

EO14117 监管框架下 中美跨境数据合规： 中国企业的影响与应对

敏于知

监管背景与企业影响：EO14117 在中美跨境数据监管中的定位

近年来，美国以国家安全为核心，系统性重构其跨境数据监管体系。在这一背景下，2024年2月底签署的第14117号行政命令（Executive Order 14117，“EO14117”）成为当前中美跨境数据监管框架中的关键制度支点。

与以个人隐私权保护为中心的传统数据保护立法不同，EO14117明确将监管重点转向数据在规模化聚合、算法分析及推断应用过程中可能引发的国家安全风险，并据此建立针对特定国家与主体的数据交易限制机制，旨在防止受关注国家获取或利用与可识别美国自然人相关的批量敏感个人数据，以及具有国家安全敏感性的美国政府相关数据。

为落实 EO14117 的监管要求，美国司法部随后发布并实施《最终规则》（Final Rule），对受监管数据、交易类型及相关合规义务作出具体规定。自 2025 年 4 月 8 日《最终规则》正式生效以来，随着监管制度全面落地，监管关注点已从企业是否理解相关规则，逐步转向企业是否已经建立并持续运行可审计、可验证的合规机制。

在此背景下，EO14117 的影响正从监管政策层面逐步传导至企业的市场合作与业务运营环境。美国企业、云服务商、技术合作方及金融机构，正在将相关风险纳入合作前的尽职调查与合规评估，并相应收紧数据访问、技术支持及跨境协作安排。对于涉及跨境数据访问或数据密集型业务的企业而言，相关要求已逐渐转化为现实的合规与运营压力。未能建立系统性、可审计的合规机制，可能不仅带来监管风险，还可能在商业合作、供应链稳定性及市场信誉层面产生连锁影响。

EO14117 合规必要性

	美国企业正在主动限制中国访问 为降低 EO14117 合规责任，越来越多的美国机构开始限制或阻断中国用户对美国系统、平台和 API 的访问，已对业务运营和协作造成实质性影响。 » 若缺乏基于业务场景的合规规划，企业将持续面临突发性访问中断。		EO14117 覆盖的数据范围远超企业普遍预期 技术数据、行为数据、位置数据，即便已匿名化或聚合，只要存在再识别可能，仍可能被纳入监管；部分 AI 输出数据亦在范围之内。 » 许多企业低估了其日常业务中涉及的美敏感数据规模。
	合作伙伴加强尽职调查并要求合规证明 全球合作伙伴正日益要求确认不存在受监管的数据交易。若企业无法提供充分的合规证据，可能导致系统集成暂停或服务中止。 » 无法证明合规的企业将被视为高风险合作对象。		内部协同不足削弱合规落地能力 IT、法务、合规、采购及业务团队之间缺乏协同，容易在访问控制、数据管理及第三方尽调方面形成漏洞。 » 缺乏跨职能治理，企业将难以形成可信的 EO14117 合规证据链。
	监管“连锁反应”导致海外客户收缩合作 美国监管要求正在通过国际供应链向外传导，促使第三国客户为规避风险而减少或终止合作。 » 任何涉及美国数据的业务链条，都可能引发对中国实体的合作限制。		监管执法与合规审查持续强化 监管机构持续关注受关注国家及相关交易安排。若未能建立清晰的合规判断与控制机制，可能面临更高的执法与监管风险。 » 延迟开展数据梳理与控制措施实施，将显著提升执法风险。

在具体适用过程中，EO14117 的监管并非简单以单一因素作出判断，而是通过分步骤的分析路径展开。企业通常需要先识别业务中可能触发监管关注的高风险场景，再结合主体身份、数据类型及相关交易安排进行具体判断，以确定是否落入《最终规则》的适用范围，并据此承担相应的合规义务或限制要求。

常见高风险业务场景：EO14117 对中国企业运营的现实影响

在实践中，生命科学与生物医药、云服务与 IT 外包、金融科技以及 AI 模型训练等数据密集型行业，通常更容易触发相关监管关注。部分中国企业已在日常运营中感受到相关影响，例如跨境系统访问被收紧、全球统一平台调整、跨区域协作复杂度上升等。这些变化本身并非合规判断的结论，而是 EO14117 风险被触发后，在组织与技术层面产生的外在表现。

EO14117 下的高风险业务场景

EO14117 的监管判断并不以是否发生数据出境为唯一标准，而是聚焦于相关业务活动是否可能使受关注国家或受控主体直接或间接获取受监管数据。在执法与合规评估实践中，下列业务活动通常更容易被视为高风险场景：



对企业运营的实质性影响

一旦高风险业务场景被纳入 EO14117 的监管视野，其影响通常将从具体业务或单一系统，上升为企业层面的治理与运营问题，主要体现在：

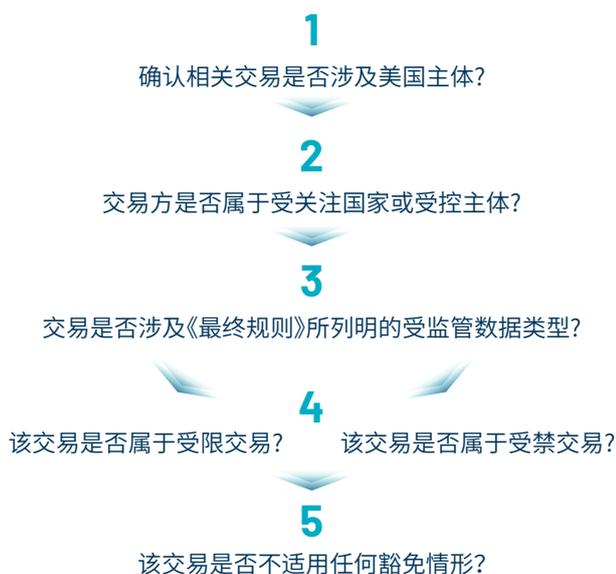
- **系统架构层面：**全球统一 IT、数据或研发平台是否仍具合规可行性；
- **协作模式层面：**跨区域协作是否存在明确、可执行的合规前提与边界；
- **运营模式层面：**集中化 IT 运维、数据分析及技术支持模式是否可持续；
- **业务连续性层面：**技术支持、研发协作与项目交付节奏是否受到实质影响。

在缺乏清晰合规判断与可行替代方案的情况下，企业往往只能采取高度保守的限制措施，从而在无意中放大 EO14117 对运营效率与业务稳定性的冲击。

适用范围与关键定义： EO14117 的监管判断框架

在识别高风险业务场景的基础上，企业还需进一步判断相关业务是否落入《最终规则》的监管范围。EO14117 的适用并不以企业注册地或国籍作为单一判断标准，而是通过对**主体属性、交易对手、数据类型、交易性质及豁免情形**的组合判断，来确定具体业务安排是否落入监管范围。

根据美国司法部发布的《最终规则》，企业在判断相关交易是否落入 EO14117 监管范围时，通常需要重点关注以下几个关键要素：



1 美国主体

“美国主体”是承担合规义务的责任主体，包括美国公民、合法永久居民、依据美国法律设立的实体，以及美国境内的个人或组织。在跨境业务实践中，中国企业在美设立的子公司、分支机构或在美国境内实际运营的关联实体，通常可能被认定为美国主体。

2 受关注国家与受控主体

《最终规则》列明特定国家为“受关注国家”，并通过“受控主体”概念，将股权控制、属地联系、雇佣关系及指定机制等因素纳入判断范围。因此，在评估交易结构时，企业不仅需要关注交易对手的注册地，还需结合其控制关系、人员安排及实际业务联系进行综合分析。

3 受监管数据类型

EO14117 主要监管两类数据：

- 批量敏感个人数据（如个人标识符、精确地理位置、生物识别、健康、财务及人类组学数据等）
- 美国政府相关数据（涉及政府人员或敏感政府区域的数据）

需要注意的是，即使数据经过去标识化或加密处理，如在技术或业务层面仍可被重新识别或关联，仍可能被认定为受监管数据。

4 交易分类

《最终规则》根据国家安全风险程度，对相关交易划分为：

- 受禁交易：如数据经纪活动或涉及批量人类组学数据的交易。
- 受限交易：包括供应商协议、雇佣协议或非被动投资安排等，在符合安全控制要求的前提下可能被允许继续存在。

具体交易分类需结合主体属性、数据类型及交易结构综合判断。

5 豁免情形

《最终规则》同时规定了若干豁免情形，例如为履行法定义务或司法程序所必需的数据处理，以及符合特定条件的被动投资等。豁免适用需严格符合规则文本，不得扩大解释。

上述定义及适用标准均来源于美国司法部发布的《最终规则》及相关配套文件，具体定义及适用细节请参考官方文档。

合规就绪评估与实践判断：EO14117 下中国企业的应对重点

从监管视角看，合规判断通常围绕几个核心问题展开：企业是否能够持续识别其业务中涉及受监管数据的场景；是否能够清晰、完整地说明数据在不同系统和业务环节中的流向、访问路径及相应的控制机制；以及是否能够通过制度设计、技术措施与审计证据，证明受关注国家或受控主体无法不当获取相关数据。

在这一背景下，合规就绪评估（Readiness Assessment）与定期审计逐渐成为企业管理 EO14117 风险的重要工具。其价值并不在于简单识别问题，而在于验证企业是否已经建立并实际运行一套可复核、可解释、可持续的合规机制。例如：是否形成清晰的方法论支持合规判断；技术与组织层面的控制措施是否嵌入业务流程；业务模式、人员或技术架构变化是否能够及时纳入合规评估；以及相关结论是否形成充分的文件化记录和证据支持，以应对监管审查或合作方尽职调查。

在实践中，有效应对 EO14117 并非依赖零散或临时性的合规措施，而需要一套结构化、可持续、且可被监管验证的治理路径。基于监管实践与审计经验，该路径通常可概括为三个相互衔接的关键步骤：识别、控制与审计。

三步构建可持续的 EO14117 合规体系

从一次性合规判断，升级为**可审计、可验证、可持续运行**的 EO14117 合规能力

1 识别

明确适用范围与业务影响边界

- 识别是否涉及美国主体及受控主体
- 界定受控系统 with 数据
- 梳理跨系统、跨地区、跨第三方的数据访问与流转路径
- 识别对业务运营产生影响的场景

2 控制

对标监管要求设计验证控制方案

- 对标美国司法部《最终规则》相关要求
- 识别控制缺口、执行偏差及对业务的实际影响
- 明确整改优先级、责任分工与实施路径
- 结合业务实际，设计合规前提下的替代方案与过渡安排

3 审计

形成可验证、可持续的合规机制

- 向管理层与关键干系人对齐合规判断与责任边界
- 建立合规状态可视化看板，支持管理决策
- 开展年度独立评估，验证控制设计与执行有效性
- 支持监管问询、合作方尽调及内部审计需求

达于行

甫瀚在 EO14117 合规领域的支持能力

围绕 EO14117 及其配套监管要求，甫瀚可从**战略、治理、控制与持续合规**多个层面，协助中国企业应对中美跨境数据监管带来的系统性影响。相关支持能力包括但不限于：

- **合规适用性与风险判断支持：**协助企业理解 EO14117 的适用边界，识别受监管主体、受监管数据及高风险业务场景，支持企业在复杂业务结构下作出一致、可解释的合规判断；
- **跨境数据与访问治理优化：**结合企业实际业务模式，协助设计和优化数据流转、访问控制、组织分工及第三方管理安排，使其符合 EO14117 的风险预期；
- **合规治理与管理机制建设：**支持企业建立覆盖法务、合规、网络安全、IT 及业务部门的协同治理机制，明确职责分工与决策流程，提升组织层面的合规成熟度；
- **合规准备与独立评估支持：**通过阶段性评估、管理层沟通及独立验证，协助企业检视现有控制措施的有效性，并持续应对监管审查、合作方尽调及年度合规要求；
- **持续合规与业务支持：**在企业业务调整、技术架构变化或跨境合作演进过程中，支持其持续更新合规判断，降低合规不确定性对业务连续性的影响。

通过上述支持，甫瀚可协助中国企业将 EO14117 的监管要求融入日常管理与业务决策之中，从被动应对合规风险，逐步转向可持续、可预期的跨境数据治理模式。在满足监管要求的同时，降低合规不确定性对跨境协作、技术运营及业务拓展的影响，从而提升跨境业务运营的稳定性与合作的可持续性。

关于甫瀚咨询

甫瀚咨询（上海）有限公司是一家具有全球视野的咨询机构。我们在中国开展业务至今已逾二十年，分别在上海、北京、深圳、成都和香港设有五个区域团队。依托甫瀚全球网络，我们能迅速汇聚甫瀚全球超过 25 个国家 90 个分支机构的资源与洞见，灵活调动更适合的专业团队为客户带来高质量的交付，并支持中国企业的海外拓展。

甫瀚咨询的业务遍及运营与财务管理绩效优化、风控与合规、内部审计、信息技术咨询、数字化转型，以及气候变化与可持续发展等领域。我们为中国各行业优秀企业、世界 500 强企业、全球各地资本市场的上市公司以及拟上市公司提供成熟及定制化的解决方案，亦为成长型企业提供陪伴式服务。

公司地址

北京

朝阳区建国门外大街 1 号
国贸写字楼 1 座 718 室
电话：(86.10) 8515 1233

上海

徐汇区虹桥路 1 号
港汇恒隆广场办公楼 1 座
2301+2310 室
电话：(86.21) 5153 6900

深圳

福田区中心四路 1 号
嘉里建设广场 1 座 1404 室
电话：(86.755) 2598 2086

成都

锦江区红星路三段 1 号
国际金融中心 1 号
办公楼 25 楼

香港

中环 干诺道中 41 号
盈置大厦 9 楼
电话：(852) 2238 0499

protiviti®
甫瀚

© 甫瀚咨询（上海）有限公司是 Protiviti 网络下的中国成员公司，Protiviti 网络由成立于全球各地的采用 Protiviti 名称独立经营的咨询公司组成。成员公司具有自主经营权，并非 Protiviti Inc. 或 Protiviti 网络下的其他公司的代理人，且并未获得使 Protiviti 网络下的其他公司承担义务或约束该等其他公司的授权。



关注甫瀚咨询
获取更多资讯