of compliance challenges for cross-border data transmission to Chinese enterprises. It is advised to solve the compliance issues of cross-border data transmission for Chinese enterprises from the perspectives of systems, mechanisms, and technologies.

Key Words: TikTok, cross-border data transfer, essentially equivalent protection, digital sovereignty, regulatory expansion

（责任编辑：朱晓峰）