Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)



亚太数字经济与人工智能法律问答指南(蓝皮书)

Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

作者

序

目录

APEC数字经济总体环境

APEC数据保护与隐私法规

APEC跨境数据流动

APEC人工智能法律与监管

APEC算法治理与自动决策系统

APEC数字贸易
电子商务与平台经济

APEC网络安全与技术合规

APEC产业应用场景
制造业、IoT、电动车、跨境电商等

APEC知识产权与数字内容

亚太数字经济与人工智能法律问答指南(蓝皮书)

Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

编委会主任

李　岚　郑丹妮

执行主编

钟泳妍　章婉纯　吴冠辰　湛楚莹

编委会秘书 (按姓氏首字笔画排列)

王　丹　左李福　冷勇达　孟　昕　范晓荧　戴佳兵　傅　颉

韦　征　秦雨歌

编委会成员(按姓氏首字笔画排列)

王熙雨　王孝冉　王鹤臻　刘元兵　刘舒玮　何　杨　何　欣

李亚兵　李姿质　闵祥虎　沈晓雪　杨昊菲　张逸雯　叶晓君

郑子俊　徐银萍　牛誉翔　孙　霖　李佳芮　傅哲迅　薛　菁

蓝娅倩　陈瑜琪　陆雪儿　郭小萱

支持单位（特别鸣谢）(排名不分先后)

北京大成（深圳）律师事务所

北京高文（深圳）律师事务所

北京浩天（深圳）律师事务所

北京金诚同达（深圳）律师事务所

北京天达共和（深圳）律师事务所

北京瀛和（深圳）律师事务所

北京中银（深圳）律师事务所

北京市安理（深圳）律师事务所

北京市君泽君（深圳）律师事务所

北京市京师（深圳）律师事务所

北京市隆安（深圳）律师事务所

北京市盈科（深圳）律师事务所

广东广和律师事务所

广东华商律师事务所

广东知恒律师事务所

广东卓建律师事务所

泰和泰（深圳）律师事务所

万商天勤（深圳）律师事务所

暨南大学法学院

深圳大学法学院

中国人民大学社会科学高等研究院（深圳）涉外法治与发展研究中心

中国人民大学社会科学高等研究院（深圳）知识产权与创新研究中心

惠州市德赛西威汽车电子股份有限公司

中国建筑第二工程局有限公司

更多免费行业报告　并购家　www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

序

当中国企业的身影越来越多地出现在新加坡的写字楼、曼谷的产业园、吉隆坡的港口、胡志明市的工厂和墨西哥的近岸基地，一个朴素而深刻的命题也随之浮现：走出去，靠什么行稳致远？

答案里，“法治”是绕不开的关键词。

今天的出海，早已不是简单的商品输出。我们正处在一个规则加速重构的时代，数字经济与人工智能正在重塑全球贸易的规则，跨境数据怎么流、算法怎么管、平台责任怎么划，每一个都是新课题；而亚太每个市场在投资准入、税务、劳工、知识产权与争议解决上各有其法、各行其道。对出海的中国企业而言，机遇很大，但规则暗礁也很多。语言不通、法域陌生、信息不对称，常常让最好的商业构想，折戟于最细小的法律细节。

涉外法治是国家治理体系的重要一环，也是企业远航的压舱石。党的十八大以来，党和国家高度重视涉外法治建设，为广大法律人指明了方向：把服务国家高水平对外开放，视为义不容辞的使命。深圳，作为改革开放的窗口、粤港澳大湾区的核心引擎、毗邻港澳而面向世界的前沿，更有责任也更有条件在这一进程中走在全国前列；深圳律师，理应成为中国企业出海最可靠的同行者。

摆在读者面前的这两部蓝皮书，就是深圳律师行业交出的一份答卷——一部聚焦亚太数字经济与人工智能的法律前沿，一部深入新加坡、泰国、马来西亚、美国、墨西哥、越南、印度尼西亚七大市场的投资、贸易与法律查明。两本书各有侧重，把繁复的域外规则拆解为一问一答，让企业在决策的每一个关口，都能找到看得懂、用得上的答案，真正成为企业出海的一张“法律地图”、出海前的一次“法律体检”。

一部好的工具书，胜过千言万语。愿这两本蓝皮书成为中国企业驶向亚太的可靠罗盘，愿法律专业之光照亮更多企业走深走实、行稳致远的出海之路。

是为序。

深圳市律师协会会长 张斌

二0二六年八月

一、 APEC数字经济总体环境

Q1. APEC如何通过《亚太经合组织互联网和数字经济路线图》推动各经济体在数字经济领域关键议题政策的协调与共享？各经济体在该领域通常采取怎样的发展导向与监管思路？ 2
Q2. APEC各经济体在数据保护、平台监管、人工智能治理与数字竞争等数字监管领域的共性和差异主要有哪些？ 5
Q3. 数字经济给中国企业的出海模式带来了哪些变化？ 6
Q4. APEC各经济体存在哪些数字贸易的规则原则或共识？这些规则如何在经济体间初步落地？ 9
Q5. 从市场准入、数据合规要求、监管透明度及政策支持等维度看，APEC哪些经济体对数字企业具有相对“友好”的合规要求/政策环境？ 11
Q6. 哪些经济体的数据跨境流动和AI治理相对完善？ 12
Q7. 提供数字服务（如云服务、AI审计、数据治理等）的各类专业资格在APEC经济体间互认机制现状如何？相关机制对跨境数字服务贸易的实际影响如何？ 14
Q8. 数字经济企业进入APEC经济体市场通常面临哪些共性的法律与合规门槛？ 16
Q9. APEC商务旅行卡（ABTC）如何便利各界人士在APEC成员间流动？ 19
Q10. 结合APEC既有合作框架与政策文件，各经济体的数字经济在未来五年有哪些监管趋势？ 21

二、 APEC数据保护与隐私法规

Q11. APEC各经济体的数据保护法律体系有何不同？在个人信息保护机制模式以及数据处理的原则性要求方面存在哪些共性？ 24
Q12. 哪些APEC经济体的国内法在个人信息保护模式、保护强度与法律责任上与欧盟GDPR高度趋同？ 26
Q13. 如何识别企业处理的数据是否构成“个人信息”？ 28
Q14. APEC各经济体是否要求企业设立数据管理相关机构或岗位（如数据保护官/DPO）？相关要求通常适用于哪些类型的主体或业务场景？ 31
Q15. 在数据处理原则层面，APEC经济体是否普遍要求数据最小化原则？ 33
Q16. 数据泄露事件在APEC各经济体的报告要求是什么？ 35
Q17. APEC各经济体对儿童个人信息保护标准有哪些异同？ 38
Q19. APEC各经济体采集用户行为数据（包括App SDK、Cookies）的合法性基础有哪些？用户同意在其中扮演何种角色？ 40
Q20. 在APEC跨境营运中，若第三方处理者发生数据泄露或非法买卖，各方（如第三方处理者、企业相关人员等）的责任如何界定？ 43
Q21. 在APEC各经济体中，如何判断某项数据处理活动需开展“隐私影响评估”（如PIA、DPIA等）？ 45
Q22. 在同时适用多个APEC成员经济体数据保护要求的情况下，企业通常可以通过哪些合规策略来协调差异、降低整体合规成本？ 26
Q23. 企业如何就其数据保护与隐私合规的问题，在全球通用框架与当地法律特定要求之间取得平衡？ 35
Q24. APEC经济体对于敏感个人数据的监管通常体现在哪些方面？ 49

三、 APEC跨境数据流动

Q25. APEC CBPR（跨境隐私规则）体系是什么？其在促进跨境数据流动方面发挥了何种作用？ 54
Q26. APEC哪些经济体要求数据本地化？ 54
Q27. APEC哪些经济体要求跨境传输前需要当地主管机关审批或备案？ 55
Q28. 若企业发生跨境数据泄露，是否需同时向多个国家/地区报告？ 58
Q29. 如何在美国、日本、新加坡之间实现个人信息的合规跨境传输？ 60
Q30. 数据跨境传输协议（DTA/SCC)在APEC经济中是否有效？ 62
Q31. 企业能否依靠合同作为跨境传输的主要合法性依据？ 64
Q32. APEC经济体对云服务商的数据存储合规要求是否一致？ 66
Q33. 企业通常基于哪些因素判断拟跨境的数据是否落入重点监管范围？ 68
Q34. APEC各经济体主要对哪些行业数据进行重点监管？ 70
Q35. 当发生跨境数据纠纷时，APEC各经济体对“云端取证”效力的承认现状如何？企业如何避免数据储存地法律与司法调查要求的冲突？ 72
Q36. 有关数据跨境传输，APEC各经济体对“用户明确同意”有哪些具体适用和例外规则？ 72
Q37. 监管机构在哪些情况下会要求企业提供源代码或数据样本？相关要求的适用范围和合规边界是什么？ 73
Q38. 若数据需存储在当地，企业应如何设计混合云架构以规避合规风险？ 74
Q39. 企业如何避免“隐性跨境数据流动”的监管风险？ 75
Q40. 在多国数据流动场景下，数字平台的合规责任包含哪些触发条件与类型？ 77

四、APEC人工智能法律与监管

Q41. APEC经济体在人工智能治理方面有哪些共同原则、政策倡议或合作机制？这些共识在不同经济体的落地路径上存在哪些差异？ 80
Q42. 美国在AI监管中，对行业自律的依赖程度及核心监管趋势如何？ 81
Q43. 哪些APEC经济体在数字行业准入、税收优惠及政策扶持方面具有相对优势？ 82
Q44. 在尚未出台人工智能专门立法的APEC经济体，其开展相应监管的依据是什么？ 84
Q45. APEC各经济体针对AI辅助“深度伪造”（Deepfake）诈骗有哪些监管应对路径？在此场景下，企业有哪些反诈合规义务？ 86
Q46. APEC各经济体对“跨境交付”和“商业存在”数字服务有哪些外资股比限制？ 87
Q47. 哪些 APEC 经济体明确规定企业负有 AI模型训练数据来源的披露义务？ 89
Q48.跨境AI侵权纠纷实践中，包含哪些主流纠纷解决机制？分别如何兼顾纠纷解决效率与数字资产的执行可操作性？ 90
Q49. 企业训练模型使用公开数据是否需要授权？ 91
Q50. APEC主要经济体围绕AIGC生成内容的版权保护，司法实践与主管机关对独创性标准以及人类作者身份的要求有何差异？ 92
Q51. 在APEC经济体销售带AI功能的硬件产品通常需要哪些认证？ 93
Q52. AI系统造成损害时，不同主体的责任如何分配？ 94
Q53. AI模型输出不准确，在何种情况下可能构成法律风险？ 97
Q54. 在对AI提出透明度或可解释性要求的监管或行业场景中，AI产品如何满足可解释性要求？ 98
Q55. 中小企业部署AI时应特别注意哪些合规要求？ 99

五、APEC算法治理与自动决策系统

Q56. APEC各经济体对算法的公平性、透明度、可解释性分别建立了何种规制体系？存在哪些差异？ 101
Q57. 哪些APEC经济体设置了推荐算法的监管备案制度？未要求备案的经济体，通过何种监管路径保障推荐算法的合规性？ 102
Q58. APEC各经济体对“个性化推荐”提出了哪些合规要求？ 104
Q59. 在何种情况下，自动决策系统是否必须需要人工复核机制？ 106

更多免费行业报告 并购家 www.ipoipo.net

亚太数字经济与人工智能法律问答指南(蓝皮书)
Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q60. 在自动化决策或算法推荐等应用场景中，如何判断算法是否存在歧视风险? 107
Q61. 若算法自动决策导致服务贸易合同违约（如金融授信失败），企业的法律责任是什么？责任认定通常会考虑哪些因素，是否存在合理的抗辩或免责空间? 108
Q62. 如何合规处理自动决策对用户权益的影响? 110
Q63. 哪些行业的算法监管相对严格（如金融、就业）? 113
Q64. 在何种情况下，算法模型需要定期审计? 115
Q65. 企业使用第三方算法需要承担哪些合规义务? 117

六、APEC数字贸易、电子商务与平台经济

Q66. APEC经济体在推动数字贸易发展的过程中通常强调哪些原则性共识? 120
Q67. APEC各经济体对电子合同与电子签名的法律效力如何认定？存在哪些差异? 122
Q68. 数字产品（如软件）以及数据交付服务，在不同经济体下通常享有哪些关税及税收优惠政策? 124
Q69. 跨境电商平台需承担哪些消费者保护义务? 126
Q70.平台在内容管理上需承担哪些合规义务? 129
Q71. APEC各经济体针对平台算法排序规则，分别设置了哪些强制披露规则? 131
Q72. 电商数据（交易记录、评论）通常受到哪些数据跨境传输的合规限制? 134
Q73. 各经济体对非银行机构提供跨境支付与结算服务有哪些准入牌照要求及/或金融监管要求? 135
Q74. 在何种情况下，平台在多国运营时需设本地代表或制定联络主体? 140
Q75. 跨境提供数据专业服务的情境中，有关数据服务合同如何确定适用法律与争议解决的管辖方式? 142

七、APEC网络安全与技术合规

Q76. 哪些APEC经济体实施数据基础设施的安全审查? 144
Q77. 网络产品进入各成员经济体，通常可能涉及哪些安全认证、技术合规评估或准入要求? 145
Q78. 云服务商的合规责任有哪些? 146
Q79. 工控系统与IoT设备是否须通过当地安全测试? 148
Q80. 若企业系统遭网络攻击，应如何进行处置？是否必须向监管机构报告? 149
Q81. 各成员经济体通常如何管控加密技术的进出口? 154
Q82. 硬件产品的固件在何种情况下可能触发备案、公告、测试或重新认证等合规要求? 156
Q83. 安全事件应急预案是否是强制要求? 157
Q84.跨境运营的企业如何统一网络安全管理? 159
Q85. 跨境运营中，企业在处理安全日志传输时通常需遵循哪些数据合规要求? 160

八、APEC产业应用场景（制造业、IoT、电动车、跨境电商等）

Q86. 在智能制造场景下，各经济体对智能制造数据有哪些特殊监管要求？生产运营数据、设备运行数据与质量数据等通常在何种情况下会被纳入重点监管范围? 164
Q87. 智能硬件采集用户数据是否需额外披露? 165
Q88. 跨境电商店铺推荐算法在各经济体通常受哪些监管要求? 166
Q89. 各经济体针对物联网设备的无线电认证分别设立了何种监管机制? 167
Q90. 各经济体如何对电动车数据（电池、定位）进行监管否构成敏感数据? 169
Q91. 工业互联网平台的跨境数据流动风险有哪些? 171
Q92. 各经济体下，AI质检系统产生的数据需要遵循哪些数据保护相关规则? 172
Q93. 企业在多个APEC 经济体使用同一智能设备系统，需要满足哪些跨境合规要求? 173
Q94. APEC主要经济体对IoT产品在当地建立“数据镜像”均设立了何种监管规则? 175
Q95. APEC主要经济体对制造业AI项目（如预测性维护）的数据用途披露分别设立了哪些监管要求？逻辑有何差异? 175

九、APEC知识产权与数字内容

Q96. 如何判断AI模型的数据训练（数据收集和整理、训练）和内容生成是否侵犯版权? 178
Q97. AI模型的数据训练和内容生成侵犯版权，应如何承担责任? 179
Q98. 云端软件及相关服务（即通过网络提供软件功能或技术支撑的服务形态），应如何通过知识产权进行全面保护? 181
Q99. 针对算法及模型权重，可采取哪些保护措施，以抵御窃取风险? 182
Q100. 企业如何应对海外市场的版权、内容合规投诉? 184

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容



亚太数字经济与人工智能法律问答指南(蓝皮书)
Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

Q1

APEC如何通过《亚太经合组织互联网和数字经济路线图》推动各经济体在数字经济领域关键议题政策的协调与共享？各经济体在该领域通常采取怎样的发展导向与监管思路？

（撰写人：左李福）

答：

一、背景简介

1.制定目的：为应对数字时代挑战、促进区域经济合作、释放创新潜力、增强经济韧性，并落实APEC的长期愿景，推动亚太地区实现包容、可持续和高质量的发展。

2.制定背景：旨在落实2014年APEC领导人认可的《促进互联网经济合作倡议》，为成员经济体在数字基础设施建设、政策协调、数据流动及弥合数字鸿沟等关键领域提供合作框架和行动指南。《亚太经合组织互联网和数字经济路线图》（APEC Internet and Digital Economy Roadmap, AIDER）在2016年经APEC部长级会议批准起草提案后，由互联网经济特别指导小组组织制定的，2017年正式发布。

3.后续更新：《亚太经合组织互联网和数字经济路线图》（APEC Internet and Digital Economy Roadmap）系动态文件，在2018年巴新莫尔斯比港会议及2021年第二十八次领导人非正式会议等场合，均被重申并要求各成员加强落实。

二、核心提要

1.AIDER 以非约束性自愿机制为核心，通过11大领域行动框架、DESG 统筹机制、标准互认与能力建设，推动亚太数字经济政策协调与经验共享，避免区域规则碎片化。

2.各经济体呈现三类发展与监管模式：发达经济体侧重创新引领 + 精细数据流动监管；新兴经济体强调安全主权 + 普惠数字化；发展中经济体以基础建设优先 + 轻量监管为特征。

3.区域协同核心在于平衡差异：区域协作的核心难点在于平衡数据主权自由流动、事前守门人审查与事后反垄断的分歧，通过 APEC 框架孵化共识。

三、法规矩阵与专业洞察

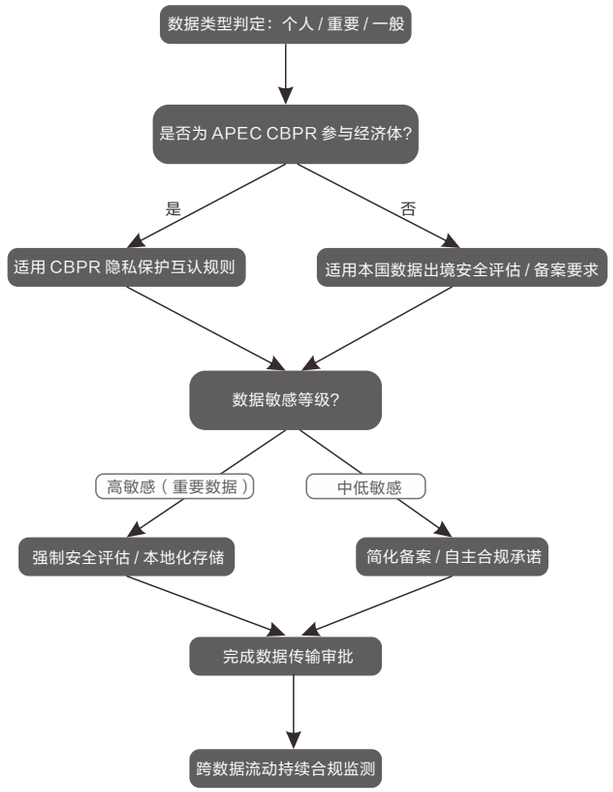
1.核心法规与政策要求对比表

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

维度	发达经济体 （美 / 新 / 日）	新兴经济体 （中 / 印尼 / 泰）	发展中经济体 （秘鲁/巴布亚新几内亚）
数据流动政策	支持跨境自由流动，参与 CBPR，限制不必要本地化	数据主权与安全审查 + 出境评估，有限流动 + 主权优先	基础数据保护规则，依赖 APEC 互认框架
平台监管模式	事后反垄断 + 守门人义务 + 透明度要求	事前常态化监管 + 算法治理 + 消费者保护	轻量备案制，以发展与普惠为核心
数字发展重点	AI / 云计算 / 半导体前沿技术，数字贸易枢纽	数字新基建 + 跨境电商 + 中小企业数字化	宽带普及 + 电子政务 + 普惠金融
监管工具	监管沙盒、风险分级、行业自律	数据分类分级、平台合规清单、专项整治	基础安全防范、APEC 能力建设项目
APEC 协作参与度	深度参与 CBPR、标准制定与规则输出	积极参与能力建设，推动安全导向规则	依赖援助，逐步对接区域框架

2.数据跨境流动合规判断流程图



3.说明与结论

（1）对比表说明

发达经济体以“数据自由流动 + 精细监管”为核心，积极主导 APEC 数字规则；新兴经济体在保障数据主权的前提下，逐步对接区域互认框架；发展中经济体仍以补基础为核心，深度依赖 APEC 能力建设。

（2）流程图说明

APEC 框架下数据跨境流动的核心逻辑是“互认优先、分级监管”，CBPR 为参与经济体提供简化路径，非参与经济体则需遵循本国安全审查要求，同时按数据敏感等级实施差异化管理。

（3）结论

AIDER 通过非约束性机制兼容多元制度，以标准互认和能力建设为抓手，在尊重各经济体发展阶段差异的前提下，推动亚太数字经济政策渐进趋同。

（4）案例阐释

①虚拟案例：

某跨境电商企业（总部在新加坡，业务覆盖中国、印尼、秘鲁）拟实现用户消费数据跨境流动以优化供应链。

②合规路径：

新加坡–美国： 由于两国均为 CBPR/全球CBPR论坛成员，企业可依托已获取的 CBPR 机构隐私认证，直接激活低成本的免审流动机制。

新加坡–中国：中国非 APEC CBPR或全球CBPR论坛成员。该方向的数据往来不能适用 CBPR 互认。企业必须按照中国《 数据安全法 》及《 个人信息保护法 》，采用签署网信办版《 个人信息出境标准合同 》并向地方网信部门备案的路径完成合规。

新加坡–秘鲁： 秘鲁属于发展中经济体，主要通过 APEC 能力建设项目提供的简易数字化通道对接基础保护标准，进行轻量级合规合规备案即可。

③实践启示：

企业可依托 AIDER 框架下的互认机制降低合规成本，同时需针对性适配不同经济体的监管要求，体现了 APEC“多元平衡、渐进协同”的核心逻辑。

四、行动清单

- ☐ 梳理本经济体数字经济核心政策，对标 AIDER 11大领域明确协作方向
- ☐ 评估数据跨境流动需求，判定是否加入 APEC CBPR 等互认机制
- ☐ 针对平台经济，建立“事前规范 + 事后监管”的复合治理框架
- ☐ 制定中小企业数字化赋能专项计划，对接 APEC 相关能力建设项目
- ☐ 参与 APEC 数字经济指导组（DESG）专题会议，分享最佳实践与政策经验
- ☐ 建立数据分类分级管理制度，平衡数据安全与跨境流动需求

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

☐ 针对发展中经济体合作伙伴，提供数字基建与人才培训援助，弥合数字鸿沟

☐ 跟踪生成式 AI 等前沿技术议题，参与 APEC 数字经济规则更新与标准制定

Q2

APEC各经济体在数据保护、平台监管、人工智能治理与数字竞争等数字监管领域的共性和差异主要有哪些 ？（撰写人：徐银萍）

答：

根据APEC的官方报告及近期会议成果，各经济体在数据保护、平台监管、人工智能治理与数字竞争等数字监管领域的共性和差异，可以用“在顶层共识下，因发展水平与监管传统而路径分化”来概括。

一、下面的表格汇总了四个核心领域的主要差异和共性，可以帮助快速把握整体情况。

监管领域	主要差异点（代表经济体/模式）	主要共性（APEC层面）
数据保护与跨境流动	严格本地化（如中国、俄罗斯）；条件式流动（如日本、新加坡，通过认证协议）；相对宽松流动（如美国，传统上强调行业自律，近年州级综合隐私立法与FTC执法亦显著加强）	认同数据隐私保护的重要性；致力于在《互联网和数字经济路线图》下探索可信数据流通方案。
平台监管与责任	事前监管与拆分风险（如中国反垄断执法）；事后追责与行业共治（如美国、新加坡，侧重事后反垄断与行业标准）	关注平台垄断、消费者权益（如“黑暗模式”）及在线安全问题；认为需要竞争政策与行业监管协同。
人工智能治理	全面立法与硬性合规（如中国、欧盟模式，新加坡MAS的行业强监管，韩国《人工智能基本法》于2026年1月施行）；柔性指南与原则导向（如美国、日本）	倡导发展 “负责任、可信赖的AI”关注安全、公平、透明；同意加强国际合作与能力建设。
数字市场竞争	结构性救济（如中、欧，倾向于拆分、强制开放接口）；行为性救济（如美、澳，更倾向罚款、禁止特定行为）	认识到数字市场竞争问题的复杂性；认可需在创新激励与防止市场扭曲间寻求平衡。

二、各领域监管特点详解：

1. 数据保护与跨境流动

严格本地化模式：以数据主权和安全为优先，要求数据境内存储，出境需安全评估。

条件式流动模式：在充分保护前提下促进流通，通过建立双边/多边认证机制（如APEC跨境隐私规则体系CBPR）实现数据合规跨境。

宽松流动模式：依靠市场力量和行业自律，立法相对宽松，以促进商业和创新为首要目标。

2. 平台监管与责任

事前监管（“守门人”模式）：对大型平台施加事前义务，如禁止自我优待、要求互操作性等，以预防垄断行为。

事后追责与共治模式：基于反垄断法事后处罚，同时鼓励平台与政府、社会共同制定内容审核、消费者保护等行业标准。

3. 人工智能治理

全面立法与硬性合规：通过专门性法律或强效力的部门规章，为AI系统设定明确的合规红线，如安全评估、算法备案等要求。

柔性指南与原则导向：发布不具有强制法律约束力的伦理框架或指南（如可信AI原则），鼓励企业自愿采纳，同时通过APEC等平台推动形成区域软法共识。

4. 数字市场竞争

结构性救济：认为数字市场垄断根源于结构性问题，倾向于采取分拆业务、强制开放核心设施等强干预措施。

行为性救济：认为处罚滥用行为即可恢复竞争，倾向于采取高额罚款、禁止签订排他协议等行为性纠正措施。

Q3

数字经济给中国企业的出海模式带来了哪些变化？（撰写人：徐银萍）

答：

数字经济驱动中国企业出海从传统“产品输出”转向“数字＋品牌＋生态”的综合输出，出海路径更高效、模式更多元、竞争力更聚焦价值与技术，同时推动本地化与合规体系升级。以下是具体变化与关键特征：

一、核心变化总览

维度	传统出海	数字经济下的出海	关键驱动技术 / 模式
价值定位	以低价代工、产能输出为主	技术赋能、品牌溢价、生态共建	AI / 大数据 / 云计算 / 工业互联网
路径模式	线下渠道、贸易为主	跨境电商、DTC、数字服务、技术出海	跨境平台 / 独立站 / 云服务 / 数字基建
供应链	大批量、长周期、刚性	小单快反、柔性生产、全球协同	数据预测 / 智能调度 / 5G+IoT
触达方式	经销商 / 展会	算法推荐、内容营销、私域运营	社交媒体 / TikTok/AI 营销工具
本地化	产品适配	内容、运营、合规、生态深度融合	本地数据合规 / 支付 / 客服体系
投资与风控	单点投资、信息滞后	全球数据协同、动态风控、轻资产扩张	区块链 / 实时数据分析 / ESG 工具

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、分维度深度解析

1. 价值与模式：从“卖产品”到“输出数字生态”

(1)技术与标准输出成核心：不再局限于硬件出口，逐步转向云服务、AI 解决方案、数字基建（如数据中心、智慧城市）等综合能力输出。部分云服务和通信技术企业在东南亚、中东等地区参与数字化转型项目，带动通信网络、云服务、电子支付等数字基础设施合作。例如，阿里云、华为云为东南亚、中东等地区提供数字化转型服务；“数字丝绸之路”推动通信网络与电子支付体系共建。

(2)品牌从“功能型”升级为“文化+技术型”：依托数字内容与算法实现文化共鸣，如《黑神话：悟空》以顶级引擎结合中国 IP 破圈，微短剧在东南亚/拉美通过轻量化叙事快速渗透，形成“内容+品牌”协同效应。

(3)DTC 模式崛起：跨境电商平台（SHEIN、Temu等）与独立站通过“小单快反”智能供应链，精准匹配个性化需求，缩短从设计到交付周期，提升市场响应速度。

(4)2. 供应链：数智化重构效率与韧性

(5)柔性生产与全球协同：大数据预测市场需求，先小批量试销再放量，降低库存风险；5G+IoT 实现跨区域工厂实时调度，如安吉家居企业集群快速响应全球订单，澄海玩具产业带通过平台连接 5 万 + 工厂与 4 万 + 采购商。

(6)跨境物流与支付升级：区块链提升清关与结算透明度，降低交易成本；跨境支付生态（如蚂蚁跨境）缩短中小企业结算周期，提升资金周转效率。

3. 渠道与触达：数字营销与私域运营主导增长

(7)算法驱动的精准获客：TikTok、Instagram 等平台通过 AI 推荐实现内容破圈，独立站用 SEO/SEM + 社媒矩阵构建私域；AI 工具（如亚马逊 Agentic AI、阿里国际站 AI Agent）覆盖选品、刊登、客服全流程，提升转化效率。

(8)内容与流量闭环：短视频、直播、UGC 内容成为出海标配，例如安克创新通过 YouTube 测评与 TikTok 挑战赛打造品牌认知，实现从“流量”到“留量”的转化。

4. 本地化与合规：从“适配”到“深度融入”

(1)运营本地化：建立本地数据中心、客服团队与支付体系，适配区域法规（如GDPR、东南亚数据保护法），字节跳动在美先通过算法实现内容本土化，再推进研发中心布局。

(2)ESG 与风控数字化：数字工具实时监测碳排放、劳工标准等 ESG 指标，区块链实现供应链溯源，提升合规透明度与可持续价值。

5. 投资与扩张：轻资产与全球协同并行

(1)投资模式多元化：从传统产能投资转向数字服务、研发中心、本地生态共建，如海尔在德国建智能工厂，依托工业互联网平台 COSMOPlat 提升订单响应速度 50%。

(2)轻资产扩张：通过云服务、技术授权、品牌合作等方式降低海外建厂成本，聚焦核心技术与运营能力输出。

6. 风控与合规：数据驱动的动态治理

(1)实时风控体系：利用大数据与 AI 监测汇率、地缘政治、供应链中断等风险，提前预警并调整策略。

(2)数据合规成为底线：建立本地数据存储与跨境传输机制，适配目标市场的个人信息保护、网络安全和数据安全法律、法规，降低合规风险。

三、典型案例

1.SHEIN：以数据预测选品，“小单快反”供应链实现 7-15 天快速上新，全球 DTC 渠道覆盖 150 + 国家，2024 年营收超 300 亿美元。

2.阿里云：为东南亚电商平台提供云计算与大数据服务，助力其实现订单处理效率提升 40%，同时输出中国云计算标准。

3.海尔：COSMOPlat 工业互联网平台赋能德国工厂，订单响应时间缩短 50%，推动“制造 + 数字服务”一体化出海。

4. 安克创新：通过 AI 优化产品设计与营销，E1 打印机以“消费级价格 + 工业级性能”切入海外空白市场，2025 年 Q1 北美营收占比 45%，同比增长 36.91%。

四、挑战与应对

1.核心挑战：数据合规壁垒（如 GDPR、数据本地化要求）、数字鸿沟（部分地区基础设施薄弱）、本地竞争加剧。

2.应对策略：构建“本地数据中心 + 跨境合规通道”的双轨体系，确保数据安全流动；与本地企业合作共建数字基建，降低进入门槛；以 ESG 与可持续发展为抓手，提升品牌信任度与市场准入优先级。

五、总结与趋势

数字经济推动中国企业出海进入“数智化引领”新阶段，核心是从“成本优势”转向“技术 + 品牌 + 生态”的综合竞争力，实现从“走出去”到“走进去”再到“引领规则”的跃迁。未来，AI 与工业互联网将进一步深化全链路协同，数字服务与内容出海将成为新增长极，而合规与本地化能力将决定企业出海的长期成败。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q4

APEC各经济体存在哪些数字贸易的规则原则或共识？这些规则如何在经济体间初步落地？

（撰写人：王熙雨）

答：

一、核心提要

《亚太经合组织互联网和数字经济路线图》（AIDER）提出11项区域共识性原则，构成APEC数字经济治理的框架。

规则落地路径呈现“软法+渐进式对齐”特征：通过国内法改革、区域试点、能力建设、区域协定吸收与CBPR扩展实现初步落地。

成员经济体在监管强度上存在差异，但在方向性原则上高度一致：均强调互操作性、透明度、风险管理与贸易便利化。

二、法规矩阵与专业洞察

1.APEC的数字贸易规则原则

(1)发展数字基础设施（Development of digital infrastructure）：建设高速、可靠、可扩展的数字网络与技术基础，为数字经济活动提供底层支撑。

(2)促进互操作性（Promotion of Interoperability）：推动技术标准、数据格式与系统之间的兼容性，减少跨境数字活动的制度与技术摩擦。

(3)实现普及性宽带接入（Achievement of universal broadband access）：确保能获得可负担的宽带服务，缩小数字鸿沟。

(4)构建互联网与数字经济的整体性政府政策框架（Development of holistic government policy frameworks for the Internet and Digital Economy）：推动政府在数字经济领域形成协调一致、跨部门联动的政策体系。

(5)推动影响互联网与数字经济的监管方式的协调与合作（Promoting coherence and cooperation of regulatory approaches affecting the Internet and Digital Economy）：减少监管碎片化，通过跨境合作提升数字经济监管的一致性与透明度。

(6)促进创新与关键数字技术和服务的采用（Promoting innovation and adoption of enabling technologies and services）：支持新兴技术研发、试点与应用，推动区域创新生态发展。

(7)提升ICT使用中的信任与安全（Enhancing trust and security in the use of ICTs）：加强网络安全、隐私保护与风险管理，提升数字环境的可信度。

(8)在尊重适用国内法律法规的前提下，促进互联网与数字经济发展所需的信息与数据自由流动（Facilitating the free flow of information and data for the development of the Internet and Digital Economy, while respecting applicable domestic laws and regulations）：在尊重国内法律的前提下，推动跨境数据流动以支持贸易、创新与经济增长。

(9)完善互联网与数字经济基础测量体系（Improvement of baseline Internet and Digital Economy measurements）：建立统一、可比的数据指标体系，为政策制定提供可靠依据。

(10)提升互联网与数字经济的包容性（Enhancing inclusiveness of Internet and Digital Economy）：确保中小企业、弱势群体与偏远地区能够公平参与数字经济。

(11)促进电子商务并推进数字贸易合作（Facilitation of E-commerce and Advancing Cooperation on Digital Trade）：推动跨境电商便利化、数字贸易规则协调与区域合作。

2.这些规则如何在APEC经济体间初步落地?

APEC的落地方式不是“强制执行”，而是通过软法工具推动成员经济体逐步对齐。

(1)区域框架与路线图（AIDER-APEC Internet and Digital Economy Roadmap）提供11个数字经济发展方向，成员经济体据此制定本国数字贸易政策，是区域数字贸易规则的“框架”。

(2)跨境隐私规则体系（CBPR）互认机制

美国、日本、韩国、新加坡等9个经济体已加入，通过认证方式实现跨境数据流动。企业通过认证即可在成员经济体间合法传输个人数据。

(3)数字贸易便利化指标（DTFI）

APEC对各经济体的数字贸易便利化水平进行量化评估，促使成员在无纸化贸易、电子认证等方面对齐。各经济体根据指标改进本国通关与贸易流程。

(4)试点项目

例如：电子原产地证书互认、区域单一窗口互联、数字身份互操作试点等。

(5)国内立法与政策改革

APEC原则通过以下方式进入各经济体国内法：数据保护法（如日本APPI、韩国PIPA、中国PIPL）、电子交易法、网络安全法、数字贸易章节（如CPTPP、DEPA），各经济体在本国法律中吸收APEC原则。

综上，APEC的数字贸易规则体系以软法为主，通过AIDER、CBPR、数字贸易便利化指标、试点项目与国内立法改革等方式逐步落地。尽管各经济体监管强度不同，但在跨境数据流动、无纸化贸易、互操作性、消费者保护与数字包容等方面已形成一定共识，为区域数字贸易一体化奠定基础。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q5

从市场准入、数据合规要求、监管透明度及政策支持等维度看，APEC哪些经济体对数字企业具有相对“友好”的合规要求/政策环境？（撰写人：孟昕）

答：

一、核心提要

对数字企业而言，一个经济体的合规环境是否“友好”，通常要从市场准入、数据治理规则、监管透明度以及政策支持等维度综合判断

在APEC经济体中，新加坡和澳大利亚被普遍认为是数字企业较为友好的经济体。中国虽然在数据跨境流动方面监管较严格，但数字经济政策和市场规模为数字经济参与企业提供了重要的发展土壤。

APEC跨境隐私规则体系（APEC CBPR System）为区域数据流动提供了重要制度基础。

一、法规矩阵与专业洞察

评估一个经济体对于数字企业的合规环境时，企业通常从市场准入、数据治理要求、监管透明度及政策支持等维度评估。关注的问题，例如：市场准入与外商投资审查相关规定，数据治理与数据跨境流动规则，监管透明度与规则稳定性，以及对于相关行业的政策支持情况。

新加坡长期被认为是数字经济监管环境较为友好的经济体之一。从市场准入维度看，新加坡对数字服务和互联网企业总体保持较为开放的政策环境。在数据治理方面，新加坡的《个人数据保护法》（Personal Data Protection Act, PDPA）建立了较为清晰的数据保护制度，并通过监管机构发布指南、示例和合规工具，帮助企业理解法律要求。此外，新加坡还加入了APEC跨境隐私规则体系（APEC CBPR System），为企业开展跨境数据流动提供了制度基础。在政策层面，新加坡政府长期推动Smart Nation战略，支持数字经济和智慧城市发展。

中国是全球规模最大的数字经济市场之一，在移动互联网、电子商务及数字经济基础设施建设等领域具有明显优势。在数据治理方面，中国通过了《网络安全法》《数据安全法》和《个人信息保护法》建立了较为完整的数据治理体系，并配套实施了数据出境安全评估、标准合同备案及个人信息保护认证制度，并通过《促进和规范数据跨境流动规定》及各自贸区"数据出境负面清单"进一步优化跨境流动管理，对跨境数据流动采取相对透明的监管。此外，近年来推动“数字中国”“人工智能+”等国家战略，为数字企业提供较好的发展土壤。

澳大利亚也是对数字企业较“友好”的经济体之一。从市场准入维度看，澳大利亚对数字服务和技术企业总体保持开放政策。在数据治理方面，澳大利亚通过了《隐私法1988》（Privacy Act 1988），确立澳大利亚隐私原则（Australia Privacy Principles, APP），还加入了全球跨境隐私规则（Global CBPR）体系。在监管透明度方面，由澳大利亚信息专员办公室（OAIC）负责执法监管，通过指南、案例和执法通告等方式向企业解释法律要求，有助于企业预判合规成本。此外，澳大利亚政府近年来持续推出数字经济和人工智能发展相关发展政策。

综上所述，从市场准入、数据治理规则、监管透明度及政策支持等维度综合评估，中国、新加坡和澳大利亚在APEC经济体中通常被认为对数字经济企业具有相对友好的营商环境。需要指出的是，监管严格程度并不必然等同于营商环境不友好。对于数字企业而言，更重要的是监管规则是否明确、制度是否具有可预期性，以及是否存在清晰的合规路径。因此，建议在APEC经济体开展业务的数字企业结合自身业务模式、数据处理活动以及合规成本，对不同经济体的数据治理要求、跨境数据流动规则以及产业政策进行综合评估，从而选择最适合的市场和合规策略。

三、行动清单

在APEC经济体开展数字业务前，企业可以参考以下行动清单进行初步规划：

□评估目标经济体的市场准入政策

□梳理拟开展的数据处理活动情况

□检索相关法律、法规及政策

□评估行业监管沟通度及合规可预期性

Q6

哪些经济体的数据跨境流动和AI治理相对完善？（撰写人：郭小萱）

答：

一、核心提要

欧盟确立了“基本权利保护”的高门槛范式：数据跨境以《通用数据保护条例》（GDPR）的充分保护决定或标准合同条款等适当保障措施为底线；AI治理通过《人工智能法案》（AI Act）确立了全球首个基于风险分级的强监管框架。

亚太地区呈现“安全、务实与发展”的多维进路：中国依托《数据安全法》（DSL）与《个人信息保护法》（PIPL）实施以安全评估为核心的跨境双轨制，并划定算法透明法定红线；美国与APEC倾向原则导向，依赖自愿性AI风险管理框架与CBPR问责机制。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

新加坡聚焦“等效保护与商业平衡”：依据《个人数据保护法》（PDPA），数据仅在接收方提供等效保护标准时方可出境，为出海企业提供务实通道。

二、法规矩阵与专业洞察

经济体	数据跨境流动规则	人工智能（AI）治理思路
欧盟	GDPR：向第三国传输须具备需具备“充分保护决定”，或采用标准数据保护条款等保障措施。	AI Act：风险分级法，禁止潜意识操纵等AI系统，对高风险系统设定严格的合格评定与透明度义务。
中国	PIPL & DSL：出境需经国家网信部门安全评估、专业机构认证或订立标准合同；对重要数据实施更严格出境管理。	PIPL：强调自动化决策透明度和结果公平，不得实行不合理差别待遇，并赋予个人拒绝权。
APEC/美国	CBPR：建立自愿性体系，通过问责代理机构审查，促进商业数据自由流动。	NIST AI RMF：提供将AI风险管理结构化为“治理、映射、测量、管理”四大功能的自愿性框架。
新加坡	PDPA：禁止个人数据转移至境外，除非数据在接收方提供等效保护标准时方可出境。	依托PDPA原则，在数据创新与个人数据保护之间寻求商业与权利的平衡。

当前，全球在数据跨境和人工智能领域的治理正呈现出“区域化协同”与“属地化监管”并存的特征，各主要经济体的立法逻辑差异显著。

欧盟构建了全球最为严密且具有强制性的成文法网络。在数据出境方面，GDPR严格要求数据接收国必须具备“充分保护水平”；对于不符合充分性保护认定的国家，企业必须依赖SCC或BCR等法律工具。在AI合规方面，欧盟《人工智能法案》（AI Act）以风险为导向，将AI系统划分为不同等级。例如，该法案第5条明确禁止使用能够实质性扭曲人类行为并造成重大伤害的潜意识操纵技术。同时，针对被归类为“高风险”的系统（如用于人员招聘、关键基础设施管理的AI），法案要求其在投放市场前必须通过严格的合格评定程序，并具备可追溯的日志记录和人类监督机制。

中国从国家安全与公民权益双重维度建立起严密的监管体系。在跨境数据流动方面，《数据安全法》（DSL）第31条对涉及国家安全的核心与重要数据设立了严格的出境审批机制。同时，《个人信息保护法》（PIPL）第38条为一般个人信息出境提供了安全评估、个人信息保护认证及签订标准合同三种合法路径。在AI应用治理层面，PIPL第24条精准规制了“大数据杀熟”及算法歧视问题，要求通过自动化决策作出对个人权益有重大影响的决定时，必须向个人提供说明并允许其拒绝仅由机器作出的决定。

亚太地区（APEC经济体及美国、新加坡）则更注重合规的务实性与灵活性。APEC的CBPR体系允许企业通过受认可的“问责代理人”进行隐私实践认证，大幅降低了跨司法管辖区的交易摩擦。在AI治理方面，美国国家标准与技术研究院（NIST）发布的《AI风险管理框架》（AI RMF 1.0）代表了一种非强制性、灵活的治理思路，它通过“治理、映射、测量、管理”四大功能，帮助组织在AI生命周期内主动识别和降低风险。新加坡的《个人数据保护法》（PDPA）第26条则采取了“等效保护”原则，要求跨境传输必须确保接收方提供与新加坡相当的保护水平。

【案例介绍】一家新加坡医疗AI企业拓展中欧市场：在欧盟，其辅助诊断系统落入AI Act“高风险”区间，投放前需通过第三方合格评定，患者健康数据跨境需符合GDPR的SCC机制；在中国，敏感医疗数据回传新加坡需触发PIPL和DSL的数据出境安全评估程序。若AI诊断建议构成重大影响的自动化决策，必须保障中国患者的知情权与拒绝权。

三、行动清单

对于计划在上述主要经济体开展数据跨境或AI业务的出海企业，建议采取以下自查行动：

□数据资产与流向盘点：梳理企业内部数据流向，清晰界定是否涉及“敏感个人信息”或特定司法管辖区定义的“重要数据”，这直接决定了出境的合规门槛（DSL第31条）。

□确立跨境合法性基础：根据目标市场落实合法出境路径。例如，评估是否需要采用GDPR第46条规定的SCC机制，或向中国网信部门申报PIPL第38条规定的安全评估/签订标准合同。

□开展AI风险分级与影响评估：在部署AI系统前，依据欧盟AI Act第6条主动对模型风险进行分类，并参考NIST AI RMF实施全面的测量与映射。

□落实算法透明与退出机制：针对用户端的AI应用，防范PIPL第24条规制的自动化决策歧视，确保算法决策可解释，并为用户提供拒绝纯自动化决策的便捷选项。

□部署人类监督与干预：为高风险AI系统设计“人在回路（Human-in-the-loop）”机制，确保系统在异常或超出预定边界时能够受人类监督或安全中止（AI Act第14条）。

Q7

提供数字服务（如云服务、AI审计、数据治理等）的各类专业资格在APEC经济体间互认机制现状如何？相关机制对跨境数字服务贸易的实际影响如何？

（撰写人：孟昕）

答：

一、核心提要

APEC目前尚未建立全面覆盖数字服务领域、并适用于全部成员经济体的统一专业资格互认机制。数字服务领域在APEC内部更接近标准协调和规则对接阶段，而非执业资格自动互认阶段。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

目前APEC经济体之间尚未建立专门覆盖云服务、AI审计、数据治理等全部数字服务领域并适用于全部成员经济体的统一的专业资格的认证协议或互认机制，但“数字凭证（Digital Credentialling）”作为新兴支持工具。

从现有制度看，APEC的专业资格认证安排仍然主要集中于工程、会计、建筑、护理等传统持证行业。由于数字服务行业与传统行业比较，存在行业边界不统一、市场化认证多于法定认定的情况，目前对于数字服务领域相关执业资格尚未有统一资质，因此数字服务领域在APEC内部更接近标准协调和规则对接阶段，而非执业资格自动互认阶段。

虽然不存在统一的数字服务资格互认，但APEC现有机制仍然对跨境数字服务贸易有一定的支持。APEC持续推动成员经济体在资源基础上开展相关专业资格互认的合作。根据APEC 2024年发布的《Mutual Recognition Agreements for Professional Qualifications and Licensure in APEC: Experiences, Impediments and Opportunities》统计，目前，APEC各经济体已经签订超过210项专业资格互认协议，主要集中于传统持证行业。此外，在APEC标准与合格评定分委会（SCSC）框架下，部分经济体围绕特定数字服务领域开展合作项目，如围绕隐私安全、网络安全、云计算、人工智能、数据合规等议题持续开展标准对话、政策协调等。各方都在尝试推动相关标准和合格评定方法的协调，但尚未形成具有强制力的互认机制。

此外，APEC Digital Economy Steering Group（DESG，数字经济指导组）等正在重点推进经济体间数字基础设施、技术创新、数据和信息跨境流通等方面的对话和合作。

法律服务领域可以作为理解数字服务跨境准入逻辑的一个直观例子。在法律服务领域，虽然不像上述工程师、建筑行业，在APEC经济体内形成成熟的互认网络，很多经济体已经允许法律服务采取“有限准入”或“外国法律顾问”模式提供服务。例如，新加坡允许外国律师取得limited licence，以外国法律顾问身份提供外国法和国际法咨询；日本也允许外国律师以注册外国律师（Gaikokuho-Jimu-Bengoshi）身份提供外国法服务；中国也允许外国律所通过驻华代表机构提供外国法相关服务。这些制度安排有助于提供数字服务相关跨境法律服务的支持，这也说明，跨境专业服务早期的现实路径往往不是直接的、全面的资格自动互认，而是有限准入、合同责任安排等。

综上所述，APEC目前尚无统一的、面向数字服务行业的专业资格互认机制，现有安排仍以传统受监管职业互认为主。与此同时，制度层面部分经济体已经形成规则协调、标准合作等制度基础，这类安排对跨境数字服务贸易的现实意义，主要是帮助企业降低部分制度摩擦、增强合规可预期性。

三、行动清单

□持续关注APEC及目标经济体关于数字贸易、专业服务开放、数据流动和行业准入的政策

□核查是否存在资格互认、承认或衔接机制

□关注目标经济体是否允许通过有限执业、代表机构、本地合作、项目制服务或其他附条件开放方式进入市场

Q8

数字经济企业进入APEC经济体市场通常面临哪些共性的法律与合规门槛？

（撰写人：王熙雨）

答：

一、核心提要

APEC 经济体虽监管虽监管路径差异显著，但通过APEC CBPR、标准协调等机制呈现一定趋同趋势。数字企业进入区域市场时，通常会面临以下八类常见法律与合规门槛。

二、法规矩阵与专业洞察

1.数据跨境流动与数据本地化要求

几乎所有 APEC 经济体都对跨境数据传输设置合规要求，包括：

- 数据跨境传输评估
- 数据接收方保护能力要求
- 数据本地存储或镜像要求（部分经济体）
- 个人信息跨境传输的同意机制

典型影响：企业需建立跨境数据合规体系（合同、评估、加密、存储策略）

2.隐私保护与个人信息处理规则

APEC 经济体普遍采用隐私保护框架（多数参考 OECD/CBPR），要求企业：

- 明确个人信息收集目的
- 建立用户同意机制
- 提供访问、更正、删除等权利
- 设立数据保护负责人（部分经济体）
- 建立数据泄露通报机制

典型影响： 企业需对产品、APP、平台进行隐私合规改造。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

3.网络安全与关键信息基础设施要求

多数经济体要求：

- 网络安全等级保护
- 安全事件通报
- 关键信息基础设施运营者的额外义务
- 加密技术使用规范

典型影响：企业需投入安全体系建设，满足本地安全审查要求。

4.数字平台与电子商务监管

APEC 经济体普遍对平台经济实施监管，包括：

- 平台责任（内容管理、消费者保护）
- 电子合同与电子签名要求
- 电子支付与反洗钱要求
- 平台透明度与算法治理（部分经济体）

典型影响： 跨境电商、平台型企业需满足本地电商法与消费者保护要求。

5.税务合规与数字服务税

数字企业常面临：

- 增值税/消费税对跨境数字服务的适用
- 常设机构（PE）认定风险
- 转移定价要求

典型影响： 企业需评估常设机构（PE）、增值税/转移定价、OECD、双边税收协定等问题。

6.内容监管与本地化合规

涉及：

- 内容审核义务
- 广告与营销合规
- 未成年人保护
- 本地文化与媒体监管（部分经济体）

典型影响：平台需建立本地化内容审核机制。

7.数字身份、电子认证与无纸化贸易要求

APEC 强调互操作性，但各经济体仍有差异：

- 电子签名法律效力
- 数字身份体系兼容性
- 电子发票、电子原产地证书等要求

典型影响：企业需适配本地电子认证体系。

8.中小企业、包容性与本地合作要求

部分经济体要求：

- 本地合作伙伴制度
- 本地人才与供应链参与
- 包容性数字化要求

典型影响：企业需建立本地合作网络与合规运营模式。

三、行动清单

□ 建立跨境数据合规体系：识别业务中涉及跨境数据流动的场景，建立数据分类、跨境传输评估、合同条款与加密措施。

□ 完成隐私保护制度建设：对照各经济体隐私法要求，完善用户同意机制、隐私政策、数据主体权利响应流程与泄露通报机制。

□ 开展网络安全能力评估：根据当地网络安全等级要求，建立安全管理制度、事件响应机制与本地化安全审查准备。

□适配本地电子商务与平台监管要求：梳理电子合同、电子签名、消费者保护、广告合规、平台责任等要求，调整业务流程。

□评估税务影响与数字服务税风险：识别是否触发数字服务税、增值税/消费税义务或常设机构风险，建立税务合规策略。

□建立内容管理与本地化审核机制：根据当地内容监管要求，制定内容审核标准、未成年人保护机制与广告合规流程。

□建立本地合作与包容性机制：根据当地政策要求，识别本地合作伙伴、人才培养、供应链参与等合规义务。

□构建数字经济合规矩阵：将数据、隐私、安全、平台、税务、内容、认证等要求纳入统一合规框架，形成可执行的区域合规路线图。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q9

APEC商务旅行卡（ABTC）如何便利各界人士在APEC成员间流动？

（撰写人：郭小萱）

答：

随着企业在亚太地区的业务拓展，您和高管团队是否经常为频繁办理各国签证而耗费大量时间和精力？APEC商务旅行卡（ABTC）正是亚太经合组织（APEC）为解决这一问题而设立的商务便利化工具。本指南将从核心价值、申请资格、使用便利及最新动态四个方面，为您解析ABTC如何助力企业高效出行。

一、 核心价值：一卡在手，16个经济体免签

APEC商务旅行卡是目前区域内最高效的商务出入境证件之一，其核心便利体现在：

1.覆盖范围广：中国籍持卡人可免签入境16个亚太经济体（包括日本、韩国、澳大利亚、新西兰、新加坡、马来西亚等主要贸易伙伴，美、加暂不审批但提供快速通关便利，港、台地区互不适用）。

2.通关速度快：各经济体主要国际机场均设有APEC专用通道，持卡人可享受快速通关礼遇，大幅减少入境排队时间。

3.停留时间长：根据经济体不同，单次入境允许停留60天或90天，充分满足商务考察、商务谈判、客户拜访等需求。

4.长期有效：卡片有效期长达五年，期间无需为前往上述16个经济体重复办理签证。

二、 申请资格：您的企业人员符合条件吗？

根据规定，我国企业主及以下四类人员如因业务需要经常前往APEC经济体，且无刑事犯罪或拒签记录，均有资格申办：

1.国有企业：中央和地方大型国有企业的管理人员、主要业务人员和技术人员。

2.民营企业：各类民营企业的管理人员和核心业务人员。

3.外资企业：中外合资、外商独资和台港澳资企业中的大陆人员。

4.政府官员：从事APEC事务或负责旅行卡业务的政府官员。

特别提示：外国人不能在中国申请，需向其所属经济体提出申请。

三、 申办与使用流程（实务操作）

（一）如何申办？

申办流程已大幅简化，您无需自行对接外交部，只需从企业所在地的人民政府外事办公室（地方外办）入手：

1.第一步：联系地方外办。可直接访问您企业注册地的外办官网或电话咨询，获取当地的具体申请材料清单和收费标准。各地要求可能略有差异。

2.第二步：在线提交申请。自2023年6月起，全国已有34个地方外办（包括天津、重庆、四川、湖北等）启用了APEC商务旅行卡申请管理新系统。您可以在线提交申请并实时查询进度。

新系统网址：https://consular.mfa.gov.cn/APEC/

3.第三步：等待审批。 初审通过后，材料将逐级上报至外交部领事司终审，并提交其他16个经济体分别审批。所需时间：外交部审核约5个工作日，全部经济体批准约需2-3个月。加急办理：若急欲前往某个已获批的经济体，可申请提前制卡，待其余经济体批准后再换卡。

（二）如何使用与管理？

1.使用方式：持卡人必须持申办旅行卡时的有效护照和有效旅行卡出入获批经济体。请务必使用专用通道（标识通常为“APEC Business Travel Card”）。

2.管理责任：民营企业持卡人的卡片由企业自行管理，但需制定管理细则并报地方外办备案。持卡人如离开原单位或身份变更，原单位需及时注销卡片，或经协商移交新单位并备案。

3.重要提醒：避免“签证覆盖”

问题：澳大利亚和新西兰要求申请人只能持有一个有效入境许可。如果您在旅行卡有效期内，另外申请了澳、新的纸质签证，后发的签证将自动覆盖并失效旅行卡上对应的五年期入境许可。

建议：除非特殊情况，不建议持卡人另外申请同类签证。

四、 最新动态：迎接数字化时代（虚拟ABTC）

为顺应全球旅行数字化趋势，APEC已正式推出虚拟APEC商务旅行卡，进一步提升了便利性和安全性。什么是虚拟ABTC？它是实体卡的数字化版本，于2021年3月1日正式启用。持卡人可在智能设备上展示虚拟卡，享受与实体卡同等的便利。

5.虚拟ABTC主要优势：

(1)实时更新：如果卡的有效期或可入境经济体发生变化，虚拟卡会实时更新，持卡人可立即使用。

(2)安全高效：降低了实体卡丢失或被盗的风险，查验流程更便捷。

(3)广泛认可：截至2025年，包括澳大利亚、日本、韩国、马来西亚、新西兰等在内的14个主要经济体已接受虚拟ABTC入境（注：俄罗斯暂不接受虚拟卡，但有临时替代方案）。

6.如何使用？

持卡人在抵达APEC经济体、通过专用通道时，只需在智能设备上出示虚拟ABTC即可，流程与出示实体卡完全一致。

总结：

对于致力于拓展亚太市场的企业而言，APEC商务旅行卡不仅是一张签证，更是一张提升商务效率、彰显企业信誉的“国际名片”。建议您立即联系企业注册地的外事办公室，了解具体申办事宜，让您的

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

核心团队享受到跨境通行的最大便利。

（以上信息来源于中国领事服务网https://cs.mfa.gov.cn/zggmcg/apecshlxk/及APEC官方网站https://www.apec.org/groups/committee-on-trade-and-investment/business-mobility-group，截至2026年2月更新）

Q10

结合APEC既有合作框架与政策文件，各经济体的数字经济在未来五年有哪些监管趋势？（撰写人：左李福）

答：

一、核心提要

1.数据治理将从“本地化”向“可信流动+分级分类”转型：各经济体将深化全球跨境隐私规则（Global CBPR）等互认机制，在保障数据主权与安全的前提下，推动区域内中低敏感数据的跨境自由流动，同时强化高敏感数据的出境管控与安全评估。

2.AI与生成式技术将成为监管核心焦点：以“风险分级”为核心的AI监管框架将成为主流，各经济体将在APEC框架下协同制定伦理准则、透明度要求与安全标准，同时通过监管沙盒平衡技术创新与风险防控。

3.平台治理与数字包容将走向精细化协同：针对大型平台的“守门人义务”将进一步强化，同时各经济体将在APEC框架下推进中小企业数字化赋能、数字适老化与反数字鸿沟行动，实现发展与监管的平衡。

二、法规矩阵与专业洞察

1.主流APEC成员经济体监管趋势对比表

监管维度	发达经济体（美/新/日/韩）	新兴经济体（中/印尼/泰）	发展中经济体（秘鲁/巴布亚新几内亚）
数据治理	深化CBPR互认，推动“数据自由流动+隐私保护”双轨制，限制不必要本地化	完善数据分类分级与出境安全评估，逐步对接APEC互认框架，强化数据主权	建立基础数据保护规则，依赖APEC能力建设实现合规升级
AI与生成式技术监管	风险分级监管+伦理准则，推动APEC区域AI国际标准制定与安全承诺落地，采用监管沙盒	构建“安全评估+算法备案+伦理约束”体系，参与APEC AI治理对话	聚焦基础安全风险防范，逐步引入AI伦理指引与应用规范
平台经济监管	强化“守门人”义务、反垄断与数据透明化，推动跨平台互操作性	常态化监管+算法治理+消费者保护，规范平台垄断与不正当竞争	轻量备案制，重点保护消费者与中小商家权益
数字包容与普惠	聚焦数字技能培训、适老化改造，推动中小企业数字化转型	优先覆盖乡村与弱势群体，推进数字基建与普惠金融及数字支付	普及宽带与移动互联网，依托APEC项目提升数字可及性
APEC协作方向	主导规则输出，推动Global CBPR扩容与AI治理标准落地	积极参与能力建设，倡导“安全与发展并重”的监管路径	深度依赖APEC援助，逐步对接区域合规框架

发达经济体将继续主导APEC数字规则制定，推动数据自由流动与前沿技术监管；新兴经济体在保障数据主权的同时，逐步对接区域互认框架，强化平台与AI治理；发展中经济体仍以补基础为核心，通过APEC能力建设实现监管升级。

1.结论

未来五年监管的核心逻辑是“在发展中规范、在规范中发展”，既保障各经济体的发展权与数据主权，又通过APEC框架降低跨境合规成本，推动亚太数字经济向更开放、更安全、更包容的方向演进。

三、行动清单

- ☐ 梳理本经济体数据分类分级规则，评估加入Global CBPR的可行性与路径
- ☐ 制定AI与生成式技术监管路线图，明确风险分级标准与伦理准则
- ☐ 针对大型平台开展“守门人义务”研究，完善反垄断与数据透明化监管工具
- ☐ 对接APEC数字包容项目，制定中小企业数字化与反数字鸿沟行动计划
- ☐ 参与APEC数字经济指导组（DESG）专题会议，跟踪数据流动、AI治理等规则更新
- ☐ 建立监管沙盒机制，为AI、跨境数据流动等创新场景提供试验空间
- ☐ 开展数据保护与数字技能培训，提升企业与公众的合规意识与数字素养
- ☐ 针对发展中经济体合作伙伴，提供数字基建与监管能力援助，推动区域协同发展

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容



亚太数字经济与人工智能法律问答指南(蓝皮书)
Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

Q11

APEC各经济体的数据保护法律体系有何不同？在个人信息保护机制模式以及数据处理的原则性要求方面存在哪些共性？

（撰写人：陈瑜琪）

答：

一、核心提要

APEC成员的数据保护法律体系的不同主要体现在立法模式与监管机制方面；APEC隐私框架本身不具有法律约束力，各经济体有权自主决定是否及如何在其国内实施框架原则，这导致区域内法律体系呈现显著多样性；APEC成员大多采用权利本位模式，保护个人信息以保护相应权利为途径；APEC经济体在数据处理方面遵循合法性、正当性、必要性原则、数据质量原则、数据存储期限限制原则、数据安全原则。这与APEC隐私框架的九项核心原则及OECD隐私指南一脉相承。

二、法规矩阵与专业洞察

经济体成员	立法框架	监管机制
中国	《个人信息保护法》（PIPL）、《数据安全法》、《网络安全法》	国家网信部门统筹协调
美国	缺乏统一的联邦层面通用数据隐私法，但拥有众多针对特定行业的法律	联邦层面没有统一的数据保护监管机构，而是由多个部门根据不同的行业法律进行监管
俄罗斯	《联邦个人数据法》（第152-FZ号联邦法）	涉及多个部门，包括联邦电信、信息技术和大众传媒监督局、联邦安全局等
日本	《个人信息保护法》（APPI）	个人信息保护委员会(PPC)
韩国	《个人信息保护法》（PIPA）	个人信息保护委员会（PIPC）
新加坡	《个人数据保护法》（PDPA）	个人数据保护委员会（PDPC）
澳大利亚	《1988年隐私法》	澳大利亚信息专员办公室（OAIC）
泰国	《个人数据保护法》（PDPA）	个人数据保护委员会
加拿大	《个人信息保护和电子文件法》（PIPEDA）	隐私专员办公室（OPC）

APEC经济体成员在数据保护的立法框架方面，大多数国家采用综合性统一立法模式，而美国则采用部门立法与行业自律结合模式。同时，APEC经济体成员设置了不同的数据保护监管机构，多数经济体设立独立监管机构，而美国和俄罗斯则采用多部门协调监管的方式。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

表：个人信息保护机制模式的共性

具体权利	含义
知情权	数据主体有权知悉其个人信息被收集、处理、使用的情况，包括处理者名称、目的、方式等。
访问权	数据主体有权向数据控制者查询、获取其个人信息。
更正权	数据主体有权要求更正不准确或不完整的个人信息。
删除权	数据主体有权在法定情形下要求删除其个人信息。

大多数APEC成员经济体采用权利本位模式，将数据主体的权利保护作为数据保护法律的核心。

表：数据处理的原则性要求方面的共性

具体权利	含义
合法性、正当性、必要性原则	个人信息的收集应限于与业务目的直接相关且必要的范围，不得过度收集数据
数据质量原则	确保个人信息的准确性、完整性和时效性，以降低错误数据带来的风险
数据存储期限限制原则	数据仅在为达成收集目的所必要的时间期限内保存，超出期限应予以删除或匿名化
数据安全原则	采取与风险相适应的组织和技术措施保护个人信息免遭未经授权的访问、泄露、篡改或破坏
防止损害原则	防止个人信息被滥用而导致对个人的损害，作为框架的首要原则
透明原则	确保个人能够知晓哪些信息被收集、用途为何
选择权/同意原则	确保个人对收集、使用、传输和披露个人信息的选择权
访问与更正原则	个人的访问与更正权利
责任原则	确保处理个人信息的组织承担责任，对违反原则的行为负责

尽管保护水平存在差异，但各经济体在数据处理的要求方面存在以上的共同原则。

三、行动清单

- □ 已明确目标经济体的数据保护核心适用法律
- □ 已梳理目标经济体的监管机构设置、监管权限和监管要求
- □ 已确认目标经济体数据处理的核心原则
- □ 已评估自身数据处理行为与目标经济体合规要求的匹配度
- □ 已规划针对目标经济体数据保护要求的合规整改

Q12

哪些APEC经济体的国内法在个人信息保护模式、保护强度与法律责任上与欧盟GDPR高度趋同？

（撰写人：陈瑜琪）

答：

一、核心提要

在APEC经济体中，中国、韩国、日本、新加坡、澳大利亚、加拿大等经济体的国内法在保护水平上均表现出向欧盟GDPR靠拢的趋势；读者可借此明确趋同的APEC经济体，理解其趋同及差异点，锁定合规重点；企业可自查现状，并制定后续合规调整方案，降低风险。

二、法规矩阵与专业洞察

1.保护模式的趋同

对比维度	欧盟GDPR	中国国内法	韩国国内法	日本国内法	新加坡国内法	澳大利亚国内法	加拿大国内法
立法模式	统一综合性法规（《通用数据保护条例》GDPR）	统一综合性法规（《个人信息保护法》PIPL）	统一综合性法规（《个人信息保护法》PIPA）	统一综合性法规（《个人信息保护法》APPI）	统一综合性法规（《个人数据保护法》PDPA）	统一综合性法规（《1988年隐私法》Privacy Act）	统一综合性法规（《个人信息保护与电子文件法》PIPEDA；拟被《消费者隐私保护法》CPPA取代）
监管机构	各成员国独立数据保护机构	网信办等多部门	个人信息保护委员会（PIPC）	个人信息保护委员会(PPC)	个人数据保护委员会（PDPC）	澳大利亚信息专员办公室（OAIC）	加拿大隐私专员办公室（OPC）
权利体系	全面					全面（访问权、更正权、销毁/去标识化权等）	全面（拟引入算法透明度权、数据处置权等）

洞察：在个人信息保护模式方面，这些经济体普遍采用了综合性立法模式，建立了相对独立的数据保护监管机构，并构建了较为完善的数据主体权利体系。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

2.保护强度的趋同

对比维度	欧盟GDPR	中国国内法	韩国国内法	日本国内法	新加坡国内法	澳大利亚国内法	加拿大国内法
合法基础体系	多种合法处理基础	告知-明示同意为核心，辅以其他合法基础	明确同意为核心基础	知情同意为核心基础	同意为核心基础之一	同意为核心基础（APP原则）	同意为核心基础（PIPEDA实质性同意原则）
数据泄露通知	72小时内通知监管机构和数据主体	及时告知履行保护职责的部门和个人	72小时内通知监管机构(2026年修正案)	尽快通知监管机构和数据主体	72小时内通知监管机构	若可能造成重大伤害，须通知OAIC和受影响个人	若可能造成重大伤害，须通知OPC和受影响个人（尽快而非固定72小时）
数据保护影响评估（DPIA）	高风险处理时进行	在特定情况下进行	高风险处理时建议进行	在特定情况下进行	在特定情况下进行	作为最佳实践存在（起源于澳大利亚、加拿大等国）	作为最佳实践存在（起源于澳大利亚、加拿大等国）
数据保护官（DPO）	特定情形强制要求	特定情形应当指定（大型平台强制）	强制要求（首席隐私官CPO权限强化）	建议设置	强制要求（所有注册企业须任命）	建议设置	建议任命数据隐私官

洞察：在保护强度方面，这些经济体都采用了与欧盟GDPR较为类似的合法基础体系，要求进行数据泄露的通知，也建立了数据保护影响评估和数据保护官机制。

3.法律责任的趋同

对比维度	欧盟GDPR	中国国内法	韩国国内法	日本国内法	新加坡国内法	澳大利亚国内法	加拿大国内法
行政罚款上限	2000万欧元或全球年营业额 4%	5000万元或年营业额5%，以较高者为准	最高1亿韩元；2026年引入营业总额10%的加重处罚	最高1亿日元（约70万欧元，非百分比模式）	年营业额10%或100万新元，以较高者为准	最高5000万澳元或3倍收益或30%收入（2024年改革后）	PIPEDA：最高10万加元；拟议CPPA：最高1000万加元或全球收入3%（严重违规最高2500万加元或5%）尚未通过
民事赔偿	损害赔偿						
刑事责任	严重违规可能涉及	严重违规涉及刑事起诉	严重违规涉及刑事起诉	最高50万日元、最高1年监禁	最高5000新元罚款、最高2年监禁	严重违规可能涉及（如《隐私法》刑事条款）	严重违规可能涉及

洞察：在法律责任方面，这些经济体普遍设置了较高额的行政罚款，也建立了完善的民事赔偿体系，设置了针对严重违法行为的刑事制裁方式。

三、行动清单

□ 已明确与GDPR高度趋同的APEC经济体，了解其核心趋同点

□ 已对照表格，了解经济体与GDPR在保护模式、保护强度上的差异

□ 已梳理经济体与GDPR在法律责任上的差异，明确高风险点（特别注意：日本罚款模式为固定金额而非百分比；加拿大当前PIPEDA罚款远低于GDPR但CPPA拟大幅提高；澳大利亚罚款上限超过GDPR）

□ 已制定针对趋同经济体的相关调整计划

□ 已进行经济体相关法律的监控，追踪其立法更新（如韩国2026年PIPA修正案加重处罚、加拿大CPPA立法进展、澳大利亚2024年提高罚款上限）

Q13

如何识别企业处理的数据是否构成“个人信息”？ **（撰写人：秦雨歌）**

答：

一、核心提要

“可识别性”是判断个人信息的核心标准：APEC隐私框架将个人信息定义为“与已识别或可识别个人有关的任何信息”。亚太地区主要经济体的国内立法（如中国、新加坡、韩国、日本、澳大利亚、加拿大等）均采用与此高度一致的定义方式。

“匿名化”是法定的脱敏出口：各经济体对匿名化的具体标准存在差异，但均要求达到“无法识别且不能复原”或同等效果。需注意，“去标识化”不等于匿名化，仍属个人信息范畴。

“组合识别”是企业最容易忽视的高风险领域：单条数据（如IP地址、设备ID）孤立看似无法识别个人，但与其他数据结合后“合理可能”指向特定个人时，即构成个人信息。APEC隐私框架明确指出，可能用于与个人交易的信息（如电话号码、电子邮件、IP地址），即使本身不直接识别个人，也可能纳入保护范围。企业须以“处理时掌握的全部数据集”为单位进行判断。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

主要法域	核心法规	个人信息定义标准	匿名化/去标识化标准
中国	《个人信息保护法》（PIPL）	以电子或者其他方式记录的与已识别或可识别自然人有关的各类信息，匿名化信息除外	匿名化：无法识别且不能复原；去标识化：不借助额外信息无法识别（借助额外信息仍可识别）
美国加州	CCPA/CPRA	识别、关联、合理可能关联特定消费者或家庭	去识别化：技术+业务双重保障，不得尝试重新识别
新加坡	PDPA	关于可被识别个人的数据，真实与否不限	匿名化数据排除保护；仍可合理识别者属个人信息
韩国	个人信息保护法	可识别特定个人的信息（含结合其他信息可识别者）	假名化：不借助额外信息无法识别；匿名化排除保护
日本	APPI	可识别特定个人（含结合易获取信息识别）或含个人识别符的信息	匿名加工：无法识别且不可复原；假名加工：替换关键标识
澳大利亚	Privacy Act	可识别或合理可识别个人的信息或意见（2024年改革扩大适用范围）	处理后再无合理可能识别个人，则脱离保护
加拿大	PIPEDA	关于可识别个人的信息	匿名化后合理不可能识别则排除，建议“重新识别风险测试”

在跨境合规实务中，最隐蔽的风险在于对“可识别性”的窄化理解。监管机构可能采用“合理可能性测试”：即考虑到现有的技术手段和识别成本，如果数据接收方能够通过关联碰撞还原个人身份，则该数据即具有识别性。

APEC隐私框架将个人信息定义为“与已识别或可识别个人有关的任何信息”。APEC框架还强调，信息是数据处理的结果，更容易侵犯个人隐私，需要更强的保护。在各成员国之间存在三种判断路径：①直接识别（数据本身指向个人，如姓名、生物特征）；②组合识别（单条数据无法识别，但结合其他信息后可识别，APEC框架将“可能用于与个人交易的信息（如电话号码、电子邮件、IP地址）”纳入考虑范围，即使这些信息本身不直接识别个人，也需结合具体情境判断）；③情境识别（是否构成个人信息取决于处理者的识别能力、信息组合可能性等具体情境因素，而非仅看信息形式）。最高人民检察院进一步明确，个人信息的判断须引入“动态判断”，在具体情境中综合考量信息敏感程度、使用价值及泄露损害等。

关于“匿名化”与“去标识化”的区分：根据中国信通院发布的数据匿名化规程，数据匿名化处理是数据去标识化后应用相关技术使标识符难以复原的过程，经匿名化处理后的数据即便借助了额外信息也难以识别特定自然人。在不同法域，“匿名化”的法律效果类似，均意味着信息不再属于个人信息保护范围，而“去标识化”“假名化”则保留了一定的可识别性，仍属于个人信息范畴。中国PIPL要求匿名化达到“无法识别且不能复原”的标准。

示例：浙江检察机关批量个人信息认定案（2025年）：2025年8月，最高检发布《厘清“批量个人信息”精准适用侵犯公民个人信息罪》理论文章，明确“可识别性”认定规则：①直接识别信息有限，仅指纹、DNA等具有唯一性；②间接识别须结合其他信息，如姓名、年龄、住址组合后可识别特定个人；③重复信息应去重，以身份证号等基准要素剔除多余数据；④抽样验证信息真实性，根据数据总量确定抽样比例（1万以下抽样30%，1-10万抽样1%-10%）。

三、行动清单

□ 建立数据资产“个人信息识别清单”：逐一评估企业处理的每类数据是否满足"已识别或可识别"标准，重点审查技术标识符（IP地址、设备ID、Cookie）、行为数据、位置数据，以"处理该数据的企业所拥有的全部数据集"为判断单位并考虑接收方/第三方可能掌握的信息，而非孤立评估单条数据；APEC框架要求考虑“可能用于与个人交易的信息”。

□ 建立匿名化与去标识化的双轨管理流程：明确区分“匿名化”（不可逆、脱离保护）与“去标识化”（可逆、仍属个人信息）两类状态，分别设定技术标准和合规义务，避免混淆导致违规；匿名化处理的目标是将可识别性降低到监管和组织可接受的风险水平。

□ 建立处理技术合规审查机制：对数据处理技术（包括加密、去标识化、假名化、聚合等）进行合规审查，确保技术方案与法律定义相匹配，并保留技术方案、处理流程和风险评估的完整记录备查。

□ 建立新兴市场合规底线机制：在相关法律法规尚未明确的法域，以现有生效法律中最严格的标准作为内部合规底线，避免后续法规出台后产生系统性偏差；

□ 建立数据分类分级动态管理机制：根据数据的识别能力（直接识别/组合识别/情境识别）、敏感程度、组合可能性对数据进行分层分类，对高风险类别（如生物识别、行踪轨迹、金融账户）设置更严格的处理权限和保护措施。

□ 建立“组合识别”风险评估机制：定期评估企业自身掌握的全部数据集之间的关联风险，识别单条信息无法识别但组合后可指向特定个人的场景；同时关注合作伙伴或第三方数据接收方的数据组合能力，防范传递后的重新识别风险。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q14

APEC各经济体是否要求企业设立数据管理相关机构或岗位（如数据保护官/DPO）？相关要求通常适用于哪些类型的主体或业务场景？

（撰写人：王丹）

答：

一、核心提要

APEC 经济体对 DPO / 数据保护官等数据保护岗位的要求分为强制设立、特定条件强制设立、建议 / 自愿设立三类，跨境企业需按属地规则分层合规。

强制设立以新加坡、韩国、马来西亚、俄罗斯、新西兰、菲律宾为主要代表。

特定条件强制设立以中国、美国、印度、泰国为代表，多以处理规模、数据敏感性、业务场景为门槛，未达标可暂不强制设立。

建议/自愿设立的代表：日本、中国香港特别行政区

二、法规矩阵与专业洞察

要求类型	经济体	适用主体 / 触发条件
强制设立	新加坡	所有组织，无论规模、注册地、盈利性质，只要在新加坡境内收集、使用、披露或存储个人数据，均须任命至少一名DPO，并于2024年9月30日前向PDPC登记联系方式。不设豁免门槛。DPO可为外部机构，无需为新加坡公民，但须在新加坡本地工作。
	韩国	所有直接或间接处理个人信息的公共机构、法人、组织、个人，均须设立首席隐私官（CPO）。2026年PIPA修正案进一步强化CPO的权限和报告职能，并明确达到门槛的数据控制者须强制获得ISMS-P认证。对于境外企业，2025年10月生效的修正案要求全球年收入超过1万亿韩元（约7亿美元）或日均处理100万以上韩国用户信息的企业，须指定境内代理人承担CPO职责。
	加拿大	联邦《个人信息保护与电子文件法》（PIPEDA）适用于在加拿大境内从事商业活动并收集、使用或披露个人信息的私营机构。建议任命数据隐私官（Privacy Officer）作为组织责任制原则的具体体现。 魁北克省：《隐私法》（Law 25）适用于在魁北克开展业务或处理魁北克居民数据的所有企业，要求最高罚款可达2500万加元或全球收入的4%，含私人诉权。
	马来西亚	2024年《个人数据保护法（修正案）》明确引入DPO任命义务。具体触发条件：处理≥2万人数据 或 ≥1万人敏感数据 或涉及定期和系统地监控个人数据的活动。
强制设立	菲律宾	所有个人信息控制者/处理者均须指定DPO。此外，满足以下条件之一者须在国家隐私委员会（NPC）的NPCRS系统注册数据处理系统：（1）雇员超过250人；（2）处理敏感个人信息超过1000人；（3）数据处理可能对数据主体权利和自由产生风险。
	印度尼西亚	所有数据控制者与处理者均须任命DPO。
特定情形下强制设立	中国	根据《个人信息保护法》第52条，达到网信部门规定数量的数据控制者须指定数据保护负责人。GB/T 35273-2020第11.1条b）款具体规定：满足以下任一条件的组织，应设立专职的个人信息保护负责人（PIPO）和个人信息保护工作机构：（1）主要业务涉及个人信息处理，且从业人员规模大于200人；（2）处理超过100万人的个人信息，或预计在12个月内处理超过100万人；（3）处理超过10万人的个人敏感信息。2025年起，处理超过100万人个人信息的企业须通过在线系统报送PIPO信息，PIPO可能承担个人法律责任。
	美国	联邦层面：无统一的综合隐私法。 行业强制：《健康保险携带和责任法案》（HIPAA）要求医疗行业强制指定隐私官员；《格莱姆-里奇-布莱利法案》（GLBA）要求金融行业强制指定隐私官员。 州层面：加州CCPA/CPRA要求专人处理数据主体请求、进行DPIA或审计；弗吉尼亚州、科罗拉多州等也有类似要求。
	印度	《2023年数字个人数据保护法》（DPDPA）规定“重要数据受托人”（由中央政府根据处理量、敏感性、风险等因素指定）必须任命一名DPO和审计员，定期进行审计和数据保护影响评估。
	泰国	《个人数据保护法》（PDPA）第41条规定，以下情形下数据控制者或数据处理者须任命DPO：（1）数据控制者或数据处理者是委员会规定和公布的公共机构；（2）个人数据处理活动因涉及大规模处理个人数据，需定期监控个人数据或系统；（3）处理敏感个人数据（如种族、政治观点、宗教信仰、健康、生物识别数据等）。对于数据控制者位于泰国境外的情况，还须以书面形式授权任命泰国当地代表。
建议/自愿	日本	《个人信息保护法》（APPI）未强制要求设立DPO，但指南建议所有处理个人信息的企业设立个人数据管理负责人（隐私负责人）。2026年正在进行的APPI修订方向包括强化对数据处理方的问责要求，但尚未引入DPO强制条款。
	中国香港特别行政区	非强制，但《个人资料（隐私）条例》指南强烈建议设立DPO，尤其对于电信、金融、医疗等处理敏感数据的行业。
	澳大利亚	尚未对DPO作出强制立法要求。2024年《1988年隐私法》Tranche 1改革引入了法定侵权责任（个人可起诉，最高约47.8万澳元赔偿），Tranche 2改革方向包括取消小企业豁免、72小时泄露通报等，但DPO强制要求仍在讨论中。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

三、行动清单

□ 梳理业务覆盖的 APEC 经济体，按强制设立/特定条件设立/建议分类标注属地规则。

□ 强制设立地区：立即指定 DPO / 隐私官，完成公示与监管报备，新加坡须在PDPC系统登记并公开联系方式。

□ 条件触发地区：对照阈值自查，在中国自查个人信息处理量（超100万人/敏感信息超10万人阈值）；在泰国自查是否涉及大规模处理或敏感数据处理；在印度自查是否被指定为“重要数据受托人”。达标的，在限期内设立专职负责人岗位。

□ 建议设立地区：在日本、中国香港特别行政区、澳大利亚，即使法律未强制，也建议按数据风险与业务规模自愿配置合规负责人。APEC框架下，“责任制”原则要求组织有明确的数据保护责任人。

□ 评估是否涉及个人信息、敏感数据处理规模、是否定期监控等高风险业务，如涉及，建议均设立DPO岗位

□ 同步制定 DPO 职责、培训、考核与内部汇报流程：确保DPO具有独立报告通道（如向董事会或合规委员会直接汇报），并保留完整的履职记录。

Q15

在数据处理原则层面，APEC经济体是否普遍要求数据最小化原则？

（撰写人：秦雨歌）

答：

一、核心提要

APEC隐私框架（2015年版）第三项原则"收集限制"（Collection Limitation）明确规定个人信息的收集应限于与告知目的相关、必要且直接相关的范围，该框架属于非约束性的“软法”，不具备法律强制力。

多数APEC经济体明文规定数据最小化原则：中国、澳大利亚、韩国、加拿大等均明确要求收集限于“必要范围”或“与目的直接相关”。

部分经济体通过“目的限制”或“收集限制”原则间接实现数据最小化效果：日本、新加坡、美国加州未设独立“最小化”条款，但通过“特定目的”、“目的限制”或“收集限制”等义务在功能上约束了数据的过度收集。

二、法规矩阵与专业洞察

分类	主要经济体	规定要求
明文规定	中国	《个人信息保护法》第六条明确规定：“收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。”
	澳大利亚	根据《1988年隐私法》(Privacy Act)中的澳大利亚隐私原则(APP)，机构不得收集个人信息，除非该信息对机构的一项或多项职能或活动是合理必要的。
	韩国	《个人信息保护法》(PIPA)要求个人信息处理者应在实现处理目的所“必要的最小范围内”收集个人信息，遵循“数据最小化”原则。注：该法2023年进行了重大修订，进一步与国际标准接轨。
	加拿大	《个人信息保护与电子文件法》(PIPEDA)包含“收集限制”(Collection Limitation)原则，要求企业仅收集、使用和披露“必要的信息”(necessary information)，并明确规定“组织不得不加区分地收集个人信息”。
间接实现	日本	《个人信息保护法》(APPI)规定了“收集限制”和“目的规范”原则。个人信息处理者应在实现“特定目的”的“必要范围内”利用个人信息，并在取得该“必要”范围外的数据时需另行同意。
	新加坡	《个人数据保护法》(PDPA)不直接规定“最小化”条款，但通过目的限制义务（收集、使用和披露仅限于获得同意的目的）和保留限制义务（在不再需要时删除或匿名化数据）在功能上约束过度收集。
	美国加州	《加州隐私权法案》(CPRA)明确规定，企业收集的个人信息不得用于与告知目的“不相容”的目的，必须遵从目的限制原则。同时，CPRA要求披露数据保留期限，但本身并未规定一个独立的“收集量最小化”义务

APEC隐私框架（2015年版）的九项隐私原则之一为"收集限制"（Collection Limitation）被认为是数据最小化的体现。该原则要求个人信息的收集应限于与告知目的“相关、必要且直接相关”的范围。然而，APEC框架作为“软法”不具有法律强制力。因此，各成员经济体通过各自国内立法来实现这一原则。尚未单独使用“最小化”这一法律术语的经济体（如新加坡、日本），也主要通过“目的限制”、“使用限制”、“收集限制”等同等效力的原则，在监管与执法层面间接禁止数据过度收集。

三、行动清单

□ 建立数据收集必要性评估流程：对企业每个数据处理场景逐字段评估是否满足“直接相关且必要”标准。

□ 审查现有产品/系统的权限申请与数据收集清单：梳理App权限清单，删除与核心功能无直接关联的权限申请，重点核查通讯录、位置、相机、生物识别等高风险权限。

□ 制定数据保留期限政策并落实定期清除：数据最小化既包括收集量的最小化，也包括留存时间的最小化。须建立各经济体留存期限差异清单并定期执行。

□ 将数据最小化合规要求传导至第三方数据供应商和合作方：通过合同条款要求数据处理商严格遵守“最小必要”标准，对提供AI、广告、分析等服务的第三方供应商定期审计其数据收集范围。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

□ 建立APEC主要法域数据最小化标准差异追踪机制：持续跟踪各法域数据最小化规则的立法动态与执法尺度。

Q15

数据泄露事件在APEC各经济体的报告要求是什么？

（撰写人：王丹）

答：

一、核心提要

数据泄露事件报告类型分监管机构通报与向受影响的数据主体通报两类，触发条件、时限不必然同步，通常为“双轨通报”机制。

部分经济体要求发生泄漏后即须通报，部分要求符合特定情形时通报，通常为高风险场景（关键信息基础设施数据、敏感信息、大规模泄露、重大损害风险等）

中国等对关键信息基础设施 / 重大安全事件设半小时/1小时特急上报，印度、俄罗斯等要求6/24小时通报，严于其它经济体标准。

核心报告内容通常涵盖：泄露事件概况、受影响数据类型与规模、已采取的处置措施、补救建议、联系人及客服渠道。

二、法规矩阵与专业洞察

经济体	应通报情形和时限（监管机构）	应通报情形和时限（个人 / 数据主体）	核心报告内容
中国	1、网络安全事件：CIIO≤1小时；中央机关各部门及其直属单位≤2 小时；其他≤4小时；2、重大 / 特别重大网络安全事件：CIIO≤半小时；中央机关各部门及其直属单位≤1小时；其他≤1小时；	对个人、组织合法权益造成危害的，及时通知	事件概况、涉事系统、时间 / 类型 / 影响、已采取措施、原因分析、后续处置、联系人信息
新加坡	应予通报事件：可能致重大损害或 影响人数≥500 人；评估为应予通报事件后3 个日历日内报 PDPC。2025年修订后，最高罚则提升至年营业额10%	通知监管机构后在切实可行范围内尽快通知个人。	泄露详情、受影响人数、处置措施、补救建议、联系人
韩国	通报情形：泄漏≥1000 人数据、敏感/唯一身份标识信息、外部非法访问；泄露后72 小时内报监管；违规罚款上限为全球年收入的3%可豁免：显著降低风险	无前提条件，均须数据泄露后72 小时内通知数据主体；	泄露详情、时间方式、减损建议、处置流程、客服渠道
美国	联邦层面： 医疗健康行业：泄露后须报告监管机构（HIPAA） 金融机构：尽快通报（GLBA） 上市公司重大事件：4个工作日内向SEC报告 州层面： 加州：≥500 人，告知消费者后的15个日历日内向检察长提交通知样本 科罗拉多州：30日内通知受影响个人	特定行业：医疗健康行业发现泄漏后60 天通知个人； 加州：发现后30 日历日内通知受影响消费者	事件描述、信息类型、受影响人数、保护建议、处置措施、 联系方式
日本	满足任一即须报告：需特别保护信息、可能致经济损失的信息、恶意目的或≥1000 人数据发生/可能已发生泄漏； 3-5 天向PPC初报，30 天终报	同监管触发条件 尽快通知	泄露概况、受影响信息 / 人数、处置措施、减损建议、联系人
澳大利亚	判定为“合格泄露”（未经授权访问/披露且可能造成严重损害）后立即通报 OAIC； 时限：发现后30天内完成评估为合格泄漏后立即通报 2024年Tranche 1改革已引入法定侵权责任，个人可起诉，非经济损失赔偿上限约47.8万澳元 Tranche 2改革（含72小时泄露通报）尚在讨论中	与监管通报同步，立即通知个人	组织信息、泄露详情、数据类型 / 规模、 个人应对建议
马来西亚	有合理理由相信泄漏已造成/可能致重大损害； 时限：切实可行情况下尽快通知，且不得晚于发现后72 小时； 重大损害：可能致人身、经济、信用损害、敏感数据、可能被滥用于非法目的、≥1000 人、可能致身份盗窃等高风险	毫不拖延，不晚于报监管后 7 天通知	泄露详情、受影响范围、处置措施、减损建议、联系人
泰国	知悉后72 小时报 PDPC；豁免：不太可能对权利自由造成风险	如可能对个人权利和自由造成高风险，泄露后立即通知该事件及补救措施	泄露性质、数据类型 / 数量、受影响主体、损害程度、处置有效性、安全措施
俄罗斯	发现非法 / 意外泄露侵害个人权利，24 小时报 Roskomnadzor；72 小时内补报结果调查及责任人	与监管通报同步或尽快通知	事件情况、原因、损害、处置措施、授权联系人、调查结果

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体	应通报情形和时限（监管机构）	应通报情形和时限（个人 / 数据主体）	核心报告内容
印度	CERT-In 指令：发现或被告知后6 小时内上报； 适用主体：服务提供商、中介、数据中心、法人实体、政府机构等 系统日志须保留180天，VPS/VPN服务商须保留用户数据5年 不遵守可处IT法案下的罚款或刑事起诉	尽快通知 受影响数据主体	事件详情、日志、配合调查、专人对接、处置措施
加拿大	联邦（PIPEDA）：可能对个人造成重大损害的数据泄露，立即通知加拿大隐私专员办公室（OPC） 魁北克省（Law 25）：在魁北克开展业务或处理魁北克居民数据的企业均适用；罚款最高可达2500万加元或全球收入的4%，含私人诉权（最低1000加元法定赔偿） 2025年11月提出Bill C-15将数据可携权引入PIPEDA	可能对个人造成重大损害的泄露，立即通知受影响个人	泄露类型、受影响人数、处置措施、补救建议、联系人
新西兰	《2020年隐私法》第123条：有合理理由认为泄露已造成或可能造成严重损害的，须在切实可行范围内尽快通知隐私专员 适用主体：各类机构（为个人/家庭事务的个人机构除外）	与监管通报同步，尽快通知受影响个人	事件详情、受影响数据类型/规模、处置建议、联系方式
菲律宾	所有个人信息控制者/处理者均须通知NPC 满足以下条件之一的，须在NPCRS系统注册其所有数据处理系统： 雇员>250人 处理敏感个人信息>1000人 数据处理可能对数据主体权利和自由产生风险 注册后一旦发生泄露，应在NPC规定时限内报告（具体时限以NPC指引为准，搜索结果未明确提供具体天数）	立即通知受影响个人	事件性质、数据类型/数量、受影响主体、处置措施、安全措施

三、行动清单

□ 建立数据泄露分级标准，明确“重大损害”“高风险”“合格泄露”“敏感信息”等触发阈值，建立内部统一分类。

□ 按运营经济体，梳理监管机构 / 个人双轨通报时限与触发条件

□ 制定数据泄露事件响应 SOP，明确责任人与上报路径

□ 准备标准化报告模板，覆盖事件、数据、影响、措施、联系人等核心要素

□ 配置应急联络人，确保特急事件（1/24 小时）可即时上报

□ 开展演练，验证评估—上报—通知—处置全流程时效与合规性

Q17

APEC各经济体对儿童个人信息保护标准有哪些异同？ （撰写人：王孝冉）

答：

一、核心提要

APEC共有21个成员经济体，包括澳大利亚、文莱、加拿大、智利、中国、中国香港特别行政区、印度尼西亚、日本、韩国、马来西亚、墨西哥、新西兰、巴布亚新几内亚、秘鲁、菲律宾、俄罗斯、新加坡、中国台北、泰国、美国和越南。APEC本身并未制定专门针对儿童个人信息保护的统一强制性标准，而是通过Global CBPR提供9项指导原则，这些原则适用于所有个人信息，包括儿童数据，但未对儿童做出明确、专属的特殊规定。

这些原则强调问责制（Accountability）、防止伤害（Preventing Harm）、通知（Notice）、选择（Choice）、收集限制（Collection Limitation）、使用限制、数据完整性、安全保障以及访问与更正。框架鼓励成员经济体根据自身社会、文化、经济和法律背景灵活实施，并支持跨境隐私规则体系，以促进数据自由流动同时保障隐私。

二、法规矩阵与专业洞察

下面就APEC各经济体对儿童个人信息保护标准的异同进行比较：

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

方面	严格监管型（如中国）	代码/指南型（如澳大利亚、加拿大）	自愿框架型（CBPR/Global CBPR参与者，如美国、新加坡）	其他示例
儿童年龄定义与同意门槛	不满14周岁为敏感数据，需监护人单独同意＋身份验证	正在制定《儿童在线隐私代码》（2026年生效），强调年龄适当设计与evolving capacity（儿童逐步自治能力）	美国COPPA针对13岁以下要求可验证家长同意；CBPR早期无专属条款，2026更新后强化儿童数据处理	部分东南亚国家倾向18岁以下家长同意；新加坡等更灵活
保护强度与方法	国家监督强，最小化处理、禁止不当画像/营销，高额处罚	强调设计责任、透明度指南、隐私默认，而非仅依赖同意	基于问责制和第三方认证，企业灵活实施；不取代本地法	韩国/日本发展特定青少年指南；印尼等新兴绑定年龄适当设计
执法与救济	严厉行政处罚＋国家主导审查	监管机构开发专用代码，渐进式合规	自愿认证＋国内执法；CPEA支持跨境合作	执行力度因本地法律传统差异大（普通法vs.大陆法）
文化与侧重	强调家庭/国家保护，可能更严格	平衡家长权利与儿童自治，参考国际最佳实践	商业友好，注重经济流动与问责	西方经济体更注重自治，东亚/东南亚更注重家庭保护
与CBPR关系	国内法优先CBPR认证辅助跨境	代码可与CBPR互补	直接参与CBPR/Global CBPR，认证后互认	部分经济体尚未完全运营CBPR系统

行动清单

□ 明确目标市场儿童年龄定义：制定合规计划前，需精准识别并定义各经济体法律框架下“儿童”的年龄门槛，例如明确规定处理“不满14周岁”（中国）或“13岁以下”（美国）用户数据时的特殊义务。

□ 重建用户同意与年龄验证机制：在应用和网站中部署年龄验证技术。对达到法定儿童年龄的用户，须采用符合当地法规的“可验证的家长/监护人同意”机制（如中国的身份核验、美国的家长付款验证等）。

□ 审查并遵守数据最小化与目的限制：如中国《个人信息保护法》、韩国PIPA要求，仅收集为特定、必要目的所需的最少量儿童数据。同时遵循新加坡PDPA等法律的目的限制要求，不将已收集的儿童数据用于无关目的。

□建立跨境数据传输合规体系：依据Global CBPR论坛的认证体系和参与经济体的跨境规则（如越南2025年生效的《个人数据保护法》限制数据出境），建立内部数据跨境传输政策和合同范本。

□ 建立全球（APEC区域）儿童隐私合规追踪机制：持续监控各主要经济体的立法动态，及时更新合规要求。重要关注点包括：美国COPPA规则的定期更新、澳大利亚新的在线隐私准则、澳大利亚隐私法的改革草案等。

Q18

APEC各经济体对隐私政策文件在形式与语言方面提出了哪些要求（如必须采用当地语言）？这些要求在跨境业务中可能带来哪些合规影响?

（撰写人：戴佳兵）

答：

一、核心提要

无统一语言强制要求：APEC隐私框架及CBPR体系并未强制规定隐私政策必须使用当地语言，但各成员经济体的国内法可能提出具体语言要求（如日本要求提供日文版、韩国要求韩文版）。

多语言策略成必需：在面向多个APEC经济体的跨境业务中，企业通常需要准备多语言版本的隐私政策，以满足各地“通知”原则中的“清晰、易懂”要求，单一语言版本难以满足合规需要。

形式要求趋同化：APEC九大隐私原则要求隐私政策必须“清晰、醒目、及时”（clear, conspicuous, timely），这与GDPR的透明度要求方向一致，但执行细节因经济体而异。

二、法规矩阵与专业洞察

1.APEC主要成员经济体对隐私政策文件的形式与语言要求

成员经济体	语言要求	形式/内容要求
日本	原则上需提供日文版；外文版可作为补充	须载明使用目的、收集范围、第三方提供、咨询窗口等
韩国	强制要求韩文版；英文版不视为合规替代	须包括信息收集项目、使用目的、保留期限、权利行使方式
新加坡	无强制语言规定，但推荐使用英文；面向本地消费者的宜提供中文/马来文/泰米尔文版本	须包括收集目的、使用披露方式、访问更正权利、联系方式等，符合PDPA九项法律义务
澳大利亚	推荐英文；面向特定社区的宜提供相应语言	APP隐私政策须包括：信息类型、收集方式、目的、披露对象、跨境传输、访问更正流程等
墨西哥	强制西班牙文须	包括负责人身份、收集敏感信息时的明确同意、ARCO权利行使方式
加拿大	英文/法文均可（双语国家要求）	须在收集时或之前告知目的、使用范围、第三方披露，遵守十项公平信息原则（包括责任、同意、透明度等）

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

成员经济体	语言要求	形式/内容要求
美国	无强制语言规定，但实践中以英文为主；面向特定群体（如西班牙语社区）建议提供相应语言	FTC执法标准：隐私声明必须“清晰、醒目、真实”，不得误导消费者；各州法律（如加州CCPA）规定须披露的信息类型、消费者权利等
中国台北	实践中以繁体中文为主	须依据《个人资料保护法》制定隐私政策，载明收集目的、数据类型、使用范围、第三方分享、权利行使方式等内容
印度	DPDPA 2023要求同意语言必须使用英语以及印度宪法第八附表规定的所有22种官方语言；隐私通知同样须提供多语言版本	须在收集前提供通知，披露处理的数据类型、目的、数据主体权利行使方式、投诉渠道；重要数据受托人须任命数据保护官
菲律宾	英语为主要实践语言，他加禄语（Tagalog）同为官方语言，建议准备双语版本	须根据NPC指引制定隐私政策，涵盖收集目的、数据类型、使用限制、数据主体权利、安全措施等
新西兰	实践中以英文为主	须遵守2020年隐私法中的信息隐私原则（IPPs），包括收集目的告知、数据安全、访问更正权利等

1.专业洞察与合规影响分析

“通知”原则的语言内涵要求

APEC隐私框架的“通知”（Notice）原则要求隐私政策必须“清晰、醒目、及时”地告知个人信息的收集、使用和披露方式。这意味着：

语言可及性：如果企业仅提供英文隐私政策，而目标市场消费者以当地语言为主（如日本、韩国、墨西哥），则难以认定为“清晰、易懂”，可能构成合规缺陷。

多层披露模式：实践中，许多企业采用“分层通知”（layered notice）策略——第一层提供摘要式关键信息（使用当地语言），第二层提供完整政策（通常为英文）。

三、行动清单

□ 目标市场语言要求调研：对拟进入的每个APEC经济体，调研国内法是否对隐私政策有强制语言要求。

□ 多语言版本准备：根据目标市场语言需求，准备当地语言版本的隐私政策，确保内容与基准版本一致。

□ 建立版本控制机制：制定多语言隐私政策的同步更新流程，避免版本差异导致的法律风险。

□ CBPR认证准备：若计划申请CBPR认证，确保隐私政策符合责任代理对“清晰、醒目”的语言要求。

□ 前端语言适配：网站/APP应支持根据用户地理位置或语言偏好自动展示对应语言版本的隐私政策，并在首次访问时提示确认。

□ 定期审查更新：每年审查各经济体语言要求的变化（如是否有新的强制语言立法），及时调整。

□ 评估合规成本：综合考量多语言版隐私政策的起草、翻译、审核、维护成本与法律风险，确定优先覆盖的市场和语言范围。

Q19

APEC各经济体采集用户行为数据（包括App SDK、Cookies）的合法性基础有哪些？用户同意在其中扮演何种角色？ **（撰写人：陈瑜琪）**

答：

一、核心提要

APEC各经济体采集用户行为数据的合法性基础包括隐私框架九项原则和其他具体基础；

用户同意是众多合法性基础中的核心，但存在一些例外情况；

不同经济体对采集用户行为数据有不同的规定，应针对目标经济体进行相应的合规准备。

用户行为数据（App SDK、Cookies）采集面临的合规复杂性最高：对于"非必要"的跟踪技术（如用于行为广告的Cookies），新加坡、泰国等经济体以同意为实践基准线；敏感用户画像数据（涉及健康、宗教、政治倾向等信息）通常需获取单独明确同意。

二、法规矩阵与专业洞察

1.合法性基础

APEC隐私框架的九项原则	预防损害	防止信息滥用对个人造成损害
	告知	采集前或采集时提供清晰、易获取的隐私政策声明
	收集限制	信息采集限于与收集目的相关的范围，以合法、公平的方式进行
	使用限制	仅用于实现目的，除非已获同意或法律要求
	选择	提供清晰、显著、易懂且可负担的同意机制
	完整性	确保个人信息准确、完整并及时更新
	安全保障	采取适当措施保护个人信息
	访问与更正	个人有权查询并更正其个人信息
	问责制	企业在将个人信息转移给第三方时，必须确保第三方也遵守原则
具体情况	同意、合法利益、法定义务、合同履行等	

APEC各经济体采集用户行为数据的合法性基础主要建立在APEC隐私框架确立的九项原则上，同时也建立在各经济体成员设立的具体合法性基础之上。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

核心地位	在大多数APEC经济体中，同意是处理个人数据的首要合法性依据
	用户同意是数据跨境转移的必要条件
	敏感数据通常需要单独、明确、有时是书面的同意
	企业要获得CBPR认证，必须建立用户同意机制
例外情况	为提供用户所要求的产品或服务，或者法律另有规定时，信息的后续使用有时无需再次取得同意
	当收集的是用户已公开的信息时，有时无需取得用户同意

用户同意是十分重要的合法性基础之一，但并非唯一基础，如履行合同、法律要求等也可作为依据。同时，不同APEC经济体对用户同意有不同的具体要求，存在一些例外情况，这种差异反映了各经济体在文化、法律传统等方面的不同。

三、行动清单

☐ 已确认在各目标APEC经济体的数据处理活动符合当地数据保护法律要求

☐ 已及时发现和纠正自身潜在的合规风险

☐ 已建立同意机制，针对不同经济体采用不同的同意要求

☐ 已评估是否存在可以免除用户同意的法定情形

☐ 已进行经济体相关要求的监控，定期更新合规策略

Q20

在APEC跨境营运中，若第三方处理者发生数据泄露或非法买卖，各方（如第三方处理者、企业相关人员等）的责任如何界定？

（撰写人：戴佳兵）

答：

一、核心提要

获得APEC CBPR认证可作为区域内的统一合规基线，使企业在参与经济体内以一套标准满足多个数据保护要求，显著降低重复合规成本。

企业通常采用CBPR认证 + 本地法遵从 + 转让定价/合同机制的组合策略，在区域统一标准与各经济体国内法之间取得平衡。

APEC正推动跨境隐私执法安排（CPEA）和责任代理制度的深化，未来有望实现“一次认证、多地互认”的“信任标志”模式。

APEC建立了专门针对数据处理者的认证体系——数据处理者隐私识别（PRP）体系。通过PRP认证可证明处理者具备符合CBPR要求的隐私保护能力，帮助数据控制者识别和选择合格的处理者。

二、法规矩阵与专业洞察

1.法规矩阵比较：APEC CBPR vs. 各成员经济体国内法 vs. GDPR

比较维度	APEC CBPR体系	各成员经济体国内法（以日、韩、新为例）	欧盟GDPR
法律性质	自愿性、问责制认证体系	强制性国内法，具有域内执法效力	具有域外效力的强制性法规
适用主体	仅适用于数据控制者（有单独的PRP体系适用于处理者）	控制者+处理者	控制者+处理者
核心标准	APEC隐私框架九大原则	各经济体以APEC框架为基础制定，但存在差异	GDPR 7大原则 + 具体权利义务
跨境传输机制	CBPR认证企业之间可自由传输	通常允许依据CBPR认证豁免部分程序，但保留更高标准适用权	需依赖充分性认定、SCCs、BCRs
监管方式	第三方责任代理认证 + 经济体隐私执法机关	各经济体监管机构直接执法	各成员国DPA直接执法
对CBPR的认可	—	通常认可CBPR为合规证明，但国内法更严格时以国内法为准	不认可CBPR为充分性认定替代

三、行动清单

☐ 评估CBPR认证适用性：判断企业是否属于“数据控制者”（而非纯处理者），评估业务覆盖的经济体中是否有足够多的CBPR参与方。

☐ 进行差距分析：对照APEC隐私框架九大原则与各经济体国内法，识别CBPR未覆盖的“更高标准”要求。

☐ 申请CBPR/PRP认证：选择所在经济体认可的问责代理，启动认证程序，建立统一的区域合规基线。

☐ 建立国内法补充遵从机制：针对日本、韩国、新加坡等有更高标准的国家，制定专项合规措施（如DPO任命、泄露通知流程）。

☐ 完善合同工具箱：准备标准化的数据跨境传输协议模板，适用于与非CBPR认证方的数据传输场景。

☐ 内部政策统一化：以APEC九大原则为基础，修订全球统一的数据保护政策，减少多标准并行的管理复杂度。

☐ 关注监管互认动态：定期跟踪APEC框架下的新倡议（如WTA的三层信任生态系统），评估参与行业互认计划的可能性。

☐ 定期再认证与审计：确保每年接受问责代理的重新认证审查，维持CBPR认证有效性。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q21

在APEC各经济体中，如何判断某项数据处理活动需开展“隐私影响评估”（如PIA、DPIA等）？ **（撰写人：王丹）**

答：

一、核心提要

多数 APEC 经济体采用高风险触发模式：敏感个人信息、自动化决策、大规模处理、数据跨境、新技术应用等普遍强制要求进行PIA/DPIA。

跨境经营业务企业建议按最严口径统一开展PIA/DPIA，避免多地重复合规成本。

二、法规矩阵与专业洞察

经济体	强制 / 建议	核心触发情形
中国	强制	敏感个人信息；自动化决策；委托/提供/公开个人信息；跨境提供；其他对个人权益有重大影响的处理活动。
新加坡	强制	新系统 / 新流程；处理方式变更；组织调整；新型数据；依赖推定同意/合法利益
韩国	强制	公共机构：大规模/敏感/内外部系统联动/系统变更； 私营机构：AI/生物识别/跨境/敏感/自动化决策
美国	强制	联邦： 行政机关开发/采购涉及个人信息处理的IT 系统； 州层面：加州：销售/共享、敏感信息、自动化决策、生物识别等
加拿大	强制	联邦：新项目；重大变更；用于决策目的
马来西亚	强制	指南征求意见稿规定：敏感数据超 1 万人；自动化决策超 1 万人；一般数据超 2 万人；公共监控/创新技术/自动化决策/追踪位置、行为数据/弱势群体
印尼	强制	自动化决策；特定敏感数据；大规模处理；系统评估 / 监控；数据匹配；新技术应用；限制个人权利等
越南	强制	全量处理活动（含跨境）、法规变更；微型 / 家庭企业除外
日本	建议/非强制	私营机构非强制，指南建议进行PIA，敏感信息、AI 自动化决策等高风险场景强烈建议
中国香港特别行政区	建议/非强制	未强制，指南建议涉及高隐私风险、大量个人资料、隐私侵犯技术、组织实践变更时，进行PIA

三、行动清单

□ 跨境业务按最高合规标准统一实施，降低多地监管冲突风险。

□ 强制经济体留存评估记录，非强制经济体保留评估痕迹用于合规举证。

□ 如落入敏感个人信息、自动化决策、大规模处理、跨境、高隐私风险新技术等，一律前置开展PIA/DPIA。

□ 如仅在特定经济体开展业务的，对照目标经济体要求开展DPIA/PIA。

□ 评估处理活动是否对个人法律地位、财务、健康、声誉产生重大影响。

□ 新系统、新流程、组织 / 流程重大变更，同步更新 PIA/DPIA 报告。

Q22

在同时适用多个APEC成员经济体数据保护要求的情况下，企业通常可以通过哪些合规策略来协调差异、降低整体合规成本？ **（撰写人：戴佳兵）**

答：

一、核心提要

Global CBPR/PRP认证是多国政府联合背书的跨境数据传输机制，获得认证后可作为区域内的“信任凭证”，在多个参与经济体中简化或替代复杂的合同谈判，大幅降低重复合规成本。

对于已持有或正在申请新加坡DPTM等本地认证的企业，探索“双重认证”或“整合认证”方案，整体可节省约50%的认证成本，是最具性价比的合规投入策略。

CBPR提供的是“最低共同标准”，企业需识别各经济体国内法中的“更高标准”（如日本的数据泄露72小时报告、韩国的DPO任命要求），并建立专项补充遵从机制。

二、法规矩阵与专业洞察

1.五大合规协调策略

策略一：CBPR/PRP认证作为区域合规“锚点”

Global CBPR体系是唯一由美国、日本、韩国、新加坡、澳大利亚等15个以上经济体政府联合背书的跨境数据传输机制。获得认证后，企业可在参与经济体内以一套标准满足多地要求，替代冗长的数据传输合同谈判，显著降低法务成本。数据控制者申请CBPR，数据处理者申请PRP，认证有效期一年，需每年续认。

认证流程分为四步：内部差距分析（对照APEC九大隐私原则）、更新政策和流程、聘请问责代理进行评估、审计通过后获得认证。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

策略二：整合认证降低成本

对于已持有或正在申请新加坡DPTM等本地认证的企业，建议采用整合认证路径。由于两项认证的评估维度大量重叠（均涵盖问责制、数据主体权利、泄露响应等），共用评估材料可节省约50%的认证成本，是最具性价比的合规投入策略。新加坡信息通信媒体发展局（IMDA）已为组织提供一站式申请流程，帮助其同时申请DPTM认证和APEC CBPR/PRP认证。

策略三：国内法“就高不就低”补充遵从

CBPR提供的是“最低共同标准”，各经济体国内法可能设定更高要求，企业须逐一识别并补充遵从：

日本：数据泄露72小时内报告——在CBPR基础上建立专项泄露响应流程

韩国：DPO任命及数据保护影响评估——任命本地DPO并执行PIA

新加坡：未经同意的营销行为严格限制——建立独立的营销同意管理机制，并遵守“勿拨号”(DNC)登记册等规定。

策略四：合同机制兜底

对于与非CBPR认证方（如中国境内企业）的数据传输，需通过合同确保保护水平：在跨境传输协议中纳入APEC九大原则，约定问责代理作为争议解决机构。在申请认证前的过渡期，标准化的跨境数据传输合同模板可以作为有效的合规工具。

策略五：利用Global CAPE获取执法便利

全球隐私执法合作安排（Global CAPE）已有27个隐私执法机构参与，可在跨境执法时协助获取证据、协调调查。企业面临多国同时调查时可借此获得程序便利。目前参与机构包括澳大利亚、加拿大、中国香港特别行政区、韩国、马来西亚、墨西哥、新西兰、菲律宾、新加坡等经济体的隐私执法机构。

1.策略协同逻辑

上述策略形成“三层防御”：CBPR认证解决80%常规场景；国内法补充覆盖20%特殊要求；合同机制为非认证场景兜底。整合认证是优化降本路径，Global CAPE是执法风险缓释工具。CBPR提供基础框架，但在面对日本、韩国、新加坡等更强国内法约束时，仍需本地化补强，两者结合才能实现真正的低成本合规。

三、行动清单

- □ 判断企业属于数据控制者（CBPR）还是处理者（PRP），评估认证适用性
- □ 对照APEC九大原则与各经济体国内法，进行差距分析
- □ 选择问责代理（如新加坡IMDA）申请CBPR/PRP认证
- □ 若已持有或正在申请本地认证，评估整合认证可行性
- □ 针对日本、韩国、新加坡等国更高标准，建立专项补充机制
- □ 准备标准化数据跨境传输协议模板，用于非认证方场景
- □ 以APEC九大原则为基础统一内部政策，减少多标准并行
- □ 每年接受问责代理重新认证，维持CBPR有效性

Q23

企业如何就其数据保护与隐私合规的问题，在全球通用框架与当地法律特定要求之间取得平衡？

（撰写人：王孝冉）

答：

企业要在全球通用隐私框架（如Global CBPR）和当地具体法律要求之间取得平衡，核心是采用“全球最高标准作为基线 + 模块化本地适配”的做法。这种方法既能控制合规成本，又能满足不同辖区的监管需求，同时支持跨境数据流动。Global CBPR（是一个自愿性的认证框架，基于问责制。它提供一套统一的程序要求，重点强化敏感个人信息和儿童个人信息的处理，包括风险评估、家长同意验证以及防止潜在伤害的措施。关于企业如何在全球通用框架与当地法律特定要求之间取得平衡建议采取如下措施：

一、先做数据映射和风险评估

全面梳理数据流向，特别标记涉及儿童或敏感数据的部分。然后开展隐私影响评估（PIA），重点检查跨境场景和高风险处理活动。2026年Global CBPR更新明确要求企业评估是否处理儿童个人信息，并采取相应保障措施。这一步能帮助早发现差距。合规建议强调，在开展任何合规路径选择之前，必须先做数据流映射——弄清楚哪些数据往哪流、经过谁的手、存在哪个云上、谁有访问权限。没有数据流图，路径选择就是空谈。Global CBPR框架本身也要求处理者、代理人、承包商或其他服务提供者在个人信息被转移时，及时通知数据控制者。

二、建立全球统一政策 + 本地模块

以最严格的标准（如GDPR的数据最小化、透明原则或PIPL的儿童保护要求）设定集团级全球基线政策。然后为不同辖区开发“附加模块”：中国模块增加出境安全评估流程，美国模块加入COPPA家长验证机制，欧盟模块处理数据主体权利响应时限等。这样政策既保持一致性，又能灵活适应本地检查。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

三、利用认证和传输工具

申请Global CBPR认证，通过认可的第三方审核机构（如TrustArc、BBB National Programs）

完成审核。认证后，在参与辖区内可简化数据转移合规。对于更高要求或非覆盖地区，结合标准合同条款（SCCs）、加密技术或假名化等措施。同时要求供应商提供对应的合规证明。

四、注意各法域的特殊要求

各法域存在显著差异，需要在统一基线基础上补充本地模块。

五、建立动态合规调整机制

合规不是一次性的工作。企业应关注当地法规的最新变化，及时调整数据保护措施。建议：定期对合规情况进行内部审计；建立全球数据保护协调机制，确保各法域的负责人信息互通、标准对齐；对高风险国家/地区设立专门的合规团队。

Q24

APEC经济体对于敏感个人数据的监管通常体现在哪些方面？

（撰写人：秦雨歌）

答：

一、核心提要

1.APEC隐私框架本身未区分"敏感数据"与普通数据，但主要成员经济体均通过国内立法建立了敏感数据专项保护规则，且普遍以"一旦泄露将导致严重权益损害"作为界定标准，形成高度一致的认定逻辑

2.敏感数据核心加重义务呈现“事前约束+事中控制+事后保障”的监管链条：各经济体普遍要求比普通数据更严格的同意形式（单独同意/明示同意），限制二次利用范围，并施加更高标准的安全保障措施。

3.生物识别、健康信息是APEC区域监管最严的两类敏感数据：中国、韩国、澳大利亚、越南等均将生物识别和健康信息列为敏感类别并设加重义务。

4.2025-2026年呈现关键立法动态：日本APPI正探索部分场景下敏感个人信息处理的"有限同意豁免"（AI开发、统计用途）；韩国2026年PIPA修正案通过，进一步强化数据保护义务并引入最高全球营收10%的行政处罚；越南PDPL于2026年1月1日生效，新增强制性DPIA与跨境传输影响评估义务；美国加州CPRA于2026年1月1日对敏感个人信息处理正式启动强制性书面风险评估要求。

二、法规矩阵与专业洞察

经济体	主要列举的敏感数据类型	核心加重义务
中国	生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹、14周岁以下未成年人信息	①须具有特定目的和充分必要性；②须取得单独同意；③须额外告知处理必要性及对权益影响；④须事前开展个人信息保护影响评估；⑤14周岁以下须父母或监护人同意
韩国	思想信仰、工会会籍、政治观点、健康信息、性生活、遗传信息、犯罪记录、生物识别信息	①原则上禁止处理，例外情形须获另行明示同意；②须与其他同意项分开单独获取；③须落实超出一般个人信息的安全保护措施；④2026年2月PIPA修正案通过：引入最高全球营收10% 的行政处罚、强化CPO权限
日本	种族、信仰、社会身份、病历、犯罪记录、身体/智力/精神障碍	①须取得明示同意方可收集；②原则上禁止未经同意向第三方提供；③须建立安全管理措施；④2026年改革方向：在AI开发/统计用途等场景探索有限"同意豁免"，要求风险评估与保护措施
澳大利亚	种族/民族、政治观点、宗教信仰、工会会籍、性取向、犯罪记录、健康信息、遗传信息、生物特征信息	①一般须获明示同意（默示同意不够）；②APP 6要求二次利用须与初始目的"直接相关"（比一般信息"相关"标准更严）；③APP 7禁止以直接营销为目的处理敏感信息，除非当事人已就该目的明确同意；④正在制定儿童在线隐私法（2026年征求意见稿），要求生物特征等敏感信息处理须符合"儿童最佳利益"审查
泰国	健康信息、宗教信仰、生物识别数据（如人脸信息）、种族等	①原则上须获得明确同意，同意须以"单独勾选""书面确认"等可追溯形式获取；②极个别豁免情形须留存"豁免情形的证明材料"；③PDPC持续推进执法审计
美国加州	SSN/驾照/护照、金融账户及登录凭证、精确地理位置、种族/民族、宗教信仰、工会会籍、私人通讯、遗传/生物识别、健康信息、性取向	①用户有权限制使用敏感个人信息（须提供"限制使用敏感个人信息"功能入口）；②禁止用于与收集目的无关的推断；③须披露敏感信息的保留期限；④2026年1月1日起，处理敏感个人信息前须完成书面风险评估
越南	政治/宗教观点、健康信息、生物识别、遗传数据、性取向、犯罪记录、金融账户、地理位置	①处理前须明确告知当事人所处理为敏感数据；②须告知当事人同意的具体内容后方可处理；③须指定个人数据保护专员并通报网络安全部门；④所有数据处理（含敏感）须事前完成数据保护影响评估（DPIA）；⑤跨境传输须完成CTIA，违规罚款上限为上一财年营收的5%
新加坡	传统上未在立法层面区分"敏感"与"一般"，遵守PDPA即可处理	①法律层面未单独区分"敏感"类别，但对所有个人数据统一适用PDPA原则；②2024年9月起要求所有公司任命DPO并公开联系方式；③2020年修正案引入强制数据泄露通报制度

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

敏感数据监管呈现“高门槛、高责任”特征。与普通个人信息不同，敏感数据的处理被视为“高风险业务场景”。各法域普遍将健康信息、生物识别信息、金融账户信息、种族/民族、政治观点、宗教信仰、工会会籍、性取向、犯罪记录列为敏感数据。

三、行动清单

建立跨法域“敏感数据识别清单”：以各法域普遍认可的敏感数据类型为基础，结合业务覆盖经济体的本地扩展类别，制定统一的敏感数据分类清单，标注每类数据在适用法域对应的法律依据及加重义务；

对处理敏感数据的场景落实“单独同意”机制：在明确要求单独同意的法域，确保敏感数据同意界面独立于一般数据处理同意，不得与其他同意项捆绑；

重点关注生物识别信息的安全保障措施：生物识别信息是当前执法最活跃、风险最高的敏感数据类型，须确保加密存储、最短期限留存、访问权限严格管控；

对处理敏感数据的活动按法域差异落实评估要求：部分法域（如中国）明确规定处理敏感个人信息须事前开展数据保护影响评估并留存报告；其他法域虽无独立评估要求，但通过单独同意、限制使用、安全保障等措施实现同等保护效果。

建立敏感数据合规动态追踪机制：持续跟踪各法域敏感数据保护规则的立法动态与执法尺度，重点关注新出台或即将生效的法律以及通过执法案例确立更高保护标准的法域。



亚太数字经济与人工智能法律问答指南(蓝皮书)
Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q25

APEC CBPR（跨境隐私规则）体系是什么？其在促进跨境数据流动方面发挥了何种作用？（撰写人：戴佳兵）

答：

一、核心提要

认证机制：APEC CBPR体系是基于APEC隐私框架建立的自愿性、可认证的数据隐私保护机制，企业通过认证证明其符合国际认可的数据保护标准。

降低壁垒：它通过提供“一张认证、区域内多国互认”的模式，减少企业因应对不同国家法规而重复合规的成本，促进亚太地区可信的数据流动。

信任基石：CBPR体系的核心是建立监管机构间的互信，使数据可以更自由地从认证企业流向其他认证企业或经济体，从而支撑数字贸易发展。

二、法规矩阵与专业洞察

APEC CBPR体系并非一个具有法律强制力的“条约”，而是一个由APEC经济体成员自愿参与并建立的多边数据隐私认证机制。其核心在于通过统一的企业隐私保护标准，解决APEC区域内各经济体数据保护法规差异带来的障碍。该体系由数据隐私小组（Data Privacy Subgroup）通过联合监督小组（Joint Oversight Panel）进行统一管理，建立了经济体、责任代理（Accountability Agent）和申请组织等三级认证制度。

比较维度	APEC CBPR体系	欧盟GDPR
法律性质	自愿性、多边互认的认证体系	具有域外效力的强制性法规
适用主体	申请并获认证的企业	任何处理欧盟用户数据的主体
核心原则	预防损害、通知、限制收集、安全保障等9项隐私原则	合法性、公平透明、目的限制、数据最小化等7大原则
跨境传输机制	通过CBPR体系认证，可在成员经济体间自由传输	需依赖充分性认定、标准合同条款(SCCs)、约束性公司规则(BCRs)等机制
监管模式	由各成员经济体指定的“问责代理机构”进行认证与监督	由各欧盟成员国的数据保护机构直接监管

BPR体系的作用可类比为在APEC区域内搭建了一条“数据高速通道”。企业一旦获得CBPR认证，就表明其隐私保护水平达到了APEC框架下的高标准。有学者指出，该模式体系构建的初衷是在一套既定的隐私原则以及规则框架之下，以扩大行为体共识的方式来平衡个人隐私保护和数据自由流动，推动区域经济一体化持续增长。对于在多个APEC经济体（如美国、日本、新加坡、澳大利亚等）开展业务的企业而言，CBPR认证可以替代部分经济体复杂的逐个国家申报或合同签署要求，从而简化合规流程、提升数据流动效率。

需要注意的是，2022年4月21日，美国、加拿大、日本、新加坡、菲律宾、韩国和中国台北共同发表声明，正式建立“全球跨境隐私规则论坛”（Global CBPR Forum），并逐步将各自的APEC CBPR运营向新论坛过渡。2025年6月，全球CBPR认证正式启动；全球CBPR论坛目前成员包括：澳大利亚、加拿大、日本、韩国、墨西哥、菲律宾、新加坡、中国台北和美国。

三、行动清单

评估企业当前的业务是否主要在APEC成员经济体内开展，判断参与CBPR体系的必要性。

梳理企业现有的数据隐私政策，对照APEC隐私框架九大原则进行差距分析。

确认企业总部所在地及数据处理活动所涉的APEC成员经济体是否为CBPR体系正式成员。

若决定申请，需选择所在经济体认可的“问责代理机构”并接受其评估与监督。

将CBPR认证作为企业内部数据合规的“基准线”，并定期进行审计以维持认证。

Q26

APEC哪些经济体要求数据本地化？（撰写人：王丹）

答：

一、核心提要

涉及国家：APEC各经济体中中国、俄罗斯、印尼、越南四个经济体在国家级立法中明确要求数据本地化，其余多数经济体无强制本地存储规则。

涉及数据类型和行业：数据本地化要求多覆盖个人信息、重要数据、关键信息基础设施数据以及金融、医疗等特定行业数据。

前置条件：部分国家数据出境需满足安全评估、监管访问/批准等前置条件。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

国家	适用主体	核心数据范围	本地存储要求	其它要求
中国	关键信息基础设施运营者、大规模个人信息处理者、重要数据处理者	个人信息、重要数据；金融 / 医疗 / 地理信息	境内强制存储	出境须安全评估等
俄罗斯	境内外数据运营商	俄罗斯公民个人数据	优先使用俄罗斯数据库	向监管机构备案存储地点
印度尼西亚	公共 电子系统运营商（ESO）、私营 ESO、金融机构	电子系统数据、用户数据	公共 ESO 强制本地；私营 ESO 可境外	私营 ESO 境外存储的前提条件：提供监管机构访问权限、不影响执法；金融机构境外处理需 OJK 批准。
越南	境内实体、特定领域国外实体	个人信息、用户创建数据、用户关系数据	境内实体强制本地存储；符合条件的国外实体须保存数据至少2年	特定国外实体须设分支机构 / 代表处

中国、俄罗斯、印度尼西亚、越南四个 APEC 经济体，均在国家级立法层面确立数据本地化法律义务，整体以境内存储为原则、跨境提供为例外。

中国针对关键信息基础设施运营者、大规模个人信息和重要数据处理者，均需将境内产生的个人信息与重要数据在境内存储；确需出境应通过数据出境安全评估。同时在金融、医疗等特定行业实施更严格的本地化规则。

俄罗斯聚焦公民个人数据保护，要求境内外数据运营商、处理者收集俄罗斯公民个人数据时，必须优先使用俄罗斯数据库开展记录、存储、整理等处理活动，并向监管机构报备数据存储设施地点，以保障数据处理全流程可管可控。第 23-FZ 号联邦法律进一步明确不得使用位于俄罗斯联邦境外的数据库初始收集和处理俄罗斯联邦公民的个人数据。

印度尼西亚按主体类型区分义务：公共电子系统运营商必须境内管理、处理与存储数据；私营运营商可境外存储，但需保障监管与执法有效访问，同时跨境传输须与监管机构协调（提交报告等）。金融机构还需事先取得监管批准方可境外设立数据中心或处理数据。

越南对境内实体与境外企业实行双轨规制：境内实体需存储个人信息、用户创建数据及关系数据；而境外实体的本地化义务并非一律自动触发。根据实施细则第53/2022/ND-CP号法令（Decree 53/2022/ND-CP）第26条，须同时满足以下条件：

（a）经营电信服务、电子商务、在线支付、社交媒体、网络游戏等十类受规管业务之一；（b）收到公安网络安全部（A05）的正式数据存储要求（即其服务被用于违反越南网络安全法，公安部网络安全和高科技犯罪预防控制司已书面通知并要求企业配合且未予配合）。满足条件的外企须在越南境内存储数据并留存至少2年，须同时在越南设立分支机构或代表处。

整体来看，四地本地化规则均覆盖个人信息与关键业务数据，出境均设置安全评估、监管批准、执法访问等条件，企业跨境布局需按经济体逐一匹配主体、数据类型、行业与出境程序要求。

三、行动清单

- ☐ 梳理业务覆盖的 APEC 经济体，识别是否涉及中/俄/印尼/越
- ☐ 按当地规则界定需本地存储的数据类型（个人信息/重要数据）和特殊主体类型（如关键信息基础设施、公共机构、大规模信息处理者）
- ☐ 评估数据出境需求，准备安全评估、监管申请、备案等材料
- ☐ 涉及越南业务的外企，评估是否落入须设立分支机构/代表处情形
- ☐ 建立数据存储地点台账，留存出境合规记录

Q27

APEC哪些经济体要求跨境传输前需要当地主管机关审批或备案?

（撰写人：王丹）

答：

一、核心提要

涉及国家：中国、俄罗斯、印度尼西亚、越南四个 APEC 经济体，均要求跨境数据传输前履行审批、合同备案、通知或提交评估报告等官方程序。

监管方式：各国监管按数据类型、主体规模、传输场景分类管控，如俄罗斯和越南针对本国公民个人数据的跨境传输进行监管，中国按主体规模和数据类型实行不同的监管方式，而印尼按公共机构和私营机构分类进行管控。

特定行业：除通用监管外，金融等特定行业可能需额外取得行业主管部门批准，合规需兼顾通用规则与专项要求。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

经济体	监管方式	适用场景	事前义务
中国	数据出境安全评估/标准合同备案	安全评估：1. 重要数据出境；2. 根据2026年1月国家网信办发布的政策问答，关键信息基础设施运营者以外的数据处理者，自1月1日起累计向境外提供10万人以上、不满100万人个人信息（不含敏感个人信息）或者不满1万人敏感个人信息的，可以通过订立标准合同方式出境。若累计出境超过100万人个人信息（不含敏感个人信息）或者超过1万人敏感个人信息的，则应当申报安全评估；3. 累计提供超过一定数量个人数据的出境。其它一般情形：标准合同备案。	1. 申报国家网信部门安全评估 2. 标准合同生效后10 个工作日内向省级网信部门备案
俄罗斯	个人数据跨境传输通知 / 批准	向境外传输俄罗斯公民个人数据	1. 事前向 Roskomnadzor 提交通知； 2. 向非充分保护国家传输需获明确批准。
印度尼西亚	数据跨境协调 / 批准	1. 公共 ESO 数据出境 2. 私营 ESO 数据出境 3. 金融机构境外设数据中心	1. 向通信信息部事前 / 事后报告； 2. 公共 ESO 出境需委员会确认； 3. 金融机构需 OJK 事前批准。
越南	个人数据跨境传输影响评估提交	越南公民个人数据向境外传输	数据处理开始后 60 日内提交 CTIA 报告至公安部，变更需更新

在 APEC（亚太经合组织）经济体中，跨境数据传输的监管环境各异。虽然大多数经济体通过“标准合同（SCCs）”或“认证（如 CBPR）”允许数据流动，但有如下几个核心经济体设定了明确的政府审批、备案或事先通知要求。

中国构建双轨制数据出境监管：针对重要数据、大规模个人信息出境、自1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息的情形必须申报国家网信部门安全评估；而其它个人信息出境可签署标准合同，并在生效后 10 个工作日内向省级网信部门备案。

俄罗斯针对俄罗斯公民个人数据跨境进行监管，以事前通知为基础，同时区分接收国保护水平，向非充分保护国家传输需等待Roskomnadzor 审查，如果在 10 个工作日内监管机构未做出禁止或限制的决定，操作者方可开始传输，强化个人数据跨境安全。

印尼按主体类型差异化监管：公共 ESO 数据出境需经监管机构视特定情形批准，私营 ESO 需和通信信息部进行跨境传输协调，金融机构境外处理数据必须取得OJK 事前批准。

越南要求跨境传输越南公民个人数据时，在跨境传输开始后 60 日内提交跨境传输影响评估报告（CTIA），监管部门可检查并禁止违规传输。

整体来看，四地均以事前监管为核心，通过审批、备案、通知、评估等方式实现数据跨境可控，企业需按经济体、数据类型、主体类型和规模、行业属性逐一匹配义务，避免违规跨境导致的合规风险。

三、行动清单

- ☐ 梳理跨境数据传输涉及的国家，识别是否落入中 / 俄 / 印尼 / 越监管范围
- ☐ 按适用场景梳理传输数据类型（个人信息 / 重要数据）、主体类型和规模等，判定触发义务
- ☐ 中国场景：区分安全评估申报与标准合同备案，准备对应材料与时限安排
- ☐ 俄罗斯场景：确认数据接收国保护水平，完成事前通知或批准申请
- ☐ 印尼场景：区分公共 / 私营主体，完成通信信息部报告
- ☐ 越南场景：编制 CTIA 报告，在规定时限内提交公安部并及时更新
- ☐ 建立跨境传输审批 / 备案台账，留存官方回执与合规证明

Q28

若企业发生跨境数据泄露，是否需同时向多个国家/地区报告?

（撰写人：戴佳兵）

答：

一、核心提要

普遍存在多重报告义务：当数据泄露事件涉及多个司法管辖区的数据主体时，企业通常需要同时向多个国家的监管机构及受影响个人报告，而非仅向总部所在地报告。

触发条件各异：各国对“需要报告的数据泄露”定义不同，包括泄露类型（如个人数据、重要数据）、风险阈值（是否对个人权利造成高风险）以及报告时限。

冲突与协调：多重报告义务可能导致时限冲突或要求不一致（如报告语言、内容深度），企业需制定统一的事件响应机制以应对。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

国家/地区	核心法律	报告触发条件	报告对象	报告时限
欧盟	通用数据保护条例	可能对自然人权利与自由造成风险	监管机构（主监管机构及相关受影响成员国监管机构）	72小时，不得无故延误
美国	各州法（如CCPA、NYDFS等）	通常为“未经授权的访问/获取”	各州总检察长、受影响个人	美国各州法律差异巨大，多数要求‘无不合理延迟’（通常解释为30-90天）。加州新法要求30日内通知个人、15日内通知总检察长；纽约州NYDFS要求金融机构在确定事件后72小时内报告。
新加坡	个人数据保护法(PDPA)	导致或可能导致对受影响个人的重大伤害，或泄露规模较大	个人数据保护委员会(PDPC)及受影响个人	“尽快”，且必须在“可行情况下”
中国	个人信息保护法(PIPL)	发生或可能发生个人信息泄露、篡改、丢失	履行个人信息保护职责的部门及受影响个人	《个人信息保护法》规定应向“履行个人信息保护职责的部门”报告。实践中通常指向国家及地方网信部门。同时，根据2025年11月1日生效的《国家网络安全事件报告管理办法》，不同级别的网络安全事件有不同层级的报告对象和时限要求（如关键信息基础设施1小时内报告，一般网络运营者4小时内向属地省级网信部门报告），需结合具体案情判断。

企业不能依赖“单一窗口”报告。合规的关键在于事前识别数据资产的“国籍”，即数据主体的所在地。一旦发生泄露，企业必须启动一个并行而非顺序的报告流程，在最短的法定时限（如72小时）内，向所有相关监管机构履行报告义务。这要求企业建立全球统一的事件响应小组和多语言模板，以应对不同法域的要求。

示例：一家总部位于新加坡的跨境电商公司，其服务器设在美国，业务覆盖欧盟、中国和东南亚。某日发生黑客攻击，导致大量欧盟公民、中国公民及新加坡公民的个人数据泄露。

该公司需同时： 1）在72小时内向欧盟主要成员国监管机构报告；2）立即向中国履行个人信息保护职责的部门（如网信办）报告；3）尽快向新加坡PDPC报告；4）根据美国加州法律，向受影响用户发出通知。

若处理不当，该公司将面临来自欧盟（最高2000万欧元或全球营业额4%）、中国（最高5000万人民币或上一年度营业额5%）及新加坡（最高100万新元）的叠加性处罚。

三、行动清单

□ 考虑“通知豁免”情形：部分法域在特定条件下可豁免通知数据主体（如中国PIPL规定，若采取有效措施能有效避免损害，则可不通知个人）。响应计划中应加入对此类豁免情况的评估流程，避免不必要的通知引发风险。

□ 建立全球数据资产地图，清晰标识企业所处理个人数据的“来源国”及“存储地”。

□ 制定统一的数据泄露事件响应计划，明确不同法域的报告流程、时限及责任部门。

□ 组建跨法域的法律与IT事件响应团队，确保在72小时内能完成多国报告的初步准备。

□ 准备多语言版本的“数据主体通知”模板，确保在需要时能快速个性化并发布。

□ 定期进行数据泄露模拟演练，测试跨部门、跨地域协作及报告流程的有效性。

Q29

如何在美国、日本、新加坡之间实现个人信息的合规跨境传输?

（撰写人：陆雪儿）

答：

一、核心提要

依托白名单（充分保护国）认定与 CBPR 等多边机制，利用多边互认协议实现跨境合规集约化。

秉持问责制原则签署 SCCs与DPA实现境外接收方等位保护义务契约化。

对于涉及高风险或大规模个人信息传输，进行数据保护影响评估与传输风险评估以识别接收方所在国强制调取敏感数据之法治风险。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

国家维度	美国	日本	新加坡
核心法律	州法和行业专门法	个人信息保护法 (APPI)	个人数据保护法 (PDPA)
跨境传输基本逻辑	原则上不设限，但需遵守行业监管及联邦贸易委员会 (FTC) 的消费者保护要求；此外依第14117号行政令（EO 14117，2024年2月28日）对向中国等受关注国家的大规模敏感个人数据交易实施禁止或限制	原则限制，除非获得本人同意、接收方在白名单国家或通过 CBPR/合同认证	原则限制，要求境外接收方提供的保护水平须与 PDPA 实质相当
主要合规机制	数据隐私框架 (DPF)、CBPR、合同约束	白名单（充分保护国，目前为欧盟、英国）、APEC CBPR、个别同意、标准合同	PDPA 豁免情形、标准合同条款 (SCCs)、BCR、CBPR 认证
监管机构	FTC、州检察长	个人信息保护委员会 (PPC)	个人数据保护委员会 (PDPC)

在个人信息跨境传输的规制领域，美国、日本与新加坡既有差异亦存在共性。美国在坚守自由竞争这一基本特质的前提之下，正借助各州立法进一步强化对个人信息的保护力度。其立法模式呈现去中心化特征，以各州法律以及行业专门法律作为关键的立法支撑。在跨境数据传输方面，美国秉持原则上不设限的开放姿态，同时辅以联邦贸易委员会提出的消费者保护要求，以及数据隐私框架、APEC 跨境隐私规则（CBPR）等机制开展柔性监管。在监管执行层面，美国构建了联邦贸易委员会与州检察长共同参与的双层执法体系，形成了较为独特的监管闭环。日本与新加坡在个人信息跨境传输规制方面，均确立了统一的个人数据保护法律体系。日本以《个人信息保护法》（APPI）为基本法典，新加坡则以《个人数据保护法》（PDPA）为核心依据，二者在跨境传输问题上均遵循原则限制、例外豁免的审慎规制逻辑。日本在构建合规路径时，着重运用充分性认定、白名单制度以及个体同意等方式；新加坡则强调遵循实质相当的保护水平对等原则，要求境外的个人信息接收方必须提供与《个人数据保护法》同等水平的保护。在监管执行方面，日本与新加坡均设立了专门的信息或数据保护委员会（PPC/PDPC），由其独立行使法定的监管职权，从而形成独立且完整的监管闭环。

在具体合规工具的运用上，美国、日本与新加坡均广泛采用标准合同条款、拘束性企业规则以及 APEC CBPR 认证等工具。对于跨国实体而言，深入理解这三个不同法域在个人信息跨境传输规制方面的共性要求，即探寻合规要求的最大公约数，并构建以问责制为核心的全球数据治理体系，已成为规避法律风险、实现数据价值最大化的必由之路。

三、行动清单

- ☐ 申请 Global CBPR 认证,加入三国共同认可的机制以实现一站式互认。
- ☐ 通过法律协议约束境外接收方履行保护义务。
- ☐ 实施数据脱敏与加密技术,在传输前进行匿名化处理，降低合规敏感度。
- ☐ 建立全链路数据溯源日志，详细记录数据跨境流转路径,保障存证闭环。

Q30

数据跨境传输协议（DTA / SCC）在APEC经济体中是否有效?

（撰写人：王丹）

答：

一、核心提要

总体情况：多数 APEC 主流经济体认可 DTA/SCC作为数据跨境合规路径，但部分国家不认可或不可仅靠合同完成跨境。

国别差异：部分经济体如韩国、俄罗斯未将跨境传输协议作为合规措施，中国、越南、印尼则要求特定主体、附加通知、评估等前提条件/额外义务。

认可模板：跨境传输合同通过合同将本地法律下的“保护标准”延伸至境外接收方，是确保数据在境外受到与本国实质相当的充分保护的措施，部分经济体直接认可东盟 MCCs、欧盟 SCCs模板。

二、法规矩阵与专业洞察

经济体	SCC/DTA是否有效	具体内容
中国	是（有限制）	根据《个人信息保护法》和《个人信息出境标准合同办法》，符合特定要求的（非关键信息基础设施运营者；处理个人信息不满100万人的；自上年1月1日起累计向境外提供个人信息不满10万人的；自上年1月1日起累计向境外提供敏感个人信息不满1万人的），个人信息处理者可以通过签订国家网信部门制定的标准合同来进行跨境传输。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体	SCC/DTA是否有效	具体内容
韩国	否	《个人信息保护法》（PIPA）2023年修正案引入五类跨境转移事由，其中"数据充分性/等效性"事由可涵盖标准合同条款（SCCs），但目前仍缺乏具体实操落地细则。
美国	是（有限制）	联邦层面（允许企业自行签订具有法律约束力的合同作为合规措施，但受第14117号行政令限制）：根据第 14117 号行政命令《防止受关注国家访问美国人的大量敏感个人数据和美国政府相关数据》，2024 年《防止外国对手获取美国人数据法案》对于受关注国家、外国敌对国家访问特定类型的数据有严格的禁止/限制。
日本	是	《个人信息保护法》（APPI）要求进行跨境传输原则上应获得数据主体的同意，但也可通过采取跨境传输协议（DTA）或标准合同条款（SCCs）的方式，使接收方能够采取与日本个人信息处理经营者应采取的措施相对应的持续措施。
新加坡	是	根据《个人资料保护条例 2021》，签订符合第11条第（2）款规定的跨境传输协议即视为已采取适当措施确保接收方承担受法律约束的保护义务。
加拿大	是（部分省有更严格要求）	联邦层面《个人信息保护和电子文件法》是明确将合同作为确保第三方提供同等水平保护的合规方式的。 魁北克省：要求先做 PIA，评估通过方可签协议。
澳大利亚	是	《1988年隐私法》隐私原则 8.1（APP 8.1）要求在向海外接收方披露个人信息之前，澳大利亚实体必须采取“合理步骤”（Reasonable Steps），以确保该海外接收方不会违反澳大利亚的隐私原则（APPs）。《隐私原则指南》中明确指出：建立具有法律约束力的合同是确保海外接收方遵守隐私原则最常见且最有效的“合理步骤”。
俄罗斯	否	根据第266-FZ号联邦法，规定了俄罗斯公民个人数据本地首次存放原则；跨境事前通知+监管批准。
越南	否	根据第356/2025/ND-CP号法令，须在进行跨境传输后60日内提交 CTIA 跨境影响评估档案，包括跨境传输合同。
印度	是	根据《2023年数字个人数据保护法》（DPDPA 2023），政府可设传输负面清单，目前暂未发布。尚未有关于跨境传输的其它限制要求。
印尼	是（有附加要求）	印尼《个人数据保护法》（PDP Law□规定跨境传输数据的条件之一是采取具有法律约束力且可执行的保障措施（如标准数据保护合同），以确保个人数据获得同等水平的保护。此外，还需要与通信和信息技术部进行协调（提交报告等）。

三、行动清单

- □ 先确认目标传输国是否属于认可 DTA/SCC 的 APEC 经济体。
- □ 若为中国境内主体，自查是否符合标准合同适用的四项条件。
- □ 针对美国个人数据跨境传输，核查是否触及敏感数据与受关注国家等限制。
- □ 涉及印尼等国时，按法规要求完成通知/评估/ 备案等附加义务。
- □ 涉及韩国、俄罗斯、越南等国时，应按其法律规定采取跨境合规措施。
- □ 优先选用当地监管认可的模板（东盟 MCCs、欧盟 SCCs、中国网信办标准合同等）。
- □ 合同中明确约定境外接收方提供等效数据保护及责任承担、违约救济条款。
- □ 留存合同签署记录、传输台账、评估报告等合规证明文件。
- □ 定期复核目标国数据跨境法规更新，确保协议持续有效。

Q31

企业能否依靠合同作为跨境传输的主要合法性依据? **（撰写人：孙霖）**

答：

一、核心提要

合同是实现 APEC “问责制”的核心工具： 在 APEC 隐私保护框架下，合同是落实“问责制”（Accountability）的主要手段，绝大多数 APEC 成员经济体（如新加坡、美国、日本）均认可通过合同义务约束境外接收方。

合同效力受限于“输出地”的法定要求： 虽然合同广受认可，但企业必须区分“自由拟定合同”与“法定标准合同”。例如，中国（PIPL）要求必须采用官方模板并备案，而新加坡则允许企业基于保护水平相当的原则自主拟定。

合同需配合程序性义务方能完整合规： 仅签署合同通常不足以构成完整的合法性依据，往往需要配合个人信息保护影响评估（DPIA）或对接收方的尽职调查，以证明合同条款在境外具有可执行性。

二、法规矩阵与专业洞察

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

1.APEC 主要成员经济体跨境传输合同要求对比表

维度	中国 (PIPL)	新加坡 (PDPA)	美国/APEC CBPR 体系
合同 法律地位	法定必备路径之一 （标准合同）。	核心路径 （满足传输限制义务）。	商业实践中的 主要合规抓手。
是否 强制模板	是，必须采用国家网信办发布的标准合同文本。	否，但合同需涵盖保护水平、目的限制等核心要求。	否，强调企业自律与合同法的约束力。
政府 监管介入	高：合同签署后需向省级网信部门备案。	中：不强制备案， 但违规时需作为合规证据提交。	低：主要通过 FTC 对违约/欺诈行为 进行事后追责。
核心 合规逻辑	形式合规 + 行政备案。	结果导向：确保数据获得同等保护。	问责制导向：通过合同锁定法律责任。

1.核心洞察与结论

在 APEC 区域内，企业完全可以依靠合同作为主要合法性依据，但合同的性质正在发生从“商业契约”向“合规工具”的转变：对于强监管地区（如中国）：合同是准入证。重点不在于合同内容的谈判，而在于业务逻辑是否能严丝合缝地套入官方模板，并完成备案。对于灵活监管地区（如新加坡、澳洲）：合同是防火墙。重点在于合同中关于“损害赔偿”和“审计权”的约定，以确保在发生泄露时，境内主体能够通过问责机制免责。合同是 APEC 跨境传输的基石，但其有效性取决于企业是否根据“数据输出地”的要求选择了正确的合同范式（范本型 vs. 自拟型）。

2.实务案例

某跨国电商平台 B 的 APEC 区域数据整合：该平台计划将中国境内及新加坡分公司的会员数据汇总至美国总部服务器。

操作路径：

1.中国端： B 公司必须与美国总部签署《个人信息出境标准合同》，标准合同正文不得修改或删减，但可补充不冲突的附加条款，并向中国网信部门提交了备案文件。

2.新加坡端： B 公司与总部签署了一份内部服务协议（Inter-company Agreement），确保总部遵守新加坡 PDPA 的保护标准，无需政府审批。

风险洞察： 若 B 公司仅使用总部的通用全球隐私协议，将因未包含中国法定的“第三方受益人”条款而导致中国境内的传输行为构成违规。

三、行动清单

☐ 判定数据输出地的模板要求： 确认流出地（如中国）是否存在必须适用的法定标准合同文本，避免合同因形式不符而失效。

☐ 识别数据处理角色： 明确跨境传输是属于“委托处理”还是“数据共享”，从而在合同中准确界定双方的权利边界。

☐ 嵌入 APEC 核心隐私原则： 检查合同是否涵盖了目的限制、安全保障、个人访问权及纠正权等 APEC 框架必备要素。

☐ 执行接收方履约能力评估： 在签署合同前，通过尽职调查确认境外接收方是否有能力落实合同约定的技术安全标准。

☐ 明确第三方受益人权利： 特别针对强监管区域，确认合同中是否赋予了个人（数据主体）在权益受损时直接向接收方索赔的权利。

☐ 履行法定的备案或告知手续： 核实合同签署后是否需要在法定期限内向当地监管机构备案，或是否需要向个人告知合同的主要条款。

☐ 建立合同履行动态审计： 设定定期检查机制，确认境外接收方在实际操作中是否持续遵守合同义务，而非仅停留在纸面承诺。

Q32

APEC经济体对云服务商的数据存储合规要求是否一致？ （撰写人：孙霖）

答：

一、核心提要

不一致性显著： APEC 各经济体对云服务商（CSP）的数据存储要求极度不一致。虽然有 APEC 跨境隐私规则（CBPR）作为框架，但各国在“数据本地化”与“自由流动”之间存在显著的政策鸿沟。

监管维度差异： 合规要求通常取决于数据敏感度（如金融、政务数据）和经济体自身安全观。例如，中国、越南等强调关键行业数据本地化存储，而新加坡、美国则更倾向于保障数据跨境自由流动。

双轨并行策略： 云服务商在APEC区域运营必须采取“一国一策”的合规布局，无法依靠单一的全球化标准覆盖所有区域的法律要求。

二、法规矩阵与专业洞察

1.APEC 主要经济体数据存储合规要求对比表

经济体	核心法律/规制	对云服务商（CSP）的存储要求	监管态度
中国	《数据安全法》 《个人信息保护法》	关键信息基础设施（CIIO）及处理达到规定数量的个信须本地化存储；“重要数据”出境须经安全评估。	严格监管，强调数据主权与本地化。
新加坡	《个人数据保护法》(PDPA)	无强制本地化存储要求。只要接收方能提供同等保护水平或符合 CBPR 认证，即可自由跨境。	开放透明，支持全球互通。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体	核心法律/规制	对云服务商（CSP）的存储要求	监管态度
越南	《网络安全法》第 53 号法令	提供云服务等电信增值服务的企业，若收集用户隐私或生成数据，须在越南设立办事处并本地化存储。	极度严格，强制本地化趋势明显。
美国	《澄清境外数据合法使用法案》(CLOUD Act)	侧重于数据控制权而非存储位置。要求 CSP 即使数据在海外，在特定执法需求下也需配合调取。	侧重跨境调证，不设通用本地化门槛。
印度尼西亚	第 71 号政府条例（GR 71）	公共服务运营商须在本地存储和处理数据；私人领域运营商可有条件选择海外存储，但需向监管报备。	行业差异化监管，公共部门要求高。

1.核心洞察与结论

从上述对比可以看出，APEC 内部存在“碎片化”合规风险。

本地化壁垒：以越南和中国为代表的经济体，将数据存储位置与国家安全挂钩，导致云服务商必须在当地投资数据中心（IDC）。

认证协同：尽管 APEC 推行 CBPR 认证以促进互认，但目前 CBPR 更多解决“跨境转移”的合规性，无法完全豁免成员国国内法对于“存储地”的强制性规定。

结论：云服务商在 APEC 区域无法实现“一套架构走天下”，必须针对不同市场进行数据地理围栏（Geo-fencing）设计。

2.实务案例

案例：某跨国 SaaS 服务商在 APEC 区域的部署决策

该服务商原计划在新加坡设立统一的亚太数据中心。但在进入越南市场时发现，根据越南《网络安全法》，由于其涉及收集当地用户数据，必须在越南境内存储备份。最终，该服务商采取了“新加坡中心节点 + 越南本地存储节点”的混合云模式，导致运营成本增加了约 30%，并需额外雇佣当地合规审计团队。

第三部分：行动清单

☐ 数据映射（Data Mapping）：梳理在该经济体境内收集的数据是否属于“重要数据”、“政务数据”或“敏感行业个人信息”。

☐ 识别监管主体：确认自身是属于“公共服务运营商”还是普通“私人企业”，不同身份在印尼、中国等地对应完全不同的存储要求。

☐ 资质审查：若在需本地化存储的经济体运营，确认是否需持有当地 IDC/ISP 许可证，或需与当地有资质的厂商合作（如代运营模式）。

☐ CBPR 认证申请：尽早获得 APEC CBPR 认证，作为在新加坡、日本等认可该框架经济体进行数据流通的“通行证”。

☐ 执法响应预案：针对美国《云法案》等跨境调证法律，建立全球一致的执法数据索取响应流程，平衡存储地法律与调证需求。

☐ 合同条款更新：在与下游客户的 SLA 中，明确告知数据存储的地理位置及备份机制，满足特定国家的告知义务。

☐ 动态合规监控：持续关注 APEC 区域内法律变动（如越南新法令、中国数据出境新规），确保存储策略实时更新。

Q33

企业通常基于哪些因素判断拟跨境的数据是否落入重点监管范围?

（撰写人：戴佳兵）

答：

一、核心提要

数据性质：核心判断依据是数据是否属于“重要数据”、“敏感个人信息”或受特定行业监管的数据（如金融、医疗、健康基因信息）。

主体身份：数据处理者是否涉及国家机关、关键信息基础设施运营者(CIIO）等。

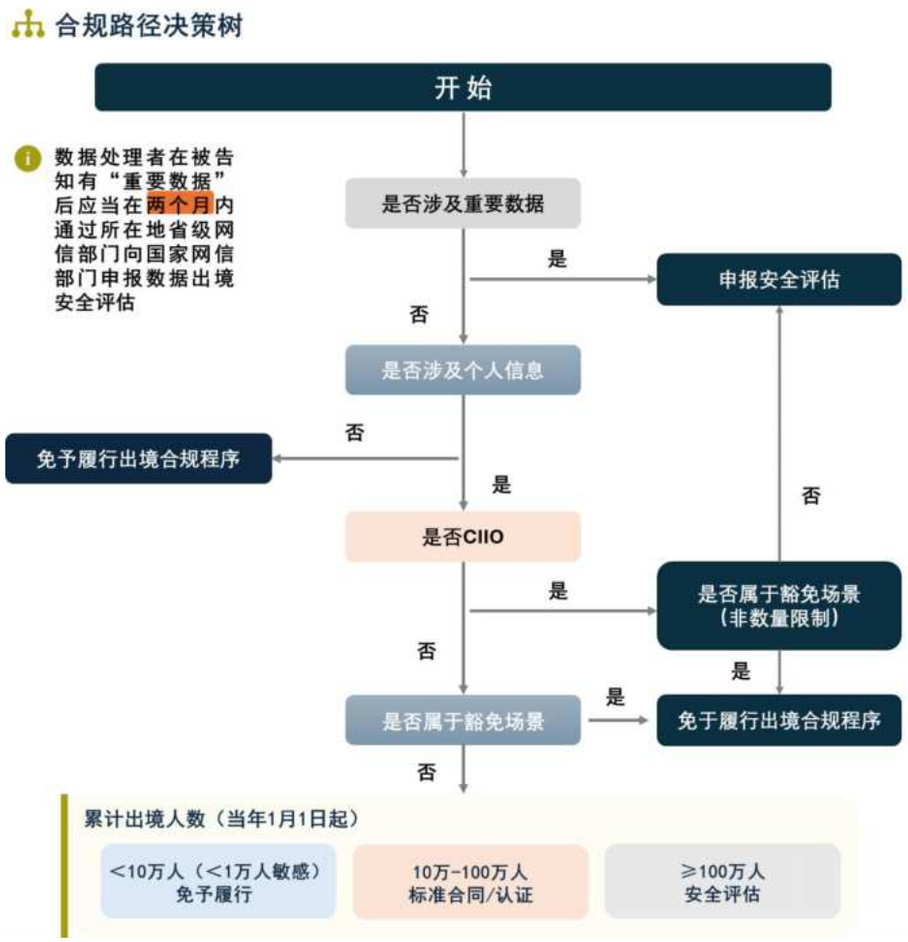
目的地风险：数据出境的目的地国家或地区的法律环境、是否与本国签署相关协定、是否为特定名单内国家，是判断是否需要履行额外申报或认证程序的关键。

二、法规矩阵与专业洞察

判断维度	欧盟（GDPR）	中国（PIPL/DSL）	新加坡（PDPA）	美国（行业法）
数据类型	敏感数据（种族、生物识别、健康、性取向等）	重要数据（国家安全相关）、敏感个人信息	个人数据（无明确敏感数据分层，但有更严格保护）	特定行业数据（如HIPAA下的健康数据）
主体/处理者身份	公共机构、大规模监控行为	关键信息基础设施运营者、重要数据处理者	组织规模、处理性质	金融机构、医疗机构、电信运营商等
出境目的地	“充分性认定”国家清单；无认定则需SCCs/BCRs	列入“限制或禁止出境清单”的国家/地区	主要看接收方是否有同等保护水平	受关注国家及相关人员的专项限制
核心监管逻辑	基于风险与权利保护	基于国家安全与公共利益优先	基于问责制与个人同意	基于行业监管与国家安全

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

中国数据出境监管合规路径决策树：



第三部分：行动清单

□识别重要数据：对照相关部门公开发布的重要数据目录，判断拟出境数据是否落入重要数据范围。

□确认主体身份：判断企业是否属于关键信息基础设施运营者(CIIO)，这将直接影响合规路径选择。

□统计出境数量：建立自当年1月1日起的累计出境个人信息数量台账，按自然人去重统计。

□区分敏感信息：将出境个人信息区分为敏感与非敏感，分别统计数量以确定适用的门槛。

□评估豁免适用：检查是否属于跨境合同必需、人力资源管理必需、紧急情况等豁免情形。

□选择合规路径：根据上述判断结果，在安全评估、标准合同/认证、免予办理三类路径中选择适用方式。

□关注自贸区负面清单：若企业在自贸区注册，可关注所在自贸区发布的数据出境负面清单，清单外数据可免予合规手续。

Q34

APEC各经济体主要对哪些行业数据进行重点监管？ （撰写人：王丹）

答：

一、核心提要

涉及行业：APEC 各经济体重点监管高度趋同，集中在金融服务与支付、医疗健康、电信与互联网、公共服务与关键基础设施四大高敏感领域。

监管方式：本地存储、出境评估、事件限时上报、第三方外包强管控、强制审计，涉及此类业务须按属地化落实合规要求。

二、法规矩阵与专业洞察

监管行业	主要经济体	核心法规	核心监管要求
金融服务与支付	中国	《银行保险机构数据安全管理办法》《中国人民银行业务领域数据安全管理办法》（2025 年施行）	数据分级分类、全流程安全管控、数据出境安全评估、金融数据本地化、事件上报与审计
	美国	GLBA 法案	隐私 / 安全 / 反欺诈规则、身份验证与访问管控、第三方外包风险管理、业务连续性要求
	韩国	《信用信息保护法》《电子金融交易法》	财务数据收集 / 共享 / 销毁规范、电子交易技术标准、征信与支付数据强监管
	印尼	OJK 第 11/2022 号条例	数据本地化存储、治理与风控、数据安全与隐私、外包监管与强制审计
医疗健康	中国	《医疗卫生机构网络安全管理办法》《人口健康信息管理办法》	医疗数据分级分类、全生命周期保护、数据出境管控、安全审计
	美国	HIPAA 法案	医疗数据处理规则、安全标准、违规通知义务、患者隐私保护
	澳大利亚	《我的健康记录法》（My Health Records Act 2012，2015年由PCEHR法更名）	权限访问控制、强制数据泄露通知、科研数据使用限制、健康数据专属保护
	新加坡	《卫生信息法》、《医疗保健服务法》	健康数据特殊保护、泄露通知、访问控制

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

监管行业	主要经济体	核心法规	核心监管要求
电信与互联网	中国	《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》	CII 认定、分级分类、本地存储、出境安全评估、合规备案
	美国	《联邦通信法》等	CPNI 数据严格保护、使用披露限制、安全防护、合规认证与备案
	越南	《网络安全法》、第 53/2022/ND-CP 号法令	数据本地存储、境内设点要求、跨境传输管控、电信与互联网行业数据监管
公共服务与关键基础设施（CII）	中国	《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》	CII 严格监管、分级分类、本地化、出境评估、供应链安全
	新加坡	2024 年《网络安全法》	CII 运营者强制事故报告、第三方风控、加密与 MFA、定期安全审计
	日本	《网络安全基本法》《经济安全保障推进法》	重要 IT 系统报备、供应链审查、事故报告与情报共享、核心数据境内存储建议

APEC 四大重点行业数据监管主要围绕本地存储、数据分级分类、事件限时上报、跨境安全、运营安全、第三方风控等维度立法，企业须着重注意是否落入特定重点监管行业及落实相关合规要求。

三、行动清单

□ 梳理本机构在 APEC 的业务场景，识别是否落入金融、医疗、电信、公共 CII四大高监管行业。

□ 梳理所开展业务国家对该特定行业的监管要求并制作合规清单。

□ 完成数据分类分级，标记个人敏感数据、重要数据等，形成清单。

□ 核查各属地特定行业的数据本地化要求，确定必须境内存储的数据范围与存储方案。

□ 建立数据跨境审批与评估机制，覆盖合同条款、安全保障、出境备案 / 申报。

□ 制定数据安全事件应急预案，明确上报时限、流程与责任人，匹配属地要求。

□ 对第三方服务商/外包商开展尽职调查与合规审计，签订数据安全与隐私条款。

□ 按行业专属规则完成合规要求梳理和落地，留存完整合规证据链。

Q35

当发生跨境数据纠纷时，APEC各经济体对“云端取证”效力的承认现状如何？企业如何避免数据储存地法律与司法调查要求的冲突？（撰写人：王鹤臻）

答：

APEC各经济体在云端取证效力问题上，形成了两种截然不同的立场，这是企业面临“双重违法”困境的根源。美国等国家采取“数据控制者主义”立场，核心逻辑是：只要网络服务提供者与其存在“最低限度联系”（如在美国上市、设有分支机构），无论数据实际存储于何处，可强制要求该企业提供其控制下的任何数据。即美国执法机关可以直接向某中资云服务商的美国子公司发出调证令，要求提供存储于中国境内的数据。美国《云法案》（CLOUD Act）是这一立场的典型代表。中国采取“数据存储地管辖”原则，核心要求是：境外数据必须通过国际司法协助渠道获取，任何境外执法机关不得直接向中国境内的数据控制者调取数据，中国《数据安全法》第36条、《国际刑事司法协助法》第4条等明确规定：非经中国主管机关批准，境内的组织、个人不得向外国司法或者执法机构提供存储于中国境内的数据，违反者可能面临严厉的行政处罚甚至刑事责任。

在云端取证场景下，传统“镜像硬盘”式的取证方式已无法适用。企业应通过API（应用程序编程接口）技术实现“符合法证标准的”数据收集。APEC框架下的Global CBPR（跨境隐私规则）认证是目前唯一由美国、日本、韩国、新加坡等15个以上经济体政府联合背书的跨境数据传输机制。由于中国目前尚未加入CBPR体系，因此申请主体需选择海外实体（如新加坡子公司）进行认证。阿里巴巴、小米、字节跳动等出海企业已通过此路径完成布局。

Q36

有关数据跨境传输，APEC各经济体对“用户明确同意”有哪些具体适用和例外规则？（撰写人：王鹤臻）

答：

APEC框架采取的是原则导向模式，其具体要求与GDPR等“规则导向”体系有所不同——它更强调通过清晰的告知保障用户的选择权，而非强制规定统一的同意形式。根据APEC隐私框架的选择权原则，在以下场景中，企业需要确保用户的同意。个人信息收集时，需要确保用户对收集行为有知情权和选择权。个人信息使用/披露时，当企业对个人信息的使用超出最初收集目的，或向第三方披露时，需要获得同意。个人信息跨境传输时，当向境外传输个人信息时，需要获得用户同意。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

在APEC跨境隐私规则体系中，“用户明确同意”并非在所有情况下都是数据跨境传输的强制性前提。其核心逻辑是“以问责制替代严格的事前同意”，即在特定条件下，允许企业通过“尽责调查”和“合理措施”来替代获取用户同意。主要适用于以下情形：

企业未采取“尽责调查+合理措施”来替代同意；数据接收方未取得CBPR认证，或企业无法通过合同等手段确保其保护水平；传输涉及的数据或场景不适合采用“问责制”路径。

需要特别留意的是，APEC框架仅设定最低标准。如果某个APEC成员经济体（如日本、加拿大等）的国内法对“同意”有更严格的规定（例如必须采用“opt-in”模式、禁止“隐含同意”等），企业仍须遵守更严格的国内法。

Q37

监管机构在哪些情况下会要求企业提供源代码或数据样本？相关要求的适用范围和合规边界是什么？ （撰写人：陆雪儿）

答：

一、核心提要

监管机构调取源代码或数据样本通常应用于反垄断审查、网络安全审查、及司法调查等场景。

企业应依最小侵害原则主张受控审计，阻断核心资产的移转。

针对AI与算法监管，监管要求正从结果导向转向逻辑导向。企业需预先准备算法说明文档及脱敏样本集，确保模型的可解释性满足法定的透明度要求。

二、法规矩阵与专业洞察

维度 国家	中国	美国	欧盟
法律依据	《数据安全法》、《算法推荐管理规定》	《行政传票权》、各行业监管准则	《人工智能法案》、《通用数据保护条例》
数据调取场景	重要数据出境评估、算法备案检查、国家安全审查	反垄断调查、司法部刑事取证	Ai系统合规性验证、数字市场法合规检查
权利的边界	采取必要措施保护商业秘密，调取范围应与审查目标一致	商业秘密保护抗辩、第四修正案权利限制	比例原则，仅限验证合规性所需的最低限度信息
数据样本侧重	脱敏后的测试数据集	用户数据抽样以验证偏见	训练数据来源的合法性与质量

在APEC框架下，监管机构仅在数据安全风险、国家安全审查及跨境合规验证等特定情形下，方可要求企业提供源代码或数据样本；同时该权力受到禁止强制技术转移、数据最小化及跨境执法合作机制等原则的严格约束，以达到监管有效性与企业技术主权之间的平衡。

三、行动清单

- ☐ 在交付敏感信息前，向监管机构提交商业秘密声明，要求书面确认其保密责任。
- ☐ 准备非技术语言的算法文档，对源代码和数据样本作技术防护。
- ☐ 若监管机构调取超必要性，援引相关行政法规并向行业主管部门申诉。

Q38

若数据需存储在当地，企业应如何设计混合云架构以规避合规风险？（撰写人：王鹤臻）

答：

合规的混合云架构应围绕以下三个原则构建：

1. 数据不离境。通过基于区域的路由机制，确保每一条数据请求都留在其合法的管辖区域内，除非经过明确授权。

2. 在网络层面，需要进行物理和逻辑的网络隔离，将敏感工作负载限制在特定的“合规区”内。密钥不留云：采用BYOK/HYOK（企业自持密钥，Bring/Hold Your Own Key）模型，即加密密钥由企业自己生成和管理，云服务商无法访问。这样即使云平台遭遇政府指令或黑客攻击，也难以解密你的数据。

3. 审计不间断：建立不可变审计日志，记录数据的一举一动（谁、何时、访问了什么），并确保日志存储在数据所在的司法管辖区内。所有日志需统一回传至中央审计中心，形成完整的合规证据链。架构设计应进行数据分类。核心财务数据、用户隐私信息（如身份证号、手机号）、高价值知识产权（如源代码、设计图纸）必须保留在本地。营销活动数据、IoT传感器数据、用于非敏感分析的脱敏数据、以及需要高并发访问的Web应用数据可上云。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q39

企业如何避免“隐性跨境数据流动”的监管风险?

（撰写人：孙霖）

答：

所谓的“隐性跨境”通常是指：数据虽然物理上存储在境内，但由于境外机构或人员拥有访问权限（如自动同步、远程运维和访问、云端共享、SDK回转、集团内部系统访问等），在法律定义上均被视为“数据出境”。

一、核心提要

确立“远程访问即出境”的合规基准： 企业必须打破“数据物理不出境就不算境外出境”的误区，将境外远程登录、API接口海外调用等行为全数纳入出境合规管控口径。

实施“最小化权限”与“脱敏处理”双重防线： 针对不可避免的境外访问需求，通过严格的RBAC（基于角色的访问控制）和动态脱敏技术，操作全程审计留痕，从技术层面将数据泄露风险降至最低。

构建以CBPR为核心的互认机制： 积极参考APEC跨境隐私规则（CBPR）体系，通过合同约束（MCCs）和合规审计，建立起符合多个成员体要求的跨境数据治理架构。

二、法规矩阵与专业洞察

1.APEC 核心成员体对“隐性跨境”的监管要求对比

维度	中国 (虽非CBPR成员但监管极严)	新加坡 (APEC CBPR核心推动者)	美国 (CBPR 框架主要发起国)
出境定义	明确规定“境外机构、组织、个人访问境内存储的数据”即构成出境。	侧重于“保护义务转移”无论形式如何，接收方需具备同等保护水平。	美国没有统一的数据出境法律定义，更关注数据处理、共享及披露行为的合规性。
核心合规路径	申报安全评估、订立标准合同 (SCC) 或通过个人信息保护认证。	可通过符合PDPA要求的跨境转移机制（包括可比保护义务、合同安排等）；参与CBPR体系可作为提升跨境合规水平的参考。	主要依赖于企业自律性合规框架及合同约定。
对隐性访问态度	严控。远程运维、集团内部VPN访问需视同出境进行备案或评估。	灵活。鼓励通过 CBPR 体系实现域外执法与合规的统一。	相对灵活。但企业仍需依法履行数据安全和隐私保护义务，发生数据泄露或违规处理时可能承担行政、民事等法律责任。

1.专业洞察与结论

目前，APEC 地区的监管趋势正从“物理流向监控”转向“处理行为监控”。企业最容易踩坑的地方在于：认为将服务器设在境内就万事大吉。结论： 企业应建立“数据出境台账”，不仅记录发出去的数据，更要记录“被谁看过”。对于隐性流动，合规的本质不再是阻止流动，而是确保流动的“透明度”与“可追溯性”，并采取限期删除等措施。

2.案例分析：某跨国科技公司 CRM 系统运维案

背景： 该公司中国区客户数据存储在上海本地服务器，但其全球技术支持中心位于东南亚某国。该中心工程师经常通过 VPN 远程登录上海服务器进行故障排除。

问题： 公司未将此行为识别为“数据出境”，导致在合规检查中被认定为未履行数据出境安全评估义务。

3.规避策略

(1)技术改造： 在运维入口增加“堡垒机”，强化权限管理，所有操作留痕、审计追溯，做到应急响应，拦截未授权的跨境传输。

(2)数据脱敏： 运维人员仅能看到脱敏后的测试数据，敏感字段（如手机号、身份证号）默认遮蔽。

(3)合同约束： 与海外中心签署包含 APEC CBPR 准则的内部数据处理协议。

三、行动清单

☐ 识别风险点： 盘点企业内部是否存在境外 IP 远程登录、境外云端同步、或跨国联合办公软件的敏感数据共享。

☐ 完善法律文件： 在与境外主体（含关联公司）签署合同时，加入专门的跨境处理条款，明确数据安全责任边界。

☐ 落实境内存储： 确保核心及重要数据境内存储，如确需远程访问，需经过内部合规审批流程。

☐ 执行敏感度审计： 对所有涉及境外访问的接口进行分级分类，严禁境外直接访问原始底表。

☐ 开展影响评估 (DPIA)： 针对“隐性流动”场景定期开展个人信息保护影响评估，并形成书面报告留存备查。

☐ 强化人员培训： 针对研发、运维及国际业务部门，普及“远程查看亦是出境”的法律概念。

☐ 部署监控告警： 建立异常流量和境外非法 IP 访问的实时告警机制，实现隐性流动的可视化管理。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q40

在多国数据流动场景下，数字平台的合规责任包含哪些触发条件与类型？

（撰写人：陆雪儿）

答：

一、核心提要

平台的合规责任不仅源于注册地，更源于数据来源地、主体国籍及处理规模。只要服务触达特定法域，即可能触发该国法律的域外适用条款。

合规义务因数据性质和主体身份的不同而有所差异，处理大规模敏感数据的平台面临强制性本地化存储与国家安全审查。

在多国流转中，平台的合规责任不仅限于自身，还包括对下游云供应商及数据接收方的尽职调查。建立以标准合同条款+和信任认证为核心的链路是降低穿透风险的关键。

二、法规矩阵与专业洞察

维度国家	中国 (PIPL/DSL)	欧盟 (GDPR)	东南亚 (以新加坡 PDPA/CBPR为例)
管辖触发条件	境内处理；或向境内个人提供产品/服务；或分析境内个人行为。	境内设有机构；或向境内主体提供商品/服务；或监控其行为。	境内收集、使用或披露；或具有显著联系的境外活动。
本地化触发阈值	强制性： 关键信息基础设施营运者 (CIIO)；关键信息基础设施运营者（CIIO）以及达到法定规模的数据处理者，应依法履行数据本地存储及跨境传输安全评估等义务。	原则上不强制，但对向不充分保护的第三国传输设置严格门槛。	原则上不强制，核心在于确保接收方提供等位保护。
核心合规工具	网信办安全评估、标准合同、保护认证。	充分性认定、标准合同条款 (SCCs)、企业约束规则 (BCR)。	APEC CBPR 认证、标准合同、受认可的豁免情形。
主要合规义务	单独同意、出境风险评估、接收方履约监督、定期安全审计。	数据保护影响评估 (DPIA)、数据处理协议 (DPA)、传输风险评估 (TIA)。	问责制要求、保障数据传输安全的合理努力义务。

该表格反映出中国、欧盟与东南亚在个人信息跨境传输领域形成了三种具有代表性的制度范式，即以国家安全为导向的强控制模式、以数据主体权利为核心的规范化模式以及以责任制为基础的灵活治理模式。三种模式在管辖规则、本地化要求及合规工具方面存在显著差异，但在强化企业责任、提升数据保护水平及推动跨境数据有序流动方面呈现出趋同趋势，体现出全球数据治理体系在多元路径下的逐步协调发展。

三、行动清单

□ 确认是否涉及跨境数据传输、对数据分类分级（识别个人/敏感/重要数据）

□ 评估是否需要加入CBPR认证体系，出境前自评估、必要时申报官方评估

□ 建立跨境数据传输合规机制，设立数据保护负责人（DPO）及跨境专项小组，跨境泄露72小时内通知监管与用户

□ 制定透明的隐私政策与用户通知，跨境前由用户勾选，清晰告知数据去向与用途

□ 建立第三方数据处理管理制度，第三方APP/SDK上架前开展跨境风险审查

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容



Q41

APEC经济体在人工智能治理方面有哪些共同原则、政策倡议或合作机制？这些共识在不同经济体的落地路径上存在哪些差异？

（撰写人：傅颉）

答：

一、核心提要

APEC层面已形成以"负责任AI"为核心的价值共识，并通过《APEC互联网和数字经济路线图》（AIDER）、《2025年亚太经合组织领导人庆州宣言》及《亚太经合组织人工智能倡议（2026-2030）》构建起持续演进的合作框架，但所有成果均属自愿性质、不具法律约束力。

各经济体落地路径呈现显著的"三轨分化"格局：以韩国、中国为代表的“专项立法先行轨”、以新加坡、日本为代表的"软法+现有法律协同轨"、以马来西亚、越南等东南亚经济体为代表的"战略路线图+能力建设轨"，三轨并行，相互之间缺乏强制对接机制。

跨境监管碎片化是APEC区域AI治理的最大挑战：无论是数据流动规则、算法透明度要求还是高风险AI的定义，均因经济体不同而存在实质差异，给跨境AI服务提供商带来多重合规负担，亦是律师在涉APEC业务中需要重点关注的法律风险点。

二、法规矩阵与专业洞察

1.主要经济体 AI 治理路径对比

经济体	核心监管依据	法律地位/生效时间	特色监管机制
韩国	《人工智能基本法》	2026年1月22日生效	“高影响力AI”强制披露、透明度指南
中国	《生成式AI服务管理暂行办法》等	已施行	算法备案制度、境内服务安全评估
新加坡	模型AI治理框架 2.0（GenAI）	2024-2025年持续更新	“AI Verify”自愿性认证、MAS FEAT原则
越南	《数字技术产业法》	2026年起施行	侧重数字基础设施与AI产业促进

APEC成员正致力于通过“APEC AI 倡议”建立具有弹性的AI生态系统，特别强调跨国界的研发协作与自愿性的信息共享 。然而，监管的分野在2026年初愈发明显：韩国已正式施行全球领先的《人工智能基本法》，要求对影响公民权利的AI系统实施严格的透明度管理；而大多数经济体仍倾向于通过“结构性改革”来移除AI采纳的障碍，而非设立硬性门槛。

2.实务案例

2025年APEC AI风险共识： 在2025年庆州峰会期间，各方虽在具体立法上保持独立，但APEC各经济体共同认可了关于“增强AI安全性与可靠性”的条款，特别是在应对AI误导性信息和提升算法可解释性方面达成了底层逻辑的一致。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

三、行动清单

□ 评估客户AI产品在韩国《人工智能基本法》下是否属于“高影响力AI”。

□ 跟踪APEC 2026年度关于“AI驱动的结构性改革”报告，预判新兴市场的政策转向。

□ 在跨境合同中加入“动态合规条款”，以应对2026年越南、韩国等新法生效后的合规衔接。

□ 利用新加坡“AI Verify”框架进行合规预演，作为进入东南亚市场的“信用护照”。

□ 建立针对不同经济体“高风险AI”定义差异的内部对照表。

Q42

美国在AI监管中，对行业自律的依赖程度及核心监管趋势如何？

（撰写人：冷勇达）

答：

一、核心提要

截至2026年，美国AI监管呈现效率与创新优先、以巩固全球 AI 技术领导地位为核心目标等特征。2025年政策调整后，联邦层面大幅减少强制性监管要求，更多依赖行业自律机制。

二、法规矩阵与专业洞察

1.监管趋势

2025年初政府换届后，美国AI战略逆转，确立AI创新与全球技术领导力为首要政策目标，以对标、对冲欧盟的强监管路径。

(1)全面废除前政府监管框架：2025年1月20日，特朗普总统签署行政命令《初步撤销有害行政令及行动》，废除拜登政府第14110号行政令。原令曾动用《国防生产法》强制前沿AI企业向政府报告红队测试结果，废除意味着联邦放弃对大型模型的部分强制审查权。

(2)确立去监管新框架：2025年1月23日，白宫发布第14179号行政令《消除美国人工智能领导地位的障碍》。指示OSTP与OMB排查阻碍AI发展的规定，核心逻辑是AI早期发展不能被官僚主义扼杀，须为私营部门松绑以确保全球领先。但须注意，联邦贸易委员会（FTC）执法、联邦采购规则、出口管制以及州级与部门监管仍然存在，联邦并未完全退出AI监管。

2.行业自律的依赖程度

基于上述“去监管”的大背景，美国目前对AI行业的自律依赖程度达到了前所未有的高度。具体体现在：

(1)安全评估下放企业内部：联邦强制报告取消后，头部AI企业（如OpenAI、Meta）由内部安全与对齐团队自行裁量模型发布，无需向政府提供证明安全性的相关报告。

(2)行业联盟防范极端风险：“前沿模型论坛”等自发联盟制定非约束性自愿准则，应对生物武器开发等极端风险。

(3)NIST标准纯属自愿参考：NIST的《AI风险管理框架》及配套指南仍存在，但严格定性为自愿性最佳实践，联邦不再将其作为企业开展业务的隐性门槛。

Q43

哪些APEC经济体在数字行业准入、税收优惠及政策扶持方面具有相对优势？

（撰写人：王熙雨）

答：

一、核心提要

APEC 区域整体呈现“准入友好度差异化、税收激励集中化、政策扶持体系化”的格局。

新加坡、中国香港特别行政区等在数字行业准入、监管透明度与跨境数据政策方面具有显著优势。

新加坡、马来西亚、越南等在数字产业税收优惠方面加大了投资激励。

中国等在数字基础设施、创新生态与政府扶持政策方面形成结构性优势。

二、法规矩阵与专业洞察

1.数字行业准入优势经济体（Market Access Leaders）

（1）新加坡

①高度开放的数字行业准入制度

②明确的跨境数据流动规则（PDPA + 数据沙盒）

③监管透明度高、审批效率快

④优势定位：区域数字业务总部首选地

（2）中国香港特别行政区

①总体准入门槛较低，但部分行业（如电信、金融）仍受监管

②数据跨境制度灵活（PDPO）

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

③国际化法律体系与自由港制度

④优势定位：跨境电商与数字贸易枢纽

2.税收优惠优势经济体（Tax Incentive Leaders）

（1）新加坡

①数字产业企业所得税优惠（如适用当地减免政策可达5% 10%，且法定税率为17%，该优惠仅适用于先锋企业、发展与扩展激励等特定激励计划）

②区域总部激励（RHQ Incentive）

③科技创新与研发抵扣

④优势定位：亚太最具竞争力的数字税制

（2）马来西亚

MSC Malaysia 计划提供税收假期（Pioneer Status）

数字服务企业可享 5 10 年免税

优势定位：成本敏感型数字企业的落地选择

（3）越南

①高科技企业满足条件享 4 年免税 + 9 年减税

②软件企业享 10% 优惠税率

③优势定位：数字制造与软件外包中心

3.政策扶持优势经济体（Policy Support Leaders）

（1）中国

①国家级数字经济战略体系完善

②数字贸易试点区、跨境电商综试区政策密集

③强大的数字基础设施（5G、云、算力）

④优势定位：超大规模市场 + 完整数字产业链

三、行动清单

□对照目标经济体的准入制度，识别业务是否涉及外资准入、数据流动等监管要求。

□评估企业是否可享受当地数字产业税收优惠（所得税优惠、研发抵扣、免税期）。

□梳理目标经济体的数字产业扶持政策（试点项目、补贴、政府采购）。

□建立“准入—税收—政策扶持”三维度的区域落地评估矩阵。

□结合企业业务模式，选择“准入友好型”“税收激励型”或“政策扶持型”经济体作为优先落地市场。

□关注 APEC 区域内的互操作性政策（如数据流动、电子认证、数字身份）。

□在区域布局中纳入本地合作伙伴、人才政策与供应链参与要求。

Q44

在尚未出台人工智能专门立法的APEC经济体，其开展相应监管的依据是什么？

（撰写人：傅颉）

答：

一、核心提要

在尚未出台专项AI法规的法域，对AI活动的执法可依据现行法律进行。例如，为了解AI开发和使用对数据隐私的影响，香港特别行政区隐私监管机构——个人资料私隐专员公署（PCPD）——于2023年8月至2024年2月间对28家机构开展了专项合规检查，评估其在AI开发或使用中收集、使用和处理个人数据的做法，以及其AI治理架构。

二、法规矩阵与专业洞察

1.部分无专门AI立法的APEC经济体现行监管依据对比

经济体	核心替代性法律依据	主要监管工具	监管机构	未来走向
新加坡	个人数据保护法（PDPA）、消费者保护法	AI Verify框架（自愿）、FEAT原则、模型AI治理框架	PDPC、MAS（金融业）、IMDA	倾向维持软法路线
中国香港特别行政区	《个人资料（私隐）条例》（PDPO）	PCPD合规指引、HKMA和SFC行业通函	个人资料私隐专员公署、金管局、证监会	专项AI立法尚无明确时间表
澳大利亚	隐私法（Privacy Act 1988）、消费者法、反歧视法	Ai伦理框架（2019）、高风险AI应用政策	OAIC、ACCC	2026年前预期出台高风险AI专项要求
马来西亚	个人数据保护法（PDPA 2010）、通信多媒体法、电脑犯罪法	国家AI治理与伦理指南（非强制）	通讯部、国家AI办公室（2024年设立）	Ai路线图2021-2025到期后将修订
印度	数字个人数据保护法（2023年，已依2025年11月公布之配套《DPDP规则》分阶段生效）	非约束性监管建议（MEITY 2024年3月通知）	电子信息技术部（MEITY）	《数字印度法》草案含高风险AI条款
菲律宾	数据隐私法、网络犯罪预防法（RA 10175）	个人数据处理需向国家隐私委员会备案	国家隐私委员会	专项AI路线图已发布，立法准备中

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

2.替代性监管依据的具体运用逻辑

（1）数据保护法律是最主要的"兜底"依据。AI系统在训练、推理、输出各阶段几乎不可避免地涉及个人数据的处理。香港特别行政区已针对政府部门制定了专项伦理AI框架，确保公共部门AI应用标准一致，并以此为范本推动私营部门参照采用。

（2）行业监管规则在金融、医疗等高风险领域构成直接约束。香港金管局（HKMA）和证监会（SFC）已就银行和金融服务业发布了专项指南，专门针对信用决策、交易算法和客户服务自动化中的AI应用。

（3）非约束性行政工具事实上构成监管预期。部分法域已开始就规制AI服务的最佳路径进行探索性实践，即便正式AI法规尚未到位。

例如，印度监管机构——电子信息技术部——于2024年3月1日发布了一项非约束性建议，要求所有AI工具（包括AI模型、使用生成式AI的软件或任何算法）在当前阶段向用户进行适当标注与告知。

3.实务案例

新加坡在无AI专项立法的情况下，构建了目前APEC区域内公认较为完善的柔性AI治理体系，堪称"软法治理"的标杆：

首先，AI Verify框架代表了新加坡面向更广泛科技部门的旗舰治理工具，提供自愿认证和测试标准，帮助各机构证明其负责任的AI实践。2024年更新后，该框架为大型语言模型和内容生成系统提供了专项指导。

其次，新加坡金融管理局（MAS）的FEAT原则（公平、伦理、问责、透明度）嵌入金融领域的行业监管，实现了法律约束的软硬衔接。这一模式表明：即便没有AI专项立法，成体系的非立法性治理工具也能形成有效的合规预期。

三、行动清单

□ 在对客户提供AI合规意见前，区分目标经济体的监管状态——是"专项AI立法"、"依托现行法律框架"还是"仅有软法指南"，避免以简单的"无专项立法"作出"无合规义务"的错误判断。

□ 对于适用数据保护法律的AI场景，重点审查AI系统在训练数据收集、推理过程个人数据使用、输出结果涉及个人信息三个环节的合规性，特别关注自动化决策告知义务。

□ 针对金融、医疗、教育等受严格行业监管的领域，系统梳理各经济体行业监管机构（如金管局、证监会、保险监管机构等）已发布的AI专项指引，并将其纳入客户合规方案。

□ 对于尚处监管探索阶段的经济体（如马来西亚、菲律宾、印度尼西亚），建议在客户合同中纳入"AI监管合规适应条款"，约定当新专项法规出台时双方的合规义务分

□ 关注监管机构的非正式执法信号（如合规检查报告、监管通函、公开咨询文件），这些文件往往预示未来正式监管方向，是风险预判的重要来源。

□ 建议客户主动参与所在经济体的AI治理咨询程序，以在立法成形前建立与监管机构的沟通渠道，并影响有利于自身的监管走向。

Q45

APEC各经济体针对AI辅助“深度伪造”（Deepfake）诈骗有哪些监管应对路径？在此场景下，企业有哪些反诈合规义务？　　**（撰写人：冷勇达）**

答：

一、APEC主要经济体监管路径

1.中国

采取“源头治理+平台责任+人格权保护”组合的严格监管模式。依据《民法典》第1019条保护肖像声音权益；《互联网信息服务深度合成管理规定》第9条要求用户实名认证，第16条、第17条及《人工智能生成合成内容标识办法》要求对生成合成内容添加标识/水印；《生成式人工智能服务管理暂行办法》第9条至第14条要求服务商承担内容生产者责任，发现违法立即处置并报告。

2.美国

依托现有反诈框架，由职能部门依据现有法律解释执行。美国金融犯罪执法局（FinCEN）《关于针对金融机构的深度伪造媒体欺诈计划的警报》将深伪诈骗纳入《银行保密法》，要求金融机构提交可疑活动报告；美国联邦贸易委员会（FTC）《禁止冒充政府和企业贸易规则》将AI克隆欺诈定性为商业欺诈，拥有直接执法权。

3.新加坡

《网络犯罪危害法令》要求社交媒体和在线平台必须积极打击深伪诈骗广告，若核实或下架不力，将承担法律责任。

二、企业反诈合规义务

1.强化身份识别与活体检测：金融机构及支付企业须引入多因素验证和高级活体检测，识别AI合成影像，落实客户尽职调查。

2.重构资金支付验证流程：建立“零信任”审批机制。对音视频指令必须通过独立通道（如预留电话、加密软件）进行二次确认，实施高额交易多重签名。

3.平台内容标识与上报：AI及社交平台需对生成内容强制添加数字水印，建立快速举报通道，并在服务条款中禁止深伪欺诈，配合执法。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q46

APEC各经济体对“跨境交付”和“商业存在”数字服务有哪些外资股比限制？

（撰写人：王熙雨）

答：

一、核心提要

跨境交付（Mode 1）数字服务在 APEC 经济体普遍未设置外资股比限制，监管主要集中在数据、内容、安全与税收，而非股权。

商业存在（Mode 3）是外资股比限制的核心领域，尤其集中在：电信、云服务、数据中心、媒体、支付与金融科技。

中国、印尼、越南、菲律宾等经济体存在显著股比限制；新加坡、中国香港特别行政区、美国、澳大利亚等经济体基本无股比限制。

二、法规矩阵与专业洞察

1. Mode 1（跨境交付）数字服务：几乎无外资股比限制

跨境交付（如 SaaS、云服务、跨境电商平台、在线教育、数字广告等）不涉及本地设立实体，因此：

- APEC 经济体普遍不对 Mode 1 设置外资股比限制
- 限制主要体现在：
  - 数据跨境传输要求
  - 隐私保护
  - 内容监管
  - 税收（部分经济体征收数字服务税）
  - 网络安全要求

结论：Mode 1 的限制是“行为监管”，不是“股权监管”。

2. Mode 3（商业存在）数字服务：外资股比限制集中在关键基础设施与敏感行业

包括：

- 电信
- 云服务
- 数据中心
- 媒体与内容
- 金融科技
- 支付与清算
- 电子认证与数字身份

开放度	代表经济体	特征
高度开放	新加坡、中国香港特别行政区、美国、澳大利亚	几乎无股比限制
中度开放	日本、韩国、马来西亚、泰国	电信有限制，其他较为开放
审慎管理	中国、印尼、越南、菲律宾	电信/云/数据中心股比限制明显

- APEC 经济体的股比限制主要源自 电信法、投资负面清单、网络安全法、媒体法、金融监管法。
- 数字基础设施（云、IDC、网络）被视为“准关键基础设施”，因此股比限制普遍存在。
- 数字平台、SaaS、跨境电商等非基础设施类服务在多数经济体可 100% 外资。
- APEC 的数字贸易规则（如 AIDER、CBPR）强调数据流动与互操作性，但不涉及股比开放，股比仍属各国主权监管。

三、行动清单

- □ 对照目标经济体的电信法与负面清单，识别是否触发股比限制。
- □ 判断业务是否属于“基础电信”“增值电信”“云服务”“数据中心”等敏感领域。
- □ 评估是否需要本地合作伙伴、合资架构或本地控股要求。
- □ 建立 Mode 1 / Mode 3 的业务拆分策略，避免不必要的股比限制。
- □ 关注数据本地化、网络安全审查等“准入后监管”。
- □ 建立区域合规矩阵，覆盖准入、股比、数据、内容、税务等要素。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q47

哪些 APEC 经济体明确规定企业负有 Ai模型训练数据来源的披露义务？

（撰写人：何杨）

答：

一、核心提要

主要关注多数经济体对披露义务持鼓励态度、中国香港监管指引（软法透明要求）。

二、法规矩阵与专业洞察

类型	APEC经济体	法律依据	披露内容（截取）
第一类：监管指引下的透明度建议（非强制披露）的APEC经济体	中国香港特别行政区	《香港生成式人工智能技术及应用指引》第3.1条	（非强制性政策倡导)开发者应在可行情况下披露训练数据来源、模型架构及评估指标。
第二类：要求特定企业/企业在特定场景下披露数据来源的APEC经济体	中国台北	《人工智慧基本法》第4条	涉及个人信息要求披露、高风险AI则要求披露。
	越南	《人工智能法》第14条	涉及高风险AI则要求披露。
	韩国	《人工智能基本法》第34条	针对高风险AI:在技术上可行的范围内，对人工智能产生的最终输出、用于得出这些输出的主要标准以及在人工智能的开发和利用中使用的学习数据进行解释。 依韩国《人工智能基本法》，该披露义务仅适用于"高影响力AI（高风险AI）"，而非所有AI系统。
第三类：不涉及个人信息、敏感信息时，对企业暂未设定强制披露义务的APEC经济体	中国、美国（加州除外）、新加坡、新西兰、澳大利亚、泰国、俄罗斯、菲律宾、日本、巴布亚新几内亚、马来西亚、墨西哥、印度尼西亚、智利、加拿大、文莱、秘鲁。		

Q48

跨境AI侵权纠纷实践中，包含哪些主流纠纷解决机制？分别如何兼顾纠纷解决效率与数字资产的执行可操作性？

（撰写人：傅颉）

答：

一、核心提要

1. 国际仲裁是跨境AI侵权纠纷的首选机制：绝大多数受访者继续选择国际仲裁解决跨境纠纷，或单独适用，或与其他ADR方式结合使用。其核心优势在于裁决的跨境可执行性（《纽约公约》覆盖172个缔约国）、程序灵活性以及AI技术事项的保密性。

2. AI侵权纠纷呈现独特的"三重不确定性"：责任主体不确定（开发者/部署者/用户的责任分配）、管辖权不确定（侵权行为发生地与损害结果地跨境分离）、证据不确定（AI"黑箱"问题导致因果关系举证困难），这三重不确定性要求纠纷解决机制具备高度的专业性和灵活性。

3. 数字资产执行可操作性是跨境AI纠纷裁判后的核心难题：AI系统本身作为数字资产，其跨境扣押、禁令救济的地域效力限制，以及AI生成内容的知识产权归属争议，均使传统执行机制在AI语境下面临全新的适用挑战，需要在争议解决协议中进行前瞻性设计。

二、法规矩阵与专业洞察

1. 解决机制对比

解决机制	核心特征	提升纠纷解决效率的方式	保障数字资产执行可操作性的方式
商事仲裁	意思自治、一裁终局、跨境可执行	1. 适用数字经济专门仲裁规则 2. 简化数字证据认定流程 3. AI 辅助仲裁材料梳理	1. 明确数字资产查封、冻结的仲裁措施 2. 依据《纽约公约》实现裁决跨境执行 3. 区块链存证固定数字资产侵权证据
诉讼	法定管辖、公权力保障、二审终审	1. 专属知识产权法院 / 数字法庭集中管辖 2. 跨境司法协助简化取证流程 3. 小额纠纷速裁程序	1. 通过国际司法条约实现判决跨境执行 2. 对数字资产的网络服务提供者采取协助执行措施 3. 技术勘验确认数字资产权属与价值
在线争议解决（ODR）	线上操作、便捷高效、柔性解决	1. 全流程线上化，无需线下开庭 2. 专业技术专家参与事实认定 3. 快速调解达成和解协议	1. 和解协议可申请仲裁 / 诉讼确认效力 2. 数字资产托管机制保障和解履行 3. 依托平台对数字资产进行临时管控

（1）商事仲裁是跨境 AI 侵权纠纷的首选机制，因其一裁终局、跨境可执行的特性，适配数字资产的跨境流动属性，尤其适用于 AI 算法侵权、AI 生成内容著作权侵权、跨境数据服务侵权等复杂纠纷；诉讼适用于当事人未约定仲裁条款、数字资产权属存在重大争议的纠纷，依托公权力保障实现证据调取和强制执行；在线争议解决（ODR）适用于小额、简单的跨境 AI 侵权纠纷，如 AI 产品的小额知识产权侵权，通过线上调解快速解决，兼顾效率与成本。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

（2）在跨境AI侵权纠纷的执行层面，数字资产的特殊性带来三方面挑战：

其一，AI系统本身的扣押与估值困难。AI模型权重、训练数据集、推理API等数字资产难以像传统财产一样被物理扣押，其价值评估亦缺乏成熟标准。在裁判后的执行阶段，需要通过禁令（injunction）限制AI系统的持续使用，而禁令的跨境效力存在地域局限。

其二，AI生成内容的知识产权归属未决。在多个APEC经济体，AI生成内容是否享有版权保护、由谁享有，目前仍无定论，这直接影响侵权认定和损害赔偿计算的基础。

其三，"黑箱"问题加大证据举证难度。AI侵权诉讼面临的复杂性包括证据层面——例如AI的"黑箱"问题——使得责任推断和因果关系举证均面临独特挑战。仲裁庭或法院可能需要借助技术专家证人和AI系统审计程序才能完成事实认定。

2. 实物案例

2025年8月，日本三大报纸集团——读卖新闻、日经新闻和朝日新闻——分别对Perplexity AI提起诉讼，指控其未经授权"爬取"逾10万篇文章。该案展示了跨境AI版权侵权纠纷的典型特征：一方面，AI服务提供商总部注册地（美国）与侵权结果发生地（日本）跨境分离，管辖权选择成为首要法律问题；另一方面，爬取行为规模巨大、自动化程度高，难以逐一举证具体侵权内容，体现了AI侵权案件中证据固定和损害量化的挑战。该案目前正通过日本国内法院途径推进，但也显示出未来采用仲裁解决同类纠纷的现实空间。

三、行动清单

- ☐ 在跨境AI合作合同中明确仲裁条款，约定适用数字经济专门仲裁规则及管辖机构
- ☐ 预先设定数字资产的“估值逻辑”，以应对侵权后的损害赔偿计算争议。
- ☐ 建立企业数字资产的区块链存证体系，固定AI算法、生成内容等核心资产的权属证据
- ☐ 梳理目标国家/地区的跨境司法/仲裁执行条约，明确数字资产执行的法律依据
- ☐ 针对跨境AI侵权纠纷，制定“仲裁为主、诉讼/ODR为辅”的多元化解决预案
- ☐ 配备兼具法律与AI技术能力的复合型人员，参与跨境AI侵权纠纷的证据梳理与认定
- ☐ 关注国际及区域内数字经济纠纷解决规则的更新，及时调整企业合规与争议解决策略
- ☐ 对企业AI业务进行跨境侵权风险排查，提前规避算法、数据、生成内容的侵权隐患

Q49

企业训练模型使用公开数据是否需要授权？（撰写人：何杨）

答：

一、核心提要

敏感信息则需要、涉及受知识产权或个人信息保护的数据通常需取得授权。

二、法规矩阵与专业洞察

企业训练模型使用公开数据并非绝对豁免授权义务，需结合数据权利属性、法律规定及使用场景综合判定，核心边界在于“公开可自由利用”与“公开但受知识产权、个人信息保护法约束”的区分。

从法律依据看，《生成式人工智能服务管理暂行办法》第七条明确要求训练数据须具备合法来源，不得侵犯他人知识产权；《著作权法》规定，即便数据公开，只要具备独创性的文字、图片、视频等作品，商业性使用原则上需取得著作权人授权，仅法定“合理使用”情形可豁免；《个人信息保护法》进一步明确，公开渠道获取的对个人权益有重大影响的个人信息，用于模型训练时需取得个人单独同意；只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。

实务案例：

案号：（2024）浙01民终10332号）

上海某文化公司经授权享有案涉奥特曼动漫形象的知识产权及维权权利。杭州某智科公司运营某AI平台，提供模型训练、图生图服务，平台内存在用户上传的奥特曼 LoRA 模型，可生成与该形象实质性相似的图片。该文化公司起诉主张智科公司侵权。一审法院认定，被告不构成直接侵权，但被告未尽到合理注意义务，存在主观过错，构成帮助侵害涉案奥特曼作品信息网络传播权的行为。二审维持原判。

综上，企业需明确：无权利负担的公开数据通常可直接使用；受著作权保护的公开作品，商业训练需优先获取授权，严格限定合理使用范围；含个人信息的公开数据，必须履行个人同意程序或符合法定例外。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q50

APEC主要经济体围绕AIGC生成内容的版权保护，司法实践与主管机关对独创性标准以及人类作者身份的要求有何差异?

（撰写人：王熙雨）

答：

一、核心提要

APEC 主要经济体普遍坚持“人类作者”原则，纯 AI 生成内容不被视为可版权保护的作品。

差异主要体现在“人类参与程度”要求不同：美国要求“可识别的人类创作贡献”，中国强调“智力投入”，日本与韩国采用“创作性表达”标准。

监管机关态度差异明显：美国采取严格审查，中国采取“有限承认 + 案例推动”，日本与韩国保持传统框架，澳大利亚倾向于保持现行制度不变。

司法实践正在成为关键推动力，尤其是美国与中国的判例逐步形成区域影响。

二、法规矩阵与专业洞察

经济体	独创性标准	人类作者要求	对 AIGC 的态度
美国	较低创造性 + 独立创作	必须有人类可识别贡献	较为严格，不保护纯 AI
中国	智力投入 + 个性化表达	人类需对生成过程有实质控制	较为灵活，部分案例承认
日本	创作性表达	人类作者原则	保守，强调人类控制
韩国	创作性表达	人类智力活动	保守，与日本类似
澳大利亚	人类技能与判断	不承认 AI 作者	保持传统框架

APEC 主要经济体在 AIGC 版权保护上形成“共同底线 + 差异化路径”的格局：共同底线是坚持人类作者原则，不承认纯 AI 作品；差异化路径体现在对“人类参与程度”的要求不同，美国较为严格，中国较为灵活，日本与韩国保持传统框架，澳大利亚维持现行制度。司法实践正在成为推动规则演进的关键力量，尤其是美国与中国的判例逐步形成区域影响。

Q51

在APEC经济体销售带AI功能的硬件产品通常需要哪些认证?

（撰写人：冷勇达）

答：

一、美国

1. FCC认证：

依据：美国《联邦通信委员会法规》第15部分（47 CFR Part 15）。

2. UL/ETL安全认证：

虽然联邦未强制要求所有产品提供UL认证，但美国职业安全与健康管理局（OSHA）要求工作场所设备必须由国家认可测试实验室（NRTL）认证。各大零售商（如亚马逊、百思买）也会强制要求提供NRTL颁发的安全证书。

依据：OSHA《联邦法规》29 CFR 1910.7。

二、中国

1. CCC认证：

涵盖产品的电气安全和电磁兼容性（如电源适配器、音视频设备、信息技术设备）。

依据：《强制性产品认证管理规定》及《中华人民共和国产品质量法》。

2. SRRC认证：

针对所有具备无线发射功能（Wi-Fi、蓝牙、5G等）的AI硬件。

依据：《中华人民共和国无线电管理条例》。

3. 进网许可(NAL)：

如果AI硬件直接接入公用电信网（如带有SIM卡的AI路由器或智能终端），需申请此证。

依据：《电信设备进网管理办法》。

三、日本

1. PSE认证：

针对电气安全。电源及特定范围内的AI硬件需申请菱形（特定电气用品）或圆形（非特定电气用品）PSE标志。

依据：日本《电气用品安全法》。

2. TELEC认证/MIC认证：

针对射频合规，带无线功能的设备必须获得此认证。

依据：日本《电波法》。

3. VCCI认证(自愿性)：

针对电磁兼容（EMC），虽为自愿，但在日本市场属于事实上的行业通行标准。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q52

Ai系统造成损害时，不同主体的责任如何分配?

（撰写人：王熙雨）

答：

一、核心提要

AI 造成损害的责任分配通常围绕“谁对风险具有控制力、谁能预见风险、谁从中获益”三个核心原则展开。

二、法规矩阵与专业洞察

在 APEC 经济体中，责任主体一般包括：开发者（Developer）、提供者/平台（Provider）、部署者/使用者（Deployers/Users）、数据提供者（Data Providers）、硬件/基础设施提供者（Infrastructure Providers）不同经济体的差异主要体现在：是否采用 产品责任路径、是否强调 使用者责任、是否引入 平台责任、是否对 高风险 AI 设定更严格义务。具体如下：

1. 开发者责任（Developer Liability）

开发者通常承担以下责任类型：

（1）产品缺陷责任（Product Liability）

适用情形：

- AI 系统存在设计缺陷、制造缺陷、警示缺陷
- 开发者未能提供合理的安全保障或风险提示

典型经济体：美国、澳大利亚、日本

（2）过失责任（Negligence）

适用情形：

- 未进行充分测试
- 未遵守行业标准
- 未采取合理的安全措施
- 未修复已知漏洞

（3）高风险 AI 的特别义务

部分经济体（如中国、韩国）对高风险 AI 要求：

- 风险评估
- 可解释性
- 人类监督
- 安全监测

2. 提供者/平台责任（Provider / Platform Liability）

平台责任在 APEC 区域差异较大，但通常包括：

（1）内容责任（Content Liability）

适用情形：

- AI 生成违法内容
- 平台未履行合理审核义务
- 未及时处理用户投诉
- 同时应考虑当地是否适用“避风港原则 + 过错责任”

典型经济体：韩国、日本、中国

（2）共同责任（Joint Liability）

部分经济体要求平台与开发者共同承担责任，尤其在：

- 生成式 AI
- 自动驾驶
- 金融科技
- 医疗 AI

3. 部署者/使用者责任（Deployer / User Liability）

APEC 多数经济体强调“使用者责任”，尤其是中国、日本、韩国。

（1）不当使用责任（Misuse Liability）

适用情形：

- 用户将 AI 用于违法用途
- 用户未遵守使用说明
- 用户未进行必要的人类监督

（2）服务瑕疵责任（Service Defect Liability）

适用情形：

- 平台提供的 AI 服务不符合承诺
- 算法推荐导致损害
- 平台未提供必要的安全保障

（3）过失责任（Negligence）

适用情形：

- 未对 AI 输出进行合理审查
- 未采取必要的安全措施
- 未对高风险场景进行人工复核

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

（4）高风险行业的特别责任

如：

- 医疗
- 金融
- 自动驾驶
- 公共安全

这些行业通常要求使用者承担更高的注意义务。

4. 数据提供者责任（Data Provider Liability）

数据质量直接影响 AI 风险，因此部分经济体引入数据责任：

（1）数据瑕疵责任

适用情形：

- 数据错误导致 AI 输出错误
- 数据偏见导致歧视性结果
- 数据泄露导致隐私损害

（2）合规义务

包括：

- 数据合法来源
- 隐私合规
- 数据最小化
- 数据安全

5. 硬件/基础设施提供者责任（Infrastructure Liability）

（1）适用情形：

- 芯片、传感器、服务器故障导致损害
- 云服务中断导致损失
- 网络安全漏洞导致攻击

（2）责任类型：

- 产品责任
- 服务合同责任
- 安全保障义务

APEC 经济体普遍采用“多主体并行责任”模式：开发者承担产品与设计责任，平台承担服务与内容责任，使用者承担操作与监督责任，数据提供者承担数据质量责任，基础设施提供者承担系统安全责任。高风险 AI 场景中，责任通常呈现“叠加式”结构。

三、行动清单

□ 明确企业在 AI 价值链中的角色（开发者/提供者/使用者）。

□ 建立 AI 风险评估机制，覆盖数据、模型、输出、部署。

□ 对高风险 AI 场景建立人类监督机制。

□ 完善用户协议、免责声明与使用说明。

□ 建立数据质量管理体系与偏见检测机制。

□ 建立 AI 安全事件响应机制与通报流程。

□ 对接各经济体的 AI 监管框架，建立区域合规矩阵。

Q53

AI模型输出不准确，在何种情况下可能构成法律风险？　　**（撰写人：何杨）**

答：

一、核心提要

侵权、隐私侵害、刑事。

二、法规矩阵与专业洞察

序号	风险类型	具体情形	法律依据（参考）
1	人格权侵害	1.1. 输出侮辱性言论、捏造信息，贬损他人名誉。 1.2. 未经授权披露/虚构他人隐私信息、肖像、身份信息。	《生成式人工智能服务管理暂行办法》第4条第4项、第9条及《中华人民共和国民法典》人格权编相关规定等。
2	知识产权侵权	2.1. 输出内容实质性抄袭受版权保护的文本、图片、代码、设计等。 2.2. 错误标注/冒用他人商标、专利。 2.3. 训练数据侵权导致输出侵权（源头过错）。	《生成式 AI 服务管理暂行办法》第 7 条等。
3	刑事风险	3.1. 利用 AI 输出诈骗信息、虚假证件、伪造文书，实施诈骗、伪造等犯罪。 3.2. 故意训练/操控 AI输出违法内容，可能构成犯罪。	《刑法》第 266 条（诈骗罪）、第 280 条（伪造、变造、买卖国家机关公文、证件、印章罪）等。

实务案例：

案号：(2024)浙0108民初10311号

法院认为：本案中，首先，从主观方面分析，被告李某某作为自媒体运营者，发布被诉侵权文章，系为增粉引流谋取其自身的商业利益，便于其账号推广相关商品；但其作为自媒体博主，负有审核所发布的信息真实性的义务，在明确知晓被诉侵权文章系人工智能自动生成，信息来源不可靠的情形下，未对被诉侵权文章内容进行最低程度的审核，亦未在文章中进行显著标注，提示公众该文章系由人工智能生成，使得包含虚假信息的内容通过互联网传播；且通过手动添加带有原告品牌标识的配图的方式进一步加强了文章的误导性，故李某某发布被诉侵权文章的主观过错明显，其行为违背了相应的商业道德。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q54

在对AI提出透明度或可解释性要求的监管或行业场景中，AI产品如何满足可解释性要求？（撰写人：冷勇达）

答：

以下是主流监管场景中AI产品满足可解释性和透明度要求的具体路径，以及对应的法律法规与标准依据：

1. 欧盟

合规要求：

（1）前端交互透明：如果产品是聊天机器人或生成式AI，须在UI界面显著位置告知用户“正在与AI互动”；深度合成内容须添加水印或明确标记为“AI生成”。

（2）底层逻辑可解释：用于医疗、招聘、信用评分等高风险AI，须附带详尽“使用说明”，解释系统功能边界与输出逻辑，便于人类监督。

法律依据：《欧盟人工智能法案》（EU AI Act）第13条、第50条。

2. 美国

合规要求：在敏感或高风险应用中，应根据场景选择适当的可解释性方法，包括使用事后解释技术（如SHAP、LIME等）对模型输出进行影响因素分析，或在适用情况下采用结构更透明的模型，以提升结果可理解性。

解释内容分层：面向数据科学家提供特征权重图，面向普通用户提供自然语言说明。

参考依据：美国国家标准与技术研究院《AI风险管理框架》（AI RMF 1.0）（自愿性行业框架）

3.中国

合规要求：

（1）算法备案与披露：具有舆论属性或社会动员能力的AI产品须在官方备案系统中说明算法原理、应用目的、运行规则与主要影响因素。

（2）用户协议说明：在服务协议中设置专门条款，解释数据收集方式、处理规则与AI服务的基本运行机制。

内容强制标识：生成式AI生成内容应进行显著标识，以确保用户能够识别其为人工智能生成内容；水印、元数据标记等技术手段可作为实现方式之一，但具体方式应满足显著、可识别的要求。

Q55

中小企业部署AI时应特别注意哪些合规要求？（撰写人：何杨）

答：

一、核心提要

法律合规：包括数据合规、知识产权合规、内容标识

服务备案：算法备案

商业秘密与保密合规：本地化部署

二、法规矩阵与专业洞察与行动清单

合规类型	具体内容	法律依据（参考）
数据合规	1. 合法收集数据： 第一，避免使用未经授权或非法获取的数据，尤其涉及个人信息、版权作品等； 第二，收集个人信息需遵循“最小必要”原则，取得用户明确同意，敏感个人信息需单独同意。	《中华人民共和国数据安全法》第32条； 《中华人民共和国个人信息保护法》第6条、第10条、第13条、第29条。
	2. 数据出境合规： 若涉及跨境数据传输，需选择合规路径，如：数据出境安全评估、个人信息保护认证、签订《个人信息出境标准合同》并备案等。	《中华人民共和国个人信息保护法》第38条、第39条； 《网络数据安全管理条例》第35条； 《数据出境安全评估办法》第4条； 《个人信息出境标准合同办法》第4条、第5条、第7条。
知识产权合规	1. 训练数据、生成内容合规： 避免在训练数据中使用未经授权的版权作品，导致侵权；同时，建议企业留存提示词优化、参数调整、手动修改等过程记录，以证明生成内容中的人类创作贡献，并在著作权归属、独创性认定或侵权争议中作为辅助证明材料；同时仍应另行审查生成内容是否与他人在先作品、商标、肖像或其他受保护权益发生冲突。	《生成式人工智能服务管理暂行办法》第7条。
内容标识	1. 履行标识义务：AI生成内容需添加显式或隐式标识。如：在文本的起始、末尾或者中间适当位置添加文字提示或者通用符号提示等标识，或者在交互场景界面、文字周边添加显著的提示标识；在图片的适当位置添加显著的提示标识等。	《生成式人工智能服务管理暂行办法》第12条； 《互联网信息服务深度合成管理规定》第16条； 《人工智能生成合成内容标识办法》第4条、第5条、第6条。
算法备案	备案要求： 若AI服务具有舆论属性或社会动员能力，需通过互联网信息服务算法备案系统进行备案，并持续履行备案更新义务。	《互联网信息服务算法推荐管理规定》第24条； 《生成式人工智能服务管理暂行办法》第17条。
商业秘密与保密合规	建议本地部署优先：在同等条件下，建议优先选择本地化部署的AI模型，减少数据上传风险，降低商业秘密泄漏可能性。	—

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容



Q56

APEC各经济体对算法的公平性、透明度、可解释性分别建立了何种规制体系？存在哪些差异？

(撰写人：王鹤臻)

答：

APEC各经济体对算法的公平性、透明度和可解释性在规制体系上的差异较大，因为这些问题涉及到不同国家的法律体系、技术发展水平、市场需求和政策环境。

一、公平性（Fairness）

公平性是算法监管中的关键问题，特别是在涉及就业、金融、健康等领域时。各经济体在公平性方面的规制往往聚焦于如何避免算法在决策过程中产生偏见（例如种族、性别、年龄等歧视）。

1.美国：美国没有统一的联邦级算法公平性法律，但在某些领域（如金融、医疗保健）有相关的规定。例如，金融行业的《公平信用报告法》（FCRA）要求确保信用评分模型不产生歧视性影响。此外，一些州（如加州）有专门的算法偏见法律。

2.欧盟：欧盟在2021年提出了《人工智能法案》，该法案对高风险AI系统（包括招聘、金融、法律等领域的算法）提出了公平性要求，特别要求算法能够经过审查，确保其结果不对特定群体产生偏见。

3.中国：我国目前没有专门的“算法公平法”，公平性要求主要分散在《个人信息保护法》第二十四条、算法推荐管理规定以及生成式人工智能和拟人化互动服务专项等部门中。《个人信息保护法》第二十四条要求自动化决策保证公平和结果公平、公正，并赋予个人对自动化决策的指示请求权、拒绝权算法推荐、生成式人工智能和拟人化交互服务规则则通过备案、安全评估、内容治理、透明提示和用户退出机制等制度，防止算法补缺和不合理差别待遇。整体而言，中国算法公平监管仍呈现“基础法+分领域部门”的混合模式，尚未形成统一的算法算法典。

二、透明度（Transparency）

透明度要求算法的操作原理、数据来源、决策流程等信息能够对用户和相关监管部门公开，尤其是在公共服务领域。

1.美国：美国的算法透明度更多体现在行业规范和自愿性规定上，如一些技术公司会发布“透明度报告”，但这些都是行业内部的做法，没有强制性要求。

2.欧盟：欧盟的《人工智能法案》要求高风险AI系统提供足够的透明度，用户应该能够理解AI如何做出决策。这也包括对外公开算法的核心机制，并允许相关机构进行审查。

3.中国：中国在《网络安全法》及《数据安全法》中提到，企业需要对其算法进行自我审查和报告，但在实际执行中透明度要求较低，且更多是针对数据安全而非算法过程本身。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

三、可解释性（Explainability）

可解释性要求算法能够提供对其决策过程的解释，尤其是当算法决策影响到个人权益时。

1.美国：美国没有强制性的法律要求算法具有可解释性，但在金融领域，如信用评分等，要求算法能够提供某些决策依据和可解释的报告。

2.欧盟：欧盟《人工智能法案》强调可解释性，特别是在高风险AI系统中，要求其决策过程对最终用户可理解，能够为用户提供反馈，并使其能质疑算法决策。

3.中国：中国在《个人信息保护法》中提到，数据处理和自动化决策必须可解释，尤其是在涉及到消费者权益时，企业应当提供透明的决策过程和解释机制，但在实施细节上较为模糊。

差异总结：

强制性与自愿性：美国和中国的算法规制体系较为松散，透明度和公平性要求多为行业自愿遵守，缺乏强制性规定。相对而言，欧盟的《人工智能法案》更为严格，要求强制执行高风险AI系统的透明度、公平性和可解释性。

领域差异：不同经济体对算法规制的重点不同。美国和欧盟主要关注金融、就业等领域，而中国则更加强调数据隐私和安全，尤其是在互联网和大数据领域。

法律覆盖范围：欧盟的法规覆盖范围较广，涉及大部分AI应用，尤其是在高风险领域。而美国更多依赖行业自律和地方性法规。中国的法规则相对较新，且强调技术和数据的安全性，但在算法决策的公开透明方面仍在探索阶段。

Q57

哪些APEC经济体设置了推荐算法的监管备案制度？未要求备案的经济体，通过何种监管路径保障推荐算法的合规性？

（撰写人：王鹤臻）

答：

一、设立推荐算法监管备案制度的经济体

1.中国

中国是目前在推荐算法监管方面最为积极的经济体之一。2022年发布的《互联网信息服务算法推荐管理规定》明确要求，所有使用算法推荐服务的互联网平台需要向主管部门备案。这些平台必须提供其算法推荐的工作原理、数据来源、规则及其对用户可能产生的影响等详细信息。

备案要求：平台需在算法使用前向相关主管部门报备，并在后续的运行过程中根据监管要求进行更新和审查。

监管路径：备案制度的实施为监管机构提供了透明度和可审查性，确保平台使用的推荐算法符合公平性、透明度、可解释性等要求。

2.韩国

韩国虽然没有明确要求所有推荐算法都进行备案，但在数据隐私和算法使用的透明度方面有明确规定。根据《个人信息保护法》和《信息通信网络法》的要求，任何涉及用户数据的推荐算法都需要在数据收集和处理前进行审查。

备案要求：在某些特定情况下，平台需要向相关部门提交数据使用和算法推荐的详细报告，尤其是在处理敏感个人数据时。

监管路径：通过数据保护法和行业规范，韩国通过对数据使用的监管来间接管理推荐算法，确保其合规性。

二、未要求推荐算法备案的经济体及其监管路径

1.美国

美国并未在联邦层面设立强制性的推荐算法备案制度，但通过现有法律框架对推荐算法进行监管。

监管路径：消费者保护法：美国联邦贸易委员会（FTC）通过《联邦贸易委员会法》以及《公平信用报告法》等消费者保护法，确保推荐算法不产生不公平或误导性结果。FTC对违反消费者权益的算法行为进行处罚。

行业自律和透明度报告：美国的科技巨头（如Google、Facebook等）通常会发布透明度报告，虽然这些报告多为自愿性质，但它们有助于提供一定的算法透明度和合规性。

数据隐私法规：例如，加利福尼亚州的《加利福尼亚消费者隐私法案》（CCPA）要求公司向消费者披露数据收集、处理及使用情况，确保推荐算法遵循数据隐私规定。

2.日本

日本没有专门设立推荐算法备案制度，但其通过《个人信息保护法》以及其他相关法规监管数据收集和处理过程，间接影响推荐算法的合规性。

监管路径：数据保护法：根据《个人信息保护法》，所有涉及到个人数据的推荐算法必须符合透明性、合法性和公正性的要求。平台需确保用户的数据使用符合隐私保护标准，且提供必要的解释权。

反垄断法：日本公平贸易委员会（JFTC）也对涉及竞争问题的推荐算法进行监管，避免算法被用来进行市场操控或不正当竞争。

3.澳大利亚

澳大利亚同样未设立专门的推荐算法备案制度，但通过现有的法律框架确保推荐算法的合规性。

监管路径：消费者保护和反垄断法：澳大利亚竞争与消费者委员会（ACCC）监管算法是否在市场中产生不正当影响，并确保消费者不受算法带来的误导或不公平待遇。该委员会也审查平台是否存在通过算法进行价格操控或不公平竞争的行为。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

隐私法：《 隐私法 》要求平台在使用个人数据时提供透明度，确保算法处理数据的合规性，并确保用户可以管理其个人数据的使用。

4.新加坡

新加坡没有强制要求推荐算法备案，但通过现有的数据保护法规和反垄断法规保障算法的合规性。

监管路径： 数据保护法：新加坡《 个人数据保护法 》（ PDPA ）规定了数据处理的透明度和用户同意要求，确保推荐算法不侵犯个人隐私。

竞争法：新加坡竞争与消费者委员会（ CCCS ）监管平台是否通过推荐算法进行不正当竞争或市场操控行为。

5.加拿大

加拿大并未设立专门的推荐算法备案制度，但通过相关法律来监管算法合规性。

监管路径： 隐私法：加拿大《 个人信息保护和电子文档法 》（ PIPEDA ）规定，企业在使用推荐算法时必须遵循严格的数据隐私要求，确保用户的个人数据不会被滥用。

反垄断法：加拿大竞争局（ Competition Bureau ）会审查涉及不公平竞争的推荐算法，确保市场公平性和竞争性。

Q58

APEC各经济体对“个性化推荐”提出了哪些合规要求?

（ 撰写人：秦雨歌 ）

答：

一、核心提要

APEC隐私框架原则：APEC隐私框架的九大原则构成了个性化推荐合规的基石（ 防止损害、通知、收集限制 、使用限制、选择权、信息完整性、安全保障、查阅与更正、问责制 ）；

立法路径呈现多元化：各经济体采取不同监管路径，其中约1/3已有专项或直接适用的立法（ 中国、韩国、日本、新加坡等 ），其余经济体主要依托通用隐私法框架间接规制，少部分国家尚无综合性数据保护法

透明度与用户控制权是共性要求："透明度/告知义务 + 用户选择退出权"是跨经济体合规的基线要求，但信息披露深度、选择退出的操作便利性要求存在差异。

二、法规矩阵与专业洞察

经济体/区域	透明度要求	退出权	其他要求
中国	公示算法基本原理、目的及运行机制；不得默认同意收集用户偏好	提供便捷关闭选项，关闭后立即停止服务；自动化决策推送须同时提供非个性化选项或便捷拒绝方式	禁止向未成年人推送诱导沉迷内容；禁止大数据差异化定价；禁止操纵热搜、榜单等公共信息呈现
新加坡	收集数据前须告知目的；《 AI治理框架 》建议披露推荐系统使用情况及决策逻辑（ 自愿 ）	用户有权撤回同意，撤回后须停止数据处理；不得以服务降级阻止用户行使撤回权	《 Ai治理框架 》建议对推荐系统建立人工监督机制（ 尤其决策结果对用户有实质性影响时 ），以及对高风险推荐场景（ 如涉及金融产品、医疗信息的个性化推荐 ）进行可解释性设计，并定期开展影响评估
美国加州	隐私政策须披露收集的数据类别、共享对象、目的说明及消费者各项权利	消费者有权拒绝出售或共享个人信息（ 含跨场景广告 ）；13-16岁未成年人须本人选择加入，13岁以下须监护人同意；须响应GPC一键退出信号	重大影响场景（ 就业、信贷、住房等 ）拟设人工复核权（ 草案 ）

上表按各经济体监管强度与模式进行分类，列举①强规制型中国，②权利导向型美国加州，③自主治理型日本、新加坡在算法透明度、用户退出权等重点合规方面的差异化要求。

三、行动清单

□ 识别适用法规：对照各经济体监管梯队，确认业务所涉产品是否触发中国、韩国等强监管法规，或其他国家的通用隐私法。

□ 用户控制界面设计：以高标准为基线（ 如中国《 互联网信息服务算法推荐管理规定 》为，确保推荐开关“显著可见”、退出步骤不超过进入步骤 ）；在加州产品中同步启用GPC信号识别，满足多市场最低要求。

□ 实施未成年人差异化策略：针对中国（ 禁止诱导沉迷 ）、韩国（ 深夜推送限制 ）、美国（ 13岁以下opt-in，加州16岁以下opt-in ）的差异化要求，建立年龄识别与推荐策略。

□ 建立季度动态追踪机制：重点跟踪业务相关国家针对人工智能、算法相关的法规要求及更新，提前启动差距分析。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q59

在何种情况下，自动决策系统是否必须需要人工复核机制?

（撰写人：秦雨歌）

答：

一、核心提要

重大影响决策强制复核：当自动决策对个人产生法律或类似重大影响（如就业、信贷、住房、医疗、福利资格等）时，必须提供人工复核机制

用户异议触发复核义务：绝大多数APEC经济体仅在当事人主动申请时才触发响应义务，企业无需主动提供

高风险领域预设监督：涉及关键基础设施、公共安全、基本权利保障的高风险AI系统，须建立实时人工监督和决策审核机制

二、法规矩阵与专业洞察

触发情形	强制程度	代表性经济体
对个人权益有重大影响的自动化决策（信贷、就业、教育、医疗等）	强制	中国
高影响AI系统在受监管领域使用	强制（特定场景）	韩国
金融信贷领域基于消费者报告的不利决定	强制（金融行业专项）	美国
当事人主动申请说明或复核	强制（须响应）	中国、新加坡、泰国
系统产生歧视性/偏差性输出并收到投诉	应依规响应	各经济体通用
涉及儿童或弱势群体的自动化决策	强制（特定群体）	中国、美国

工复核机制的适用场景在主要法域呈现较高共识：以“对个人的重大影响”为核心判断标准，但"重大影响"的界定各经济体尚无统一标准。高风险领域（如关键基础设施）预设人工监督已成为立法趋势。

三、行动清单

□ 识别重大影响决策场景：梳理业务中涉及就业、信贷、住房、医疗、保险、教育、福利资格等领域，确认是否使用自动化决策系统。

□ 建立用户异议处理通道：设立便捷的申诉渠道，允许用户对自动化决策结果提出异议，并明确告知申请人工复核的方式和时限。

□ 设计有效的人工复核机制，避免形式合规：确保复核者有权限查看完整决策依据、有能力推翻系统结论、有充足时间独立判断。

□ 完成风险评估与记录保存：对高风险自动化决策系统开展影响评估，保存评估记录备查，并按法规要求公开披露。

□ 对金融信贷、招聘筛选、医疗辅助三类高风险场景制定专项方案：这三类场景在所有有成熟立法的APEC经济体中均触发高强度复核义务，且存在行业监管叠加义务（如银保监会），须单独进行差距分析，不可依赖通用隐私合规框架覆盖。

Q60

在自动化决策或算法推荐等应用场景中，如何判断算法是否存在歧视风险?

（撰写人：秦雨歌）

答：

一、核心提要

全生命周期检测：算法歧视风险需从数据层（训练数据是否存在历史偏见或样本偏差）、模型层（算法是否对不同群体产生差异化影响）、结果层（实际运行是否导致系统性不公）进行全生命周期检测

关注“差异化影响”而非意图：判断歧视的关键是算法的实际输出对不同群体是否产生统计学意义上的显著差异，而非算法设计者是否有歧视意图

建立检测与缓解机制：需通过算法备案、影响评估、公平性测试等机制主动发现并缓解偏见，而非被动等待投诉

二、法规矩阵与专业洞察

经济体	受保护属性核心范围	量化判断标准
中国	无明文列举，以“不合理差别待遇”为认定标准	无统一量化标准；实践中以“交易价格等交易条件上的不合理差别”为核心判断
美国	种族、肤色、宗教、性别、国籍（就业）增加残障、家庭状况（住房/信贷）	4/5规则（就业）；须“业务必要性”方可抗辩
新加坡	PDPA未列举受保护属性；《AI推荐与决策系统个人数据使用指引》建议偏差评估文档化	无统一量化标准；《AI推荐与决策系统个人数据使用指引》建议使用AI Verify工具进行公平性测试
韩国	性别、年龄、种族、残障等（基本权利保障框架）	《AI基本法》要求高影响AI须建立风险管理计划；下位法规尚待细化

"代理变量"是算法歧视中最隐蔽的法律风险：网信办在发布《算法推荐管理规定》时明确，算法歧视、"大数据杀熟"、诱导沉迷等算法不合理应用，其中大数据差异定价的典型情形——以"设备类型、消费历史"等作为定价依据——已被认定为间接歧视的代理变量，平台须定期自查。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

美国四机构明确算法歧视三大来源（2023.4联合声明）：①训练数据导入历史偏见；②“黑箱”模型不透明性；③第三方部署可能扩大歧视影响。各机构将“运用集体权力保护个人权利，无论违规通过何种技术发生”。

三、行动清单

□建立算法公平性影响评估（AFIA）流程：强制执行“数据–模型–输出–影响”四层次算法公平性影响评估，作为产品上线的前置件。

□实施特征集代理变量扫描：每季度扫描推荐与决策特征集，识别与受保护属性（性别、年龄、地区等）相关系数>0.3的特征，建立敏感特征白名单。

□在高风险场景部署差异影响监控：对信贷、就业、医疗、定价等高危场景，按受保护属性分组监控输出差异；参照EEOC 4/5规则（不利群体通过率低于最优群体80%）触发人工审查设置差异影响预警阈值；对中国场景同步监控定价差异。

□针对各经济体建立"受保护属性地图"：梳理各经济体受保护属性清单，以最宽泛标准设计统一公平性审查，通过合同条款将合规要求传导至第三方供应商。

□建立歧视投诉快速响应机制并定期开展算法审计：设立投诉专线，承诺48小时确认、15个工作日完成调查；每半年审计一次，模型更新或数据集更换后上线前须审计。

Q61

若算法自动决策导致服务贸易合同违约（如金融授信失败），企业的法律责任是什么？责任认定通常会考虑哪些因素，是否存在合理的抗辩或免责空间？　　（撰写人：王鹤臻）

答：

一、算法自动决策导致合同违约的法律责任

在现代商业环境中，算法自动决策广泛应用于服务贸易合同的履行中，例如金融服务中的授信决策、保险理赔的自动处理、电子商务平台的订单处理等。然而，若算法自动决策导致违约，企业可能需要承担一定的法律责任。

1.合同责任的基本认定

根据合同法，企业与客户（或其他合同方）之间形成的服务贸易合同属于民事合同范畴。如果由于算法的错误或不当决策导致合同未能履行，或合同履行不符合约定条款，企业可能需要对其违约行为负责，承担以下几种形式的法律责任：

赔偿损失：企业需要向对方支付因违约所造成的损失，包括直接损失和间接损失。

支付违约金：若合同中约定了违约金条款，企业可能需要按照合同约定支付违约金。

修正或履行合同：在某些情况下，企业可能被要求修正算法错误并继续履行合同，或恢复合同的正常执行状态。

2.责任承担的主体

算法开发者：如果算法的开发方（例如技术提供商）与使用方（企业）之间有明确的合同关系，并且算法本身存在缺陷或未能达到合同要求，开发者可能需要承担部分责任。

算法使用者（企业）：如果企业使用外部提供的算法并依赖其做出重要决策，企业作为算法的使用者仍然需要对因其决策结果导致的合同违约负责，除非能够证明算法的失败完全由第三方的失误或不可抗力因素造成。

3.典型违约情形

金融授信失败：例如，银行或金融机构基于自动化的信用评分算法做出贷款授信决策，若算法错误导致借款人未能符合授信标准，而金融机构未按合同提供贷款，则可能构成违约。

保险理赔拒绝：若保险公司使用算法自动处理理赔请求，但算法错误拒绝理赔，导致保险合同无法履行，保险公司可能需承担违约责任。

二、责任认定时的关键因素

在判断企业是否应承担因算法自动决策导致的合同违约责任时，通常会考虑以下几个关键因素：

1.算法是否存在缺陷或错误

算法设计与执行的合理性：法院或监管机构会审查算法的设计和执行是否符合行业标准和合同约定。如果算法存在设计缺陷或执行错误，企业可能被判定为未履行合同义务，进而承担违约责任。

算法的透明度和可解释性：如果算法无法解释或提供充分的决策依据，可能会导致企业在面对合同争议时处于不利地位，法院或仲裁机构可能认为企业未能履行充分的审查义务。

2.企业的审查与监管义务

合理审查义务：企业作为算法的使用方，需对算法的决策结果进行合理审查，确保其符合合同约定。如果企业未能充分审查算法的决策，可能会被认定为疏忽，承担相应责任。

数据质量和处理流程：若算法依赖的数据质量不佳（如数据不准确、数据不完整），企业未能采取适当措施清理和验证数据，可能需要承担部分责任。

3.合同条款及免责条款

合同的免责条款：企业与客户签订的服务贸易合同中可能会包含免责条款，规定在特定情况下，如技术故障、不可抗力等情况下，企业可以免除责任。若算法的故障或错误属于合同约定的免责情形，企业可能不需要承担违约责任。

可操作性与灵活性：合同条款中关于违约的条款是否具备灵活性，允许在算法错误的情况下进行修正，可能影响法院对违约责任的认定。

4.第三方责任与外部因素

外部算法开发者或技术提供商责任：如果算法的设计或执行过程中存在第三方的技术缺陷，企业作为使用方可以通过向第三方追索来减轻其责任，尤其是在合同明确规定技术提供方承担部分责任的情况下。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

不可抗力因素：如算法受到外部攻击、数据丢失等不可预见的技术风险或自然灾害影响，企业可以主张免责。

三、合理抗辩与免责空间

在面对因算法自动决策引起的合同违约时，企业可能通过以下几种抗辩理由争取免责或减轻责任：

1.合同中的免责条款

许多服务贸易合同中会设置免责条款，特别是对于技术问题、不可抗力事件等情况。如果企业能够证明算法故障是由于这些免责条款规定的原因导致的，企业可能不需要承担违约责任。

2.技术问题的不可避免性

企业可以主张算法故障属于技术问题的不可避免性，尤其在算法的复杂性和外部环境的不确定性较高时，法院或仲裁机构可能会考虑到技术的不确定性，给予一定的宽容度。

3.第三方责任追索

如果合同明确规定第三方技术提供商或算法开发商需承担技术故障的责任，企业可向第三方追索，减轻其在违约责任中的承担。

4.数据问题

如果算法错误是由于输入数据不准确或不完整导致的，且企业已尽到合理的审查义务，企业可以主张数据问题是导致算法错误的根本原因，减轻责任。

Q62

如何合规处理自动决策对用户权益的影响？（撰写人：傅颉）

答：

一、核心提要

1.“透明告知—异议权—人工复核”是APEC区域自动决策合规的三大核心要素：无论各经济体立法路径如何分化，对自动决策的用户权利保护基本围绕这三个维度展开，且这一逻辑已从软法指南逐步向具有约束力的法律义务演变。

2.中国PIPL已确立APEC区域内非常具有操作性的自动决策合规框架：对于通过自动决策手段作出的对数据主体权益有重大影响的决定，个人有权要求个人信息处理者予以说明，并有权拒绝仅由自动决策作出的决定。Bird & Bird这一"拒绝权"是目前APEC区域内极具代表性的强制性规定。

3.合规的难点不在于"是否告知"，而在于"如何有效告知"：监管机构和法院越来越强调，合规的说明义务要求提供"有意义的解释"——既非简单披露算法存在，亦非完整暴露商业机密，需要在用户可理解性与商业利益之间寻找合理边界。

二、法规矩阵与专业洞察

1.主要APEC经济体自动决策保护对比

经济体	核心法律依据	告知义务	说明/解释权	拒绝/人工复核权	影响评估(AIA/PIPIA)
中国	PIPL 第24条	✓强制（显著方式）	✓强制（重大影响时）	✓强制（拒绝权）	✓强制（至少每年一次）
韩国	《AI基本法》(2026)	✓强制（高影响力AI）	✓ 强制	✓ 强制（异议处理）	✓ 高风险AI强制要求
新加坡	PDPA + MAS指引	✓建议披露	✓ 行业强要求（金融）	⚠鼓励人工干预	⚠ 建议风险评估
澳大利亚	隐私法修订草案	✓强制（算法透明度）	⚠视行业而定	⚠无通用强制	高风险领域强制
美国(加州)	CCPA/CPRA	✓强制（退出权通知）	✓ 强制（逻辑披露）	✓ 强制（退出权）	✓ 定期风险评估

2. APEC区域自动决策合规的核心用户权益体系

自动决策（Automated Decision-Making，ADM）是指无须人工介入、由算法或AI系统直接作出影响用户权益的判断。其对用户权益影响的核心合规维度可归纳为以下四类：

（1）知情权与透明告知义务

根据算法推荐规定，服务提供者必须披露算法正在被使用，并允许用户选择退出算法推荐。这些规定强调了确保公平和透明的基本要求；禁止服务提供者在算法推荐的情形下，基于用户个人特征向用户提供不同的价格或对用户进行歧视。

（2）说明解释权

对于通过自动决策手段（例如基于客观标准的筛选程序）对数据主体权益有重大影响的决定，数据主体有权要求个人信息处理者就其决定作出说明。

（3）拒绝权（人工复核权）

数据主体有权拒绝仅基于自动决策作出的结论，并要求转由人工审核。个人有权拒绝仅通过自动决策方式作出的决定，个人信息处理者须提供对自动决策结果的投诉渠道，并支持对结果的人工复核。

（4）算法影响评估义务

依据《个人信息保护法》第55条，使用个人信息进行自动决策的主体应当：（一）开展个人信息保护影响评估（PIPIA），根据评估结果采取有效保护措施并记录处理活动；（二）在算法使用期间定期（至少每年一次）开展影响评估，并根据结果改进保护措施；（三）提供针对自动决策结果的投诉渠道，支持对结果进行人工复核。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

3. 自动决策合规流程图



4.实务案例

澳大利亚“机器人追债”（Robodebt）事件的2025年余波： 该案因完全依赖自动化算法计算债务且缺乏人工复核，最终导致澳政府支付巨额赔偿。此案例直接推动了2025年APEC各经济体在制定AI规则时，均强调了“必须保留有效的人为干预”（Meaningful Human Intervention）作为法律底线。

三、行动清单

□ 梳理客户系统，识别涉及信贷评分、招聘筛选、保险定价等“重大影响”类自动决策场景。

□ 在用户隐私政策中设立“自动决策说明”专栏，确保告知位置“显著”且语言“通俗”。

□ 建立内部“异议处理标准流程”，确保用户提出人工复核请求后，能在法定时限内（如30日）得到人类专员的实质性答复。

□ 针对中国境内业务，每年定期开展PIPIA评估，并保留至少三年的审计记录备查。

□ 关注韩国《AI基本法》于2026年1月生效后对"高影响力AI"系统的具体合规要求，评估客户AI系统是否落入该定义，并据此启动披露义务及影响评估准备工作针对韩国业务、。

□ 在合同中明确第三方算法服务商在提供说明义务时的协助责任及费用分担。

Q63

哪些行业的算法监管相对严格（如金融、就业）？ （撰写人：傅颉）

答：

一、核心提要

1. 金融行业是APEC区域算法监管最为严格、最为成熟的领域：无论是中国、新加坡、澳大利亚还是韩国，金融监管机构均已针对AI和算法决策颁布专项规则或指引，且普遍倾向于将算法信贷评分、自动交易系统纳入强约束范畴，金融业算法监管已从"软法自律"走向"强制问责"。

2. 就业/劳工领域的算法监管正从空白走向有组织推进：算法管理工具的普及率在美国企业中高达90%，欧洲国家约为79%，日本约为40%。APEC区域多个经济体已开始通过劳动立法、数据保护法律及行业监管规则将算法雇主的用工行为纳入规制，但整体仍处于立法探索期。

3. "高风险"是触发严格算法监管的核心判断标准：信贷拒绝、医疗诊断建议、刑事司法辅助等场景因对个人基本权益影响重大，已在多个APEC经济体形成最严格的算法合规要求，律师应重点关注这些"高风险场景叠加区域"的合规义务。

二、法规矩阵与专业洞察

1. 行业算法监管严格程度对比矩阵

行业	核心监管关切	典型监管措施	核心依据
金融/信贷	算法歧视、信贷公平、系统性风险。	强制指引+透明度审查	新加坡MAS AIRG、中国征信办法
医疗/制药	诊断准确性、患者生命安全、问责制。	准入制+三类医疗器械审查	2026年起越南DTI法、各药监局规范
就业/招聘	招录偏见、隐私侵权、自动考核合理性。	数据保护评估+公平性测试	韩国AI基本法(2026)、美国加州新规
平台经济	价格歧视（杀熟）、派单算法压力。	强制备案+用户退出权	中国《算法推荐管理规定》
基础设施	系统的鲁棒性、抗攻击能力。	安全等级保护+算法容灾要求	越南、泰国网络安全法规

2025-2026年的一大趋势是“特定行业算法备案”。中国、韩国及新加坡（针对金融业）均已要求或拟要求企业在部署涉及核心利益的算法前，必须向监管机构提交关于数据来源、权重逻辑及风险对冲方案的说明。

2. 就业/劳工领域：从算法管理到监管规制的转变

就业领域的算法监管在APEC区域正处于立法加速期，核心议题集中于算法招聘（AI Hiring）、算法劳动管理（Algorithmic Management）和平台工人权益保护三个方面。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

算法管理带来的对自主权和尊严的威胁尤为突出，这些做法涉及使用自动化系统替代管理者通常执行的功能，如分配任务、确定工作时间表、下达指令、监控和评估工人，以及提供激励或施加处罚。算法管理可能过于侵入性，可能限制工人自主权并减少人际互动机会，对工作条件和平等待遇等方面产生重要影响。

在韩国，《劳动标准法》规定，韩国雇主在以对雇员不利的方式（即导致工作条件恶化）更改就业规则时，须获得工人（如有工会，则须获得工会；如无工会，则须获得多数工人）的同意。

3. 金融业算法监管的典型细分场景

（1）算法信贷评分

算法信贷评分是金融业算法监管最核心的战场。全球金融机构面临的信息明确：无论AI系统技术上多么复杂，算法决策系统都必须是透明的、公平的、可问责的。在APEC区域，中国PIPL要求信贷自动决策须提供说明；澳大利亚ASIC基于现行消费者保护法对算法信贷系统施加合规要求；新加坡MAS FEAT原则则对信贷AI系统的公平性、可解释性设定了明确预期。

（2）算法交易系统

算法高频交易因其对市场稳定性的潜在系统性影响，受到各经济体金融监管机构的高度关注，普遍要求AI交易系统具备可审计性、风险熔断机制及监管报告义务。

4. 实务案例

2025年新加坡金融管理局（MAS）AI风险指引落地：MAS于2025年11月发布的指引，首次明确了金融机构使用AI的“分层问责制”。该指引要求银行在利用算法进行信用卡审批时，必须对算法的“偏见因子”进行年度审计，并向监管机构提交公平性证明报告。这标志着APEC区域金融算法正式进入“全生命周期监管”时代。

三、行动清单

□ 核查客户主营业务是否落入金融、医疗、就业或平台运营等“高风险算法监管清单”。

□ 平台类客户应重点排查派单或价格算法，确保已在产品显著位置提供“关闭个性化推送/定价”的开关。

□ 就业服务类AI，需建立“防歧视测试记录库”，保留对性别、年龄、族群等敏感因子的脱敏处理证据。

□ 跨APEC展业的企业，建议建立“最高标准合规库”，优先对标中国及韩国的算法备案及披露要求。

□ 参加所在地监管机构组织的“算法沙盒”，在正式强制规定出台前获取合规豁免或合规辅导。

Q64

在何种情况下，算法模型需要定期审计？（撰写人：范晓荧）

答：

一、核心提要

1.高风险应用场景：当算法应用于医疗、金融、招聘、信用评估等直接影响个人重大权益（生命健康、财产安全、就业机会）的领域时，需建立定期审计机制以确保公平性与非歧视性。

2.生命周期重大更新：算法模型发生版本迭代、底层逻辑变更或训练数据集构成发生显著变化时，必须启动专项审计，以验证变更后的合规性与稳定性。

3.法律与合规要求：欧盟《人工智能法案》、美国《算法责任法案》及中国拟议框架均明确要求高风险AI系统进行定期审计。

二、法规矩阵与专业洞察

国家	核心法律依据	审计触发机制	风险分级机制	审计频率要求	特殊领域规定
中国	《互联网信息服务算法推荐管理规定》《生成式人工智能服务管理暂行办法》	– 高风险应用定期审计 – 上线前、重大变更	四级：数据/内容/模型/网络安全	年度+变更触发	医疗领域明确“AI辅助，人类决策”
新加坡	《个人数据保护法》(PDPA) 《生成式人工智能模型治理框架》(GenAI MGF)草案	场景化触发： – 部署阶段持续监测 采购阶段数据义务	三阶段：开发测试/部署/采购阶段	持续监测	数据不得用于生成式AI训练，个人数据保护优先
韩国	《AI基本法》(2024年通过)下位法令(2025年制定)	生命周期触发： –高影响AI领域(10个) – 版本迭代	高影响AI十领域	动态评估	建立AI安全认证制度
日本	《Ai企业指南》(2024年4月) 《AI促进法》(2025年6月)	多模态触发： – 重点监测生成式AI风险 – 企业自主强化风险对策	聚焦文本、图像、动画风险	年度更新《AI企业指南》	著作权保护专项文件
澳大利亚	《政府负责任使用人工智能政策》(2024年9月)	透明度触发： – AI透明度声明 – 持续监控	三支柱： 准备/使用/完善	定期更新透明度声明	公共服务适用（除国防），鼓励公司制实体采用
越南	《人工智能法》(2026年3月生效)	风险导向触发： – 高风险系统合规评估 – 事故披露	后果导向风险分类	动态调整	本土化取向

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

国家	核心法律依据	审计触发机制	风险分级机制	审计频率要求	特殊领域规定
马来西亚	《国家人工智能办公室》(NAIO)框架、《个人数据保护法》(Personal Data Protection Act, PDPA 2010)、以及《网络安全法》(Cybersecurity Act)	三位一体触发: – 网络安全/数据流动/AI创新	建立分层监管体系，区分风险等级精准施策	灵活机制: – 豁免条款吸引科技投资	禁止歧视性数字服务税
美国	《人工智能权利法案蓝图》(Blueprint for an AI Bill of Rights)《联邦算法问责法案》提案	风险事件触发、高风险领域部署前进行影响评估	多层级风险评估：基于系统影响程度划分高风险与低风险应用	定期 +事件驱动	禁止社会评分，限制执法面部识别
欧盟	《人工智能法案》(AI Act, 2024年通过)《通用数据保护条例》(GDPR)	合规性触发: – 高风险AI系统上市前合规评估 – 重大更新重新认证	四级：不可接受/高/有限/最小风险	定期 +动态审计	公共场所实时远程生物识别、限制情感识别在职场和教育中的使用

三、行动清单

□建立高风险清单：识别金融、医疗、招聘、公共舆论等高风险算法，集中审计资源。

□检查模型更新：定期核查数据源更换、逻辑调整或版本迭代，触发专项审计。

□年度内部审计：设立年度安全评估作为强制节点，符合《算法推荐管理规定》等要求。

□规范变更流程：明确上线、迭代、数据变更的审计触发规则，未经审计不得上线。

□准备备案材料：提前完成自评估、安全监测和备案文件，确保可直接报送监管。

□引入第三方审计：公共利益或复杂模型聘请独立机构，保证客观、公正、透明。

□公开披露结果：在合规与保密前提下适度公开，提升社会信任。

□制定风险分级：建立分级体系，明确不同风险等级的审计频率与深度。

□跨境数据合规：确保跨境传输符合国际规则与本地法律，保持透明。

□应急审计机制：针对争议、投诉或事故，快速启动计划外审计。

Q65

企业使用第三方算法需要承担哪些合规义务？（撰写人：范晓荧）

答：

一、核心提要

责任不因外包而豁免：无论算法是自研还是第三方提供，企业作为面向用户的服务提供者，需承担首要合规责任。

核心义务全景：企业使用第三方算法时需要建立不同维度下合规义务全景，涵盖行政准入与备案、供应链尽职调查、数据跨境与隐私保护、内容安全与标识、透明度与用户权益等核心合规义务维度。

双层合规机制：企业需要建立以全球通用框架（如 GDPR、OECD AI原则）为基线，叠加本地法律要求（如中国备案制度、美国州级隐私法、新加坡 PDPA）。

二、法规矩阵与专业洞察

合规义务	中国 (CN)	欧盟 (EU)	美国 (US)	新加坡 (SG)	马来西亚 (MY)
准入与备案	强制双重备案：算法备案、大模型登记	高风险合规评估：需进行基本权利影响评估	州级偏见审计、治理框架评估	部署阶段需持续监测，采购阶段需履行数据中介义务	分层监管体系，部分高风险应用需额外审批
供应链责任	连带责任：上游未备案，下游应用违规	透明度传导：供应商需提供技术文档	合同约束：FTC倾向追究最终服务提供者	要求服务提供商履行数据保护义务	三位一体责任：网络安全、数据保护、AI创新并行
数据与跨境	本地化与安全评估：跨境传输需审批	数据处理协议：禁止未经授权训练	用户退出权：允许拒绝画像与广告	禁止个人数据用于生成式AI训练，跨境传输需合规	跨境数据流动需合规，禁止歧视性数字服务税
标识义务	双重标识：显式“AI生成”+隐式元数据	机器可读标识：元数据强制嵌入	行业标准：C2PA，自愿性为主，广告领域严格	鼓励透明度披露，尚无强制标识	鼓励透明度声明，部分领域需公开说明
透明度与用户权益	披露算法逻辑与用途，提供拒绝推荐选项	强调基本权利保护与透明度	用户知情权、反歧视权、退出权	用户隐私优先，强调数据保护与透明度	鼓励企业发布透明度声明，保障用户权益

不同法域对第三方算法的监管重点各有差异：中国强调行政许可与内容安全；欧盟侧重风险分级与基本权利；美国则聚焦数据隐私与反歧视，州级法规差异大；新加坡突出数据保护与中介义务；马来西亚采取分层监管与灵活机制，强调跨境数据合规。企业必须建立全球基线（GDPR/OECD原则）+ 本地补充措施 的双层合规机制，明确使用第三方算法时需要承担的合规义务，降低多法域环境中的合规风险。

更多免费行业报告 并购家 www.ipoipo.net

三、行动清单

□ 备案与准入核查：确认调用的第三方算法或大模型已完成必要的备案或登记，确保“无资质不调用”

□ 供应链尽职调查与合同约束：审查第三方供应商的资质、合规性与知识产权授权链条，签署标准合同条款，明确数据保护义务、责任划分及违约赔偿机制。

□ 建立跨境数据传输审查与隐私影响评估制度：若涉及跨境传输，履行安全评估。

□ 内容安全与溯源标识：建立多语言内容过滤与人工干预机制，落实全球通用的显式提示（如“AI Generated”）与符合C2PA等国际标准的隐式标识，防止虚假信息传播与公众混淆。

□ 签署标准合同条款：明确责任划分与赔偿条款

□ 透明度披露与用户权益：在显著位置披露算法基本原理与用途，保障用户知情权，并提供关闭个性化推荐或退出算法画像的便捷选项。

□ 应急机制与动态审计：建立算法安全事件应急预案，在发生歧视、偏见或重大事故时，立即启动专项审计、阻断风险并向监管部门报告。

□ 本地化合规落地：在全球基线（如OECD原则）基础上，针对运营所在国（如美国州级隐私法、新加坡PDPA）叠加特定的本地法律合规措施。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

亚太数字经济与人工智能法律问答指南(蓝皮书)
Asia-Pacific Digital Economy and Artificial Intelligence Legal Q&A Guide (Blue Book)



作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q66

APEC经济体在推动数字贸易发展的过程中通常强调哪些原则性共识？（撰写人：沈晓雪）

答：

一、核心提要

数据跨境流动与隐私保护的平衡：APEC经济体普遍认同在保障有效的数据隐私保护前提下，应最大限度促进数据跨境自由流动。APEC跨境隐私规则（CBPR）体系成为区域内协调隐私保护标准与数据流动诉求的核心机制，反对不合理的数据本地化要求。

透明度、可预测性与监管一致性：各经济体致力于构建对企业（特别是中小微企业）友好的监管生态系统。强调国内数字贸易法律法规的透明度和可预测性，倡导在电子认证、电子签名、电子发票等领域实现监管框架的互操作性与技术标准的互认。

无纸化贸易与包容性增长：推动贸易便利化是APEC的核心共识之一，重点通过海关程序数字化和无纸化贸易降低交易成本。同时，APEC强调数字经济的包容性，致力于提升中小微企业（MSMEs）参与全球数字价值链的能力，并加强在线消费者权益保护。

二、法规矩阵与专业洞察

APEC经济体在数字贸易领域的原则性共识并非单一的强制性条约，而是通过一系列框架性文件、路线图和自愿性机制逐步确立的软法（Soft Law）体系。这些共识不仅反映了区域内主要经济体（如美国、日本、新加坡等）的政策导向，也深刻影响着CPTPP、DEPA等高标准数字贸易协定的规则重塑。

APEC数字贸易核心规则矩阵与经济体实践对比

下表梳理了APEC框架下数字贸易核心原则的法律渊源，并对比了部分主流APEC成员经济体在转化这些原则时的国内法实践差异：

核心原则	APEC框架文件依据	主流经济体实践对比(美国vs.新加坡vs.日本)
数据跨境自由流动	《APEC跨境电子商务便利化框架》(2017)；《APEC互联网与数字经济路线图》(2017)	美国：极力主张数据自由流动，反对数据本地化，主导推动全球CBPR论坛。新加坡：通过DEPA等协定积极推动数据自由流动，国内PDPA允许向具备同等保护水平的管辖区传输数据。日本：提出“基于信任的数据自由流动”（DFFT）倡议，国内法要求跨境传输需获得同意或接收方具备相当保护标准。
隐私与个人信息保护	《APEC隐私框架》(2015修订)；APEC CBPR体系及PRP系统	美国：依赖部门法和州法（如CCPA/CPRA），缺乏统一联邦隐私法，但积极推行CBPR认证。新加坡：拥有完善的个人数据保护法（PDPA），深度参与并认可CBPR作为合规跨境传输机制。日本：个人信息保护法（APPI）严格，已获得欧盟充分性认定，同时也是CBPR的积极参与国。
无纸化贸易与电子认证	《APEC无纸化贸易能力建设行动计划》；《APEC地区电子发票系统互操作性原则》(2023)	美国：拥有《全球和国家商业电子签名法》(E-SIGN)，全面认可电子签名效力。新加坡：《电子交易法》(ETA)采用UNCITRAL模型，率先推进电子提单（eBL）等可转让电子记录的法律认可。日本：通过《电子签名法》及近年来的数字化转型法案，逐步废除书面印章要求。
在线消费者保护	《APEC跨境电子商务便利化框架》(2017)	三国均拥有成熟的消费者保护法律体系，重点打击网络欺诈、虚假宣传，并逐步加强对算法推荐和暗黑模式的监管。

专业洞察：合规路径与实务挑战

从涉外法律实务的角度来看，APEC数字贸易原则性共识为跨国企业提供了一个“以合规促流动”的宏观指引。尽管APEC规则本身不具备直接的国内法强制执行力，但其衍生的CBPR体系已成为企业证明其数据跨境合规性的重要抓手。

对于在亚太地区布局数字业务的跨国企业而言，最大的挑战在于监管碎片化。虽然APEC倡导互操作性，但各经济体在数据本地化、重要数据出境安全评估、个人信息跨境标准合同等方面的国内立法仍存在显著差异。企业在设计全球数据合规架构时，不能仅依赖APEC的软法共识，而必须进行“双层合规”：一层是满足目标市场（如中国、美国、东盟国家）的硬性法律要求；另一层是利用APEC CBPR等区域性认证机制，降低跨司法管辖区的数据合规摩擦成本。

三、行动清单

针对计划或正在APEC区域内开展跨境数字贸易、数据交互的企业，建议企业法务及合规团队参照以下清单进行自查与行动部署：

□数据资产盘点与分级分类：是否已全面盘点企业在APEC区域内收集、处理和跨境传输的数据资产，并依法进行了个人信息、重要数据、核心数据的分级分类?

□跨境传输合规机制审查：针对向不同APEC经济体的数据出境活动，是否已依法采取了适当的合规路径（如：安全评估、标准合同SCC、单独同意，或探讨引入CBPR认证体系）？

□隐私政策与透明度更新：企业的全球及区域隐私政策（Privacy Notice）是否清晰、准确地披露了数据跨境流动的目的、接收方及用户权利，符合APEC隐私框架及当地法律要求?

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

□ 电子交易法律效力评估：在开展跨境B2B或B2C业务时，所采用的电子合同、电子签名、电子发票系统是否符合目标市场的国内法（如电子交易法）要求，确保具备强制执行力?

□ 消费者权益保护机制合规：面向消费者的在线交易平台（App/Web），其退换货政策、争议解决机制、营销信息推送（防范非应邀电子信息）是否符合当地消费者保护法规?

□ 监管动态监测与响应预案：是否已建立常态化的法律监测机制，跟踪APEC主要经济体（特别是业务重心所在国）在人工智能监管、反垄断及数据本地化方面的最新立法动态?

Q67

APEC各经济体对电子合同与电子签名的法律效力如何认定？存在哪些差异?

（撰写人：傅哲迅）

答：

一、核心提要

1.识别法域模式：APEC区域内电子签名效力并非“一刀切”。出海企业在签署跨境商业合同时，必须首先识别目标国/地区的法律模式（技术中立型、指令型或混合型），避免用一套电子签约系统“打天下”。

2.技术保障：在马来西亚（指令型）或中国（混合型）等地，仅有“签署意图”不足以在涉外诉讼中提供强有力的证据支撑。对于核心商事合同，建议要求采用基于非对称加密系统且由持牌CA机构认证的“可靠/数字电子签名”。

3.注意电子签名适用的例外：无论技术多么先进，各经济体均存在法定适用例外。涉及授权委托书、流通票据、遗嘱信托、不动产及特定人身关系的文书，必须严格遵循传统的“纸质+手写/物理签章”模式。

二、法规矩阵

序号	法律模式	代表国家	核心法规	核心生效要件	适用例外
1	技术中立型（最宽松）	美国	1.联邦层面：《全球及全国商业电子签名法》（ESIGN ACT）； 2.各州层面：《统一电子交易法》（UETA）	1. 签署意图 (ESIGN 15 USC §7006.(5))； 2. 双方同意 (UETA §5(b))；消费者需电子方式肯定性同意 (ESIGN 15 USC § 7001.(c)(1)(A))； 3.记录留存与获取 (ESIGN 15 USC § 7001.(d)(1))	遗嘱与信托、离婚、收养、法院命令/诉讼文件、特定消费者通知等 (ESIGN 15 USC § 7003.(a)(b))
2	指令型（最严格）	马来西亚	1.《电子商务法》(ECA 2006)； 2.《数字签名法》(DSA 1997)	1.识别身份与批准意图 (ECA Section 9(1)(b))； 2.技术手段绝对可靠 (ECA Section 9(1)(c), DSA Section 2，强制非对称加密)； 3.逻辑关联 (ECA Section 9(1)(a))； 4.双方同意(ECA Section 3(1)(2))	授权委托书、遗嘱与信托的设立、流通票据 (ECA Schedule Section 2)
3	混合型（折中平衡）	中国	《中华人民共和国电子签名法》	1.双方同意/约定使用 (《电子签名法》第三条第一款)； 2.技术可靠(《电子签名法》第十三条：专有、控制、防篡改)	涉及婚姻、收养、继承等人身关系；涉及停止供水/热/气等公共事业服务；以及法律、行政法规规定的不适用电子文书的其他情形 (《电子签名法》第三条第三款)

三、专业洞察

通过上述表格可以看出，APEC各经济体虽然普遍承认了电子签名的基础效力，但在“证明标准”上存在巨大鸿沟。美国等技术中立国家将举证重点放在“当事人意图”的重构上；而马来西亚和中国则通过法律将举证责任转移给了“底层技术”（如非对称加密和CA认证）。

结论：在跨境商事交易中，“有效”并不等同于“好用”。企业在涉外缔约时，不能采取“就低不就高”的策略。为了确保合同在任何法庭或仲裁庭都能获得最高级别的证据采信，建议出海企业统一采用符合混合型/指令型高标准的“可靠数字签名”，并在合同前端明确加入“同意使用电子交易”的管辖条款。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q68

数字产品（如软件）以及数据交付服务，在不同经济体下通常享有哪些关税及税收优惠政策？（撰写人：韦征）

答：

一、核心提要

在APEC框架下，数字产品与服务的税收环境呈现出“关税趋同，境内税分化”的鲜明特征。跨境电子传输长期享受零关税待遇；但WTO自1998年实施的电子传输免关税暂停机制已于2026年3月第14届部长级会议（MC14）到期且未获延续，各成员已具备对电子传输征收关税的法律基础，"零关税"不再是稳固的国际惯例。然而，各成员经济体在境内税收（主要包括增值税和企业所得税）方面则通过多样化的优惠政策进行竞争，以吸引数字产业投资。同时，业务的法律定性（特别是区分“营业利润”与“特许权使用费”）将直接导致显著的税负差异，是企业税务筹划的关键。

二、法规矩阵与专业洞察

本部分从关税、境内税及收入性质判定三个维度，系统梳理APEC地区的核心税收规则。

1. 关税政策矩阵：电子传输的“零关税”共识

政策框架	核心内容	主要适用范围/案例
WTO电子传输免关税暂停令	各成员方一致同意不对电子传输征收关税。该暂停令需定期延期，最新已延期至2026年WTO第14届部长级会议前。该暂停机制已于2026年3月WTO第14届部长级会议（MC14）到期且未获延续，各成员已可自主决定是否对电子传输征收关税。	APEC所有WTO成员经济体（如中、美、新、泰等）均遵守此惯例。
区域贸易协定强化条款输	CPTPP：明确规定不得对电子传（包括内容）征收关税。 RCEP：包含不对电子传输征收关税的条款。 DEPA：进一步优化数字产品的非歧视待遇。	为成员间的数字贸易提供了超越WTO的多边制度保障。
物理介质与电子传输的区别	海关依《关税及贸易总协定》（GATT 1994）第二条关税减让表，对物理载体本身（如HS 8523类）征收关税，不对其中蕴含的数据价值征税。	《海关估价协议》仅解决完税价格的确定问题，并非征税依据；纯电子传输（比特流）不经过关境，不涉及海关估价与关税。

2.境内税收优惠政策矩阵

税种	优惠政策	主要适用经济体与条件
企业所得税	“税收假期”与低税率	泰国（BOI）：软件开发、云服务、AI等领域，可获5-8年免征所得税。 越南：软件外包、新数字产品研发可享“四免九减半”。 新加坡：符合条件的知识产权收入可适用5%或10%的优惠税率。 中国：国家鼓励的重点软件企业税率可低至10%，高新技术企业为15%。
增值税	出口零税率	绝大多数APEC经济体（如新、泰、越、中）规定，向境外实体提供并在境外消费的数字服务，适用增值税0%税率，并可退还进项税。
研发激励	加计扣除/税收抵免	澳大利亚：提供研发税收激励，可抵免税款或获得现金退还。 美国：提供联邦研发税收抵免。

3. 数据交付服务的性质判定与税务影响

收入性质	判定标准	税务后果
特许权使用费	交付涉及受版权保护的算法、专有技术或专有数据库的访问许可。	来源国通常按双边税收协定的协定税率（常见10%-15%，具体视协定而定）征收预提所得税。
营业利润	提供纯数据处理、云存储或标准软件订阅（SaaS）服务。（含IaaS/PaaS/SaaS，客户通常仅获得操作使用权，不享有底层知识产权的处分权）	根据双边税收协定，在无常设机构的情况下，可申请在收入来源地免征预扣税。

VAT/GST的征收趋势转向B2C：虽然B2B数字服务出口普遍享受零税率，但向境外个人消费者（B2C）提供服务的境外平台，正面临在消费地注册并代征增值税的新义务（如泰国e-Service VAT规则）。

“高新”与“BOI”资格的税收价值：获取中国的“高新技术企业”或泰国的“BOI promoted”资格，不仅是荣誉，更是直接的所得税减免工具，能实质性地提升项目净利润。

合同定性的税负杠杆效应：一份合同被定性为“技术服务合同”还是“软件许可合同”，可能带来超过10%的利润差异。这要求法务与税务团队在合同起草阶段就协同作业。

三、行动清单

为有效利用APEC地区数字税收优惠政策并控制风险，建议企业采取以下行动：

1.优先进行“税务选址”与资格申请

规划投资架构：在向东南亚等地区拓展业务时，优先考虑在泰国、越南等提供“税收假期”的经济体设立研发与交付中心，并立即启动BOI或类似优惠资格的申请程序。

用足研发优惠：无论总部在何处，都应系统梳理并备案研发活动，积极申请中、澳、美等国的研发费用加计扣除或税收抵免。

2.优化合同架构与交易流程

实施合同分拆：在提供“软件许可+技术支持+数据服务”的一揽子解决方案时，应在法律和商业允许

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

的前提下，将不同性质的收入分拆至不同合同。确保技术服务部分在合同条款和实际履行中清晰独立，以主张其作为“营业利润”的税收待遇。

规范发票与流程：针对适用增值税零税率的出口服务，确保合同、发票和汇款流能明确证明服务提供给了境外实体并在境外消费，以满足税务局的举证要求。

3.动态管理跨境税务定性风险

进行事先裁定：在向印尼、越南等对SaaS定性存在不确定性的市场开展大规模业务前，可考虑向当地税务机关申请预先税收裁定，以锁定收入性质。

活用税收协定：当对方试图对付款征收预扣税时，及时提示其依据双边税收协定中关于“营业利润”的条款，并协助客户准备税务居民身份证明等材料，申请税收协定优惠。

关注CBPR体系：评估并参与APEC跨境隐私规则（CBPR）认证。虽然不直接节税，但能高效解决数据跨境合规问题，间接保障数据交付服务的商业可行性与利润空间。

Q69

跨境电商平台需承担哪些消费者保护义务?

（撰写人：牛誉翔）

答：

一、APEC 层面共识（非约束性、最佳实践）

APEC 以电子商务指导小组 ECSG、消费者保护公私对话 PPD、CBPR 隐私规则、ODR 在线争端解决框架为核心，形成一套自愿性、高标准、以平台为核心的消费者保护共识。

1. 信息披露义务（知情权）

平台须确保卖家真实、完整、准确披露：商品规格、成分、安全警示、原产地、价格（含税费 / 运费）、交付期、售后规则、卖家身份与联系方式。

禁止虚假宣传、隐藏费用、误导性标签；食品 / 美妆 / 母婴 / 电器等高风险品类需额外资质与警示信息。

2. 质量安全与合规义务

平台对入驻卖家实施资质审核 + 产品合规审核（认证、标准、标签）。

建立不合格 / 侵权商品下架、召回、追溯机制；对假货、不安全产品、侵权品采取删除 / 屏蔽 / 终止服务，并可追究连带责任。

遵守目的地经济体强制性标准（如食品农残、电器安全、儿童用品）。

3. 公平交易与合同规范

提供清晰易懂的格式合同，不得含不公平条款（单方面免责、不合理违约金、限制维权）。

明确约定合理的退换货规则、运费承担、拒收 / 拒付后果。

禁止价格欺诈、捆绑销售、强制搭售、恶意刷单。

4. 支付安全与资金保障

提供安全、可追溯、可退款的支付通道；保障交易数据与支付信息安全。

鼓励设立消费者保证金 / 先行赔付基金；平台在特定情形下承担先行赔付责任。

5. 个人信息与数据保护（CBPR 核心）

遵循APEC 隐私框架九原则 + CBPR 跨境隐私规则：防止损害、告知、收集限制、个人信息的利用、选择、信息完整性、安全保障、访问与更正、问责。

跨境数据流动需获得同意、具备合法 basis、采取安全措施、可追溯。

平台对卖家数据处理行为审核 + 监督 + 追责。

6. 争议解决与救济（ODR 核心）

建议平台提供免费、便捷、高效的争端解决机制，如：全天候（≥99% 可用）的在线争端解决 ODR 渠道；消费者免费提交，费用由违规卖家承担。

建议建立7×24 小时投诉响应、限时处理（如 7　15 日）、透明处理流程、可上诉至监管 / 第三方。

平台协助消费者维权、提供交易证据、配合调查；对恶意拖延、拒不配合的卖家采取处罚。

7. 平台责任与连带责任

平台对明知 / 应知卖家侵权、售假、欺诈而未采取措施的，承担连带责任。

建立卖家信用评级 + 黑名单 + 公示；对严重违规卖家永久封禁。

二、主要经济体跨境电商平台义务要点

1. 中国（最严先行赔付 + 连带责任）

先行赔付：消费者可直接要求平台退款；平台赔付后可向卖家追偿。

资质审核 + 实名登记：卖家营业执照、ICP、食品经营许可等；禁售无资质商品。

七天无理由退货（跨境普遍适用）；质量问题退货运费由平台 / 卖家承担。

数据合规：个人信息境内存储为主；跨境数据需安全评估 / 认证或其他法定路径。

侵权连带责任：平台未及时处理侵权投诉的，连带赔偿。

2. 美国（市场导向 + 透明披露 + 隐私保护）

FTC 法案：禁止虚假宣传、价格欺诈、误导性标识；全额披露税费 / 运费 / 退换货成本（如需）。

平台责任：一般不承担卖家责任，但明知欺诈而协助则追责。

隐私保护：州法为主，如加州的《加州消费者隐私法案》及其修正案《加州隐私权利法案》（CCPA, as amended by CPRA）；数据最小化、用户访问 / 删除权、数据泄露通知。

争议解决：鼓励ODR + 小额诉讼；平台提供证据、协助调解。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

3. 日本（全球最严合规 + 零容忍 + 日文全披露）

事前审查 + 全过程监管 + 零容忍：平台应根据当地法律要求审核PSE/PSC/SG 认证、日文标签、成分表、安全警示。

全日文披露：商品说明、规格、警示、售后、客服必须日文。

召回义务：发现不安全商品立即下架 + 强制召回 + 通报全行业；违规可刑事处罚 + 高额罚款 + 平台封禁。

隐私：《个人信息保护法》+CBPR 认证；严格跨境数据管控。

4. 韩国（国内代理人 + 详细披露 + 严监管）

境内代理人强制：境外平台必须指定韩国国内代理人处理投诉 / 纠纷；代理人承担相应责任。

超详细披露：真伪鉴定、使用风险、售后网点、客服电话、退换货流程强制展示。

七天无理由 + 质量问题无条件退换；平台先行赔付 + 保证金制度。

数据：《个人信息保护法》+CBPR；跨境数据需用户明确同意。

5. 澳大利亚（强隐私 + 安全标准 + 公平合同）

ACCC 监管：禁止虚假宣传、不公平合同条款、误导性行为。

隐私保护：定义较为广泛（任何个人信息 / 评论）；用户访问 / 更正 / 删除权、数据泄露强制通知。

安全标准：电器 / 玩具 / 母婴等强制认证 + 标签；平台审核 + 抽检 + 下架。

争议解决：免费 ODR + 小额仲裁；平台协助取证 + 先行赔付。

6. 东盟代表（新加坡 / 菲律宾）

新加坡：数据保护法 PDPA+CBPR；严格知情同意 + 数据安全 + 跨境控制；平台资质审核 + 侵权下架 + 争议调解。

菲律宾：平台强制下架非法商品 + 连带责任；全信息披露（价格 / 认证 / 联系方式）；建立消费者补救系统 + 安全支付 + 数据保护。

Q70

平台在内容管理上需承担哪些合规义务？（撰写人：牛誉翔）

答：

一、基础合规与透明义务（APEC 核心框架要求）

1.规则公示与本地化适配

公开清晰、可获取的内容管理规则、禁发清单、审核标准与处罚机制，建议采取多语言版本透明可查。

适配各经济体法律（如中国《电子商务法》、东盟各国广告法、隐私法），禁止一刀切，针对不同市场调整内容标准。

2.资质与入驻审核

核验商家主体资质、品牌授权、进出口许可、检验检疫证明等，源头过滤不合规主体。

对高风险品类（食品、美妆、医疗器械、药品）实施前置审查 + 动态复核。

二、商品信息内容合规（真实、准确、不误导）

1.信息真实与禁止虚假宣传

商品标题、描述、图片、视频、规格、成分、产地、价格、售后等必须真实一致，严禁夸大功效、虚构认证、伪造产地、对比贬低竞品。

广告内容符合 APEC《跨境电商便利化框架》与各经济体广告合规（如禁止医疗虚假宣传、美妆功效夸大）。

2.标签标识与多语言合规

商品标签、说明书符合目的地国语言与标准（如中文标签、东盟多语言标识），含成分、使用方法、警示、进口商信息等。

跨境信息披露需双语 / 多语对照，关键信息（价格、税费、退换货）清晰无歧义。

3.AI 生成内容合规（2025–2026 重点）

根据各成员国现行法律规定，对AI 图文、视频、文案进行标注“AI 生成”，避免误导消费者。

确保 AI 内容不侵犯版权、肖像权，训练数据合法合规。

三、知识产权（IP）内容保护（APEC IPEG 重点）

1.事前预防与审查

建立IP 数据库（商标、专利、版权、外观），上架前筛查侵权关键词、图片、文案。

商家入驻签署IP 合规承诺，明确侵权责任。

通知 – 删除与快速处置

平台应设立便捷的侵权投诉受理通道，在收到符合法定要件的有效通知后，应依据各成员国相关法律

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

规范的时效要求（如：设立24 小时侵权投诉通道，受理权利方投诉后72 小时内下架 / 屏蔽侵权内容，留存记录）。

对重复侵权、恶意侵权商家实施限流、罚款、清退、黑名单并通报监管。

2.边境与跨境协作

配合 APEC 跨境 IP 执法协作，向各经济体海关 / 监管部门共享侵权线索，协助跨境查处。

四、数据隐私与个人信息保护（APEC CBPR 体系）

1.隐私政策公示与同意

显著位置公示符合APEC 跨境隐私规则（CBPR）以及各运营地法律规范的隐私政策，说明收集目的、范围、存储期限、共享对象、用户权利（访问 / 更正 / 删除）。

收集用户信息必须明示同意，禁止强制授权、捆绑收集。

2.数据安全与跨境传输

落实数据最小化、加密存储、访问权限管控、定期安全审计，防范泄露 / 篡改 / 滥用。

跨境数据传输遵循APEC CBPR + 目的地国规则（如中国《个人信息保护法》、东盟隐私指令），必要时申请跨境传输许可。

3.用户权利响应

平台应建立清晰的用户权利响应机制，支持用户查询、更正、删除个人信息、注销账户及撤回数据授权，于各运营市场法定期限内办结并反馈（如：30 日内办结并反馈）。

五、有害内容管控（安全、公序良俗、合规）

1.禁止违法违规内容

严禁政治敏感、恐怖、暴力、色情、赌博、毒品、邪教、歧视、仇恨、造谣、煽动违法等内容。

禁止非法商品（违禁品、假冒伪劣、走私、侵权、管制刀具、野生动植物）信息。

2.公序良俗与文化适配

尊重各经济体宗教、文化、习俗，禁止冒犯性、歧视性、低俗内容。

针对不同市场调整内容尺度（如东盟宗教禁忌点）。

3.评论与 UGC 管理

建议实时监控用户评论、私信、晒单、社群内容，过滤辱骂、诽谤、广告刷屏、恶意引流。

建立UGC 审核机制，对高风险评论人工复核，违规内容及时删除并封禁账号。

六、可追溯、留存与问责（APEC 监管协作要求）

1.内容全链路留存

记录内容发布、修改、审核、投诉、处置全流程日志，并按照当地法定期限进行留存（如：不少于3年（优先遵循属地法定留存年限，无明确法定的不少于3年）），供监管调取。

2.跨境协作与信息共享

配合 APEC 跨境电商监管合作机制，向各经济体监管部门提供内容数据、处置记录，协助调查取证。

3.平台责任与问责

明确平台内容审核、管控、处置、记录、报告责任，落实首问负责制。

对未尽审核义务、纵容侵权 / 违法内容的，承担责任并接受处罚。

七、APEC 特有义务（区别于普通平台）

遵循 APEC 非约束性指南：接受 APEC《跨境电商便利化框架》《CBPR 隐私规则》《IPEG 知识产权共识》指导，推动区域规则对齐。

参与能力建设与最佳实践共享：配合 APEC 开展合规培训、经验交流，协助中小微商家合规运营。

支持跨境纠纷调解：接入 APEC 跨境电商争议解决机制，协助处理内容相关跨境纠纷

Q71

APEC各经济体针对平台算法排序规则，分别设置了哪些强制披露规则？

（撰写人：韦征）

答：

一、核心提要

在APEC区域内，针对平台“算法透明度”的监管正从自律倡议全面转向强制性披露。2026年是多个主要经济体的新规生效与深度执行的关键窗口期，其核心要求聚焦于“算法排序”，旨在保障消费者的知情权与平台内经营者的公平交易权。各经济体的监管路径呈现差异化特征，但普遍不要求公开源代码，而是强调披露排序的“逻辑”与“因素”，并要求明确标识付费排名。

二、法规矩阵与专业洞察

本部分对各经济体的核心法规、披露对象、关键要求及法律性质进行矩阵化对比与解读。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体	核心法规/框架	主要披露对象	核心披露内容要点	法律性质与特点
中国	1.《互联网信息服务算法推荐管理规定》 2.《互联网平台价格行为规则》（2026.4生效）	全体用户 + 监管部门	1. 公开公示：算法基本原理、目的意图、主要运行机制、主要控制指标（Main Indices）及排序规则。 2. 价格算法：明确禁止“大数据杀熟”，要求披露价格形成逻辑。 3. 备案制：对特定平台实行算法备案，提交详细机制说明。	最细颗粒度、分类监管。兼具对消费者和商家的双重保障，并以备案制实现穿透式监管，强制性强。
日本	《提高特定数字平台透明度及公平性法案》（TFDPA）	商家（B2B）	1. 主要因素披露：指定大型平台（“特定数字平台”）须披露决定商品/服务显示顺序的主要因素（Main Factors）。 2. 权重理由：若广告费等商业因素权重高，需说明理由。 3. 变更通知：排序规则变更前需告知商家。	“共同规制”下的“定向透明”。主要针对头部平台，侧重保护平台内经营者免受不公正待遇。
韩国	《电子商务消费者保护法》及相关监管指南（由KFTC推进）	商家（B2B）	1. 合同必备条款：平台与商家的合同中必须列明“曝光顺位标准”（Exposure Ranking Criteria）。 2. 算法中立性：需披露是否存在“自我优待”逻辑，即是否优先展示自营产品。	以“公平契约”为核心的强制化。通过合同义务将披露要求固化，竞争法色彩浓厚，重点保护中小商家。
泰国	《数字平台服务业务运营王室法令》（DPS Decree）及补充通知（2025年7月生效）	监管部门 + 用户/商家	1. 年度报告：达到规模阈值的平台需向ETDA提交报告，简述算法运作。 2. 条款透明度：在服务条款中向用户及商家说明搜索结果排序机制，特别是付费推广逻辑。	基于风险的分级申报。结合行政许可与信息披露，是东南亚地区系统化平台监管的先驱。
澳大利亚	《2024年隐私及其他立法修正案》（2026年12月起强制执行）	个人用户	1. ADM披露：若自动化决策（ADM）影响个人权益（如个性化定价），必须在隐私政策中明确说明。 2. 算法说明权：个人有权要求平台说明其个人信息如何被用于自动化排序/决策。	隐私权驱动的披露。将算法透明度深度嵌入隐私保护框架，赋予个人事后知情与解释请求权。
新加坡	模型治理与AI治理相关框架	开发者 / 用户	倡导披露算法决策的说明性、数据使用逻辑等。	引导性、非强制。强调通过行业最佳实践和治理框架推动透明，是目前监管强度较低的代表。

商业秘密 vs. 披露义务的边界：当前各司法辖区均不要求披露核心源代码。合规披露的关键在于以“通俗语言”阐明排序的逻辑、主要因素及其相对权重，这要求法务与技术人员紧密协作，在不泄露技术秘密的前提下满足监管要求。

“付费排名”是监管雷区：几乎所有经济体都要求明确区分“付费广告”与“自然排名”。若广告费是影响排序的因素之一，必须在披露文档中明确指出，否则将面临“虚假宣传”或“不公平竞争”的指控。

三、行动清单

针对2026年的关键合规窗口期，为企业提供以下可操作的行动指引：

1.立即启动“算法审计”与文档检视：

目标：全面盘查涉及商品、服务、内容排序的所有算法模型。

产出：形成一份对标多国要求的《算法排序逻辑披露说明（内部版）》，明确可对外披露的“因素”与“逻辑”表述，并划定商业秘密红线。

2.重点应对2026年两大生效法域：

中国：确保在2026年4月《互联网平台价格行为规则》生效后，所有价格相关的算法逻辑（特别是动态定价）已按要求公示，并完成必要的备案手续。

澳大利亚：在2026年12月强制合规期前，修订隐私政策，增加对自动化决策（ADM）使用的明确描述，并建立内部流程以响应个人用户的“算法说明权”请求。

3.重构平台协议与商业实践：

对商家：在服务合同中嵌入符合当地要求的“曝光顺位标准”条款（特别是针对韩国、日本、泰国市场）。

对用户：在所有涉及排序的界面，清晰、醒目地标识“广告”、“推广”或“付费”内容。

内部审查：重新评估“曝光费”、“流量费”等分层收费模式，其在日、韩、泰等国的披露要求下属于高风险点，需确保其公平性与透明度。

4.建立算法变更的合规流程：

参考日本、韩国等地的要求，建立算法排序规则重大变更前的内部评估与外部通知机制，特别是对平台内经营者的提前告知，以避免法律风险。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q72

电商数据（交易记录、评论）通常受到哪些数据跨境传输的合规限制？

（撰写人：傅哲迅）

答：

一、核心提要

1.电商交易记录（含实名、支付、收货信息等）以及带有个人标识的用户评论，在主流APEC经济体均归类为受管控个人信息。

2.APEC经济体对该类数据的跨境传输，主要包括三类：等效保护准入限制，本地化存储限制，用户授权限制。

3.数据传出方一般以数据收集地的规则为核心合规基准。

二、法规矩阵

序号	代表国家	核心法规	等效保护准入限制	本地化储存限制	用户授权限制
1	中国	1.《个人信息保护法》 2.《数据出境安全评估办法》	1. 个人信息向境外提供，应当保证境外接收方的保护水平不低于我国法定标准； 2. 需通过安全评估 / 个人信息保护认证 / 标准合同备案三项之一合规出境。 依据：《个人信息保护法》第38条	关键信息基础设施运营者、处理海量个人信息的主体，境内收集的个人信息应当在境内存储；确需出境必须经安全评估。 依据：《个人信息保护法》第40条	向境外提供个人信息，应当向个人告知境外接收方名称、地址、处理目的等，敏感个人信息跨境应当取得个人单独同意。 依据：《个人信息保护法》第39条
2	美国	1.《加州隐私法》(CPRA)； 2.行政令EO14117 3.第14117号行政令（E.O. 14117）项下执行规则*	1.跨境前核验境外接收方具备同等数据保护能力； 2.限制未经审批向受关注国家大批量跨境传输用户敏感电商数据（含中国），符合法定豁免情形的可依法跨境。 依据：CPRA § 1798.115; EO14117	暂未见强制本土要求。	1. 普通消费者数据跨境 / 售卖需提供选择退出渠道； 2.16周岁以下未成年人个人信息跨境，必须事前主动勾选同意。 依据：CPRA § 1798.120
3	新加坡	1.《个人数据保护法》（Personal DataProtection Act，PDPA）； 2.《个人数据保护条例》（Personal Data Protection Regulations，PDPR）	向境外转移个人数据，必须确保目的地或接收主体具备等效保护标准。 依据：PDPA 26	暂未见对普通电商交易、用户评论数据强制境内存储义务规定。	开展个人数据跨境前，必须清晰告知数据主体：境外目的地、接收方身份、跨境保护安排。 依据：PDPA 10 (3)
*注：全称为：Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons					

三、专业洞察

1.管控共性：中国、美国（加州）、新加坡三大 APEC 核心电商经济体，均将电商实名、支付、收货信息及可识别个人的用户评论列为受监管个人信息，跨境合规制度主要围绕等效保护准入、本地化存储、用户授权三大维度设置合规红线，且遵循数据收集地属地合规原则。

2.合规梯度差异：我国监管力度最为严苛，设置法定三重出境合规路径、特定主体强制境内存储义务及敏感信息单独同意刚性要求；美国加州无全域本地化强制规则，叠加隐私立法与国家安全行政令，侧重境外接收方能力核验与高危国别传输禁令，实行成年人与未成年人分级授权管理；新加坡以境外等效保护为底层原则，无普通电商数据本地化要求，聚焦跨境事前全要素披露，严格限定用户授权的合法生效条件。

3.实操落地建议：跨境电商企业需分区精细化适配合规体系，对华重点落实安全评估、标准合同及本地化存量管控；对美强化高危国家禁传筛查、区分用户群体配置进出授权通道；对新加坡优先佐证境外等效保护资质，完备跨境事前信息告知留存，全链路夯实用户授权合规证据链。

Q73

各经济体对非银行机构提供跨境支付与结算服务有哪些准入牌照要求及/或金融监管要求？

（撰写人：何欣）

答：

一、核心提要

APEC各经济体非银行跨境支付服务的准入共性规则如下：

1. 牌照前置强制原则：所有APEC经济体均实行非银行支付机构持牌经营制度，无牌照不得开展跨境支付、资金结算、外汇兑换、跨境汇款等相关业务，无牌经营多涉及行政处罚，部分地区归属刑事违法。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

2. 境外机构展业限制：绝大多数经济体禁止境外非银行机构直接向境内用户提供跨境支付服务，要求境外机构通过设立本地法人、分支机构或合规持牌合作机构的方式展业，仅中国香港特别行政区、新西兰等少数地区允许合规分支机构展业。

3. 客户资金隔离底线：全区域统一要求支付机构客户备付金、储值资金与机构自有资金完全隔离，实行专户存管、托管或集中缴存，严禁挪用、占用、担保客户资金，筑牢资金安全防线。

4. 合规义务全域适用：所有机构必须履行AML/CFT、KYC尽职调查义务，留存客户身份及交易记录，按时上报大额、可疑交易，严格规避洗钱、恐怖融资、电信诈骗等违法风险。

5. 真实交易背景要求：跨境支付、外汇流转必须依托真实贸易、投资、消费等合法场景，严禁虚构交易、违规跨境套利、逃汇、非法资本流动。

二、法规矩阵

经济体/地区	核心监管机构	必备准入牌照/资质	最低注册资本要求	核心差异化监管规则	法律依据
中国	中国人民银行、国家外汇管理局	1.《支付业务许可证》（跨境支付专项资质）； 2. 外管局跨境收付备案/许可	1亿元人民币（实缴），跨境机构需更高资本充足标准	1. 境外机构禁止直接展业，必须设立境内独立法人；2. 客户备付金全额缴存央行专户集中存管； 3. 交易记录留存不少于5年； 4. 严格审核跨境交易真实背景，禁止虚构交易	国务院令第768号《非银行支付机构监督管理条例》、央行跨境支付配套管理办法
中国香港特别行政区	香港金融管理局（HKMA） 香港海关	1. MSO金钱服务经营者牌照（汇款、货币兑换）； 2. SVF储值支付工具牌照（零售跨境支付、电子储值）	MSO无硬性要求； SVF牌照500万港元（实缴）	1. 境外机构可设分支机构展业，无需全资法人； 2. 交易记录留存7年；3. 外汇管制宽松，仅需履行大额交易申报义务；4. 客户资金与自有资金严格隔离	HKMA《储值支付工具监管制度》、 香港《打击洗钱及恐怖子资金筹集条例》
中国台北	中国台北金融监督管理委员会、数位发展部	1. 电子支付机构许可； 2. 洗钱防制及服务能量登记	新台币500万元（实缴）	1. 境外机构需设立本地法人，禁止直接展业；2. 客户资金专户存管，严禁挪用；3. 跨境交易需核验真实交易凭证； 4. 交易记录留存不少于5年	《电子支付机构管理条例》、中国台北地区第三方支付洗钱防制登记办法
日本	日本金融厅（FSA）、财务省	资金移动业者一类许可（跨境支付专用）	5000万日元（实缴）	1. 可本地分支展业或与本土持牌机构合作；2. 超100万日元跨境交易需向财务省申报；3. 严格依托真实场景开展跨境外汇支付	日本金融厅 《资金移动业法》
韩国	韩国金融委员会（FSC）、金融监督院（FSS）、韩国银行	1. 电子金融业务许可；2. 外汇业务备案/许可	30亿韩元（实缴）	1. 境外机构需设立本地法人，受限外资持股比例；2. 客户资金第三方托管，实时交易风险监控；3. 个人、企业跨境支付额度严格受限	韩国《电子金融交易法》 《外汇管理法》 监管细则
新加坡	新加坡金融管理局（MAS）	SPI标准支付牌照（普通跨境业务）、MPI大型支付牌照（大额跨境业务）	SPI最低10万新元，MPI按业务规模上浮	1. 无强制外汇管制，跨境资金流转灵活；2. 客户资金隔离托管，数据合规本地存储； 3. 对标国际高标准AML/CFT规则	新加坡《支付服务法》
马来西亚	马来西亚国家银行（BNM）	MSB货币服务业务牌照（跨境汇款、外汇兑换唯一资质）	200万林吉特（实缴）	1. 强制设立本地法人机构； 2. 业务系统需通过央行安全认证； 3. 所有跨境交易需按时向监管报备	马来西亚 《货币服务业务法》
泰国	泰国银行（BOT）	PSP支付服务牌照+跨境支付专项资质	5000万泰铢（实缴）	1. 严格外汇管制，个人年度跨境汇款设限；2. 所有跨境支付需核验真实交易背景； 3. 客户资金全额隔离存管	泰国 《支付服务监管条例》
印度尼西亚	印尼银行（BI）、金融服务管理局（OJK）	电子支付机构牌照+跨境支付运营专项许可	100亿印尼盾（实缴）	1. 境外机构必须设立本地法人；2. 跨境交易全部纳入央行跨境结算系统；3. 实行严苛外汇管控与反洗钱核查	印尼银行 《电子支付与跨境结算规则》
菲律宾	菲律宾中央银行（BSP）	EMI电子货币发行商牌照、汇款服务提供商牌照	按业务类型差异化设定	1. 客户资金全额托管；2. 小额个人跨境支付便利化； 3. 所有跨境汇款业务需向央行报备	菲律宾 《电子支付与汇款服务监管规则》
文莱	文莱金融管理局（AMBD）	货币服务牌	照适中门槛，无高额强制要求	全面对标马来西亚MSB监管框架，核心落实AML/CFT合规与外汇管理要求	文莱 《金融机构与支付服务监管条例》

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体/地区	核心监管机构	必备准入牌照/资质	最低注册资本要求	核心差异化监管规则	法律依据
越南	越南国家银行（SBV）	支付服务牌照+跨境结算专项许可	高门槛，按业务规模核定	1. 外资准入限制严格；2. 跨境支付仅限真实贸易场景；3. 严控违规跨境资本流动	越南《支付法》及跨境支付配套细则
俄罗斯	俄罗斯中央银行（CBR）	支付系统运营商牌照+汇款服务双牌照	5000万卢布（实缴）	1. 全量跨境资金纳入央行监控体系；2. 严格外汇管制，禁止无序资本流动；3. 双牌照缺一不可，准入门槛高	俄罗斯《支付系统与跨境结算监管法》
澳大利亚	澳大利亚审慎监管局（APRA）、AUSTRAC	AUSTRAC强制注册+AFS金融服务牌照（跨境汇款专用）	无硬性注册资本要求，需证明财务稳健	1. 核心监管聚焦反洗钱与大额交易申报；2. 客户资金强制隔离；3. 无严格外汇额度限制	澳大利亚《支付服务反洗钱监管规则》
新西兰	新西兰金融市场管理局（FMA）、储备银行（RBNZ）	FSP金融服务提供商注册+反洗钱部门备案	无注册资本硬性门槛	1. 外汇完全宽松，无跨境额度管制；2. 以交易透明化、AML合规为核心监管重点	新西兰《金融服务提供商注册规则》
巴布亚新几内亚	巴布亚新几内亚银行（BPNG）	货币服务牌照	低准入门槛	重点落实KYC身份核验、反洗钱合规，所有跨境交易需向央行报备，遵守本地外汇规则	《支付与货币服务监管条例》
美国	FinCEN、各州金融监管部门、美联储	联邦MSB注册+各州货币传输/汇款牌照（逐州申领）	无联邦统一标准，各州差异化设定	1. 监管碎片化，无全国统一牌照；2. 超1万美元跨境交易强制申报；3. 严格落实OFAC制裁名单管控；4. 反洗钱核查标准严苛	美国《MSB注册与监管规则》
加拿大	FINTRAC、各省金融监管机构	联邦MSB注册+省级支付服务许可	适中注册资本门槛	1. 双层监管体系，省域合规要求差异化；2. 跨境交易强制申报，资金隔离托管；3. 外汇管制宽松	加拿大《MSB监管规则》

经济体/地区	核心监管机构	必备准入牌照/资质	最低注册资本要求	核心差异化监管规则	法律依据
墨西哥	墨西哥银行（Banxico）、CNBV	电子支付机构牌照+跨境汇款服务牌照	达标法定注册资本	严格外汇管制，跨境交易必须核验真实背景，全程落实AML/CFT合规与资金托管要求	墨西哥《支付服务与跨境结算监管法》
智利	智利央行（BCCh）金融市场委员会（CMF）	支付服务提供商牌照+跨境支付专项许可	满足资本充足率要求	境外机构需设立本地代表处或法人，以交易透明化、反洗钱合规为核心监管导向	智利《支付机构监管细则》
秘鲁	秘鲁央行（BCRP）金融监管局（SBS）	货币服务与支付专项牌照	法定最低注册资本	严格KYC核验与反洗钱管控，客户资金全额隔离，所有跨境支付交易需向央行报备	秘鲁《非银行支付机构监管条例》

三、专业洞察

从APEC整体监管体系来看，AML/CFT、KYC、资金隔离、持牌经营是全球统一的刚性合规底线，由FSB等国际机构统一规范，所有经济体无例外执行，构成了非银行跨境支付行业的合规基石。而在准入门槛、注册资本、外汇管制、境外机构准入模式上，各区域呈现显著分化：东亚区域重“准入严控”，通过高资本门槛、严格主体审核筛选合规机构；欧美大洋洲区域重“过程监管”，降低准入门槛，强化交易事中事后核查、风险追责；东南亚区域呈现两极分化，成熟市场宽松、新兴市场严控。这种分化格局要求跨境机构不能套用单一合规模板，必须因地制宜搭建区域合规体系。

1. 牌照合规风险：美洲、东南亚等区域存在多层级、多品类牌照体系，超范围经营、牌照不全、未及时续期是高频违规风险，尤其美国逐州申领牌照的规则，极易引发区域性合规漏洞。

2. 外汇与交易风险：东亚、东南亚、拉美多数经济体实行严格外汇管制，虚构交易、跨境资金套利、超额度跨境支付是监管重点打击行为，真实交易背景留存与核验是核心风控环节。

3. 数据与留痕风险：全区域要求交易记录、客户资料长期留存（5-7年），同时多数经济体要求本地数据本地存储，跨境数据传输需用户单独授权，数据不合规、留痕不全将面临高额处罚。

4. 反洗钱合规风险：大额交易漏报、可疑交易未监测、客户身份尽职调查不到位，是全球监管核查的核心痛点，也是机构被吊销牌照的主要原因。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q74

在何种情况下，平台在多国运营时需设本地代表或制定联络主体？

（撰写人：韦征）

答：

一、核心提要

在APEC地区运营的数字平台，是否需要设立“本地代表”或“联络主体”，已不再仅基于是否有物理存在，而是主要取决于其业务的“市场存在感”及在特定法律领域（如数据隐私、税务、内容监管）的强制性要求。一旦平台的用户规模、收入或业务性质达到法定阈值，或涉及敏感行业，设立本地代表已成为一项普遍的合规义务，用以连接境外平台与本地监管机构及用户。

二、法规矩阵与专业洞察

本部分从“触发维度”和“法律领域”两个层面，梳理设立本地代表的要求，并通过成员经济体案例进行对比。

1. 触发设立本地代表的核心维度

维度	具体情形与阈值	说明与示例
规模阈值	用户数：例如在泰国，月活跃用户超过5,000人。 营业额：例如在泰国，年收入超过5,000万泰铢。 交易量：跨境电商平台年订单量达到法定标准。	达到阈值是触发本地税务登记、指定代表或提交报告等义务的明确信号。
业务性质	“守门人”平台：大型社交媒体、搜索引擎、电商、支付平台等。 敏感行业：涉及金融科技、在线医疗、未成年人保护等。	此类平台因其对社会经济的重大影响或涉及高度监管领域，几乎无例外地被要求具备本地联络主体。

2. 不同法律领域下的具体要求

法律领域	代表类型	核心要求与目的
个人信息保护	隐私代表/指定代表	旨在落实数据保护责任。例如，中国《个人信息保护法》要求符合条件的境外处理者境内设代表；许多参照GDPR模式的经济要求指定联络人以处理数据泄露事件和用户行权请求。
税务合规	税务代表	境外平台作为增值税/消费税的代扣代缴义务人时，通常需在消费地注册并指定税务联络人，负责税务申报与清缴。
平台治理与内容监管	行政联络人/本地协调员	旨在建立行政沟通渠道。例如，泰国《数字平台服务法令》要求满足条件的境外平台指定本地协调员，负责提交报告、处理投诉及政府指令。

3. APEC成员体实务案例对比

成员体	关键触发点	要求形式
泰国	年收入＞5,000万泰铢或月活跃用户＞5,000人	本地协调员（需具备接受法律文书的授权）
中国	为境内自然人提供产品或服务等目的处理个人信息，且属境外处理者	境内设立专门机构或指定代表（需向监管部门报送）
越南	提供电信服务或特定数字内容	代表处/分公司或指定代理（根据《网络安全法》）
印尼	达到“私营范围电子系统供应商”标准	本地联络主体（强制备案制）

“本地代表”的法律角色差异：需明确其在各法域下的具体法律地位。在泰国模式下，本地协调员主要承担“行政传声筒”职能；而在某些消费者保护法规下，代表可能需要承担连带责任。其职权范围（如能否签署合同）直接关系到母公司风险。

警惕“常设机构”税务风险：在设立本地代表时，必须谨慎界定其职权。若该代表被认定拥有以母公司名义签订合同的授权，可能依据中国与相关国家签订的税收协定，构成“常设机构”，从而导致母公司在该国的利润被征收企业所得税。

三、行动清单

为平台企业系统化应对APEC各经济体本地代表设立要求，建议按以下步骤开展合规工作：

第一步：评估管辖与义务触发

业务画像：梳理在各目标市场的用户数、营收额、订单量等数据，比对当地的规模阈值。

行为定性：断业务是否表现出“导向性经营”（如使用当地语言、提供本币支付、进行本地营销），这可能导致即使未达量化阈值，仍被认定为具有“市场存在感”而纳入监管。

第二步：界定代表角色与法律授权

分法域厘清：根据目标国家的具体法律（如泰国的《数字平台服务法令》、中国的《个人信息保护法》），明确所需设立代表的法定名称、资格要求和具体职责。

起草授权文件：审慎拟定对该代表的授权委托书，明确限定其权限范围（特别是排除其代表母公司签署合同的权力），以规避潜在的“常设机构”税务风险，并明确责任承担界限。

第三步：建立合规隔离与应急流程

设立合规实体：在要求较高的法域（如印尼），评估设立法律实体（如代表处）的必要性。

编制联络手：为所有本地代表编制统一的《监管联络与响应手册》，规范其与当地监管部门、用户沟通的标准流程和话术。

纳入应急体系：将本地代表明确纳入公司的数据泄露应急响应预案和重大监管问询处理流程，确保其能依法履行即时通报、协同处置的职责。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q75

跨境提供数据专业服务的情境中，有关数据服务合同如何确定适用法律与争议解决的管辖方式？

答：

跨境数据服务合同中，适用法律和争议解决条款应优先按意思自治明确约定，并尽量选择便于执行的法域与机制；实务上通常优先考虑仲裁，写清仲裁机构、仲裁地和语言，若选择诉讼则应明确具体法院及是否排他，同时还要注意数据出境、个人信息和其他强制性合规规定不能被合同约定排除。



作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q76

哪些APEC经济体实施数据基础设施的安全审查？

（撰写人：郭小萱）

答：

一、核心提要

审查普遍化但碎片化：APEC《数字经济安全保障框架》（APEC Framework for Securing the Digital Economy，2019年）建议成员经济体采用系统化风险管理方法保护关键信息基础设施（CII），但各经济体在触发条件、本地化要求与合规标准上差异显著，区域内监管规则碎片化趋势明显。

中美越三国模式最具代表性：中国依托《数据安全法》建立数据分类分级安全审查制度；美国通过第13873号总统令重点防范“外国对手”对ICTS供应链的渗透；越南《网络安全法》（第116/2025/QH15号，2026年7月1日生效）对国家安全重要信息系统实施强制事前鉴定。

企业须采取前置化合规策略：APEC《隐私框架》强调任何对跨境数据流动的限制须与风险成比例，跨国企业应提前将IT资产映射至各国监管图谱，以前置审查规避业务停摆风险。

二、法规矩阵与专业洞察

【比较法律要求】

经济体	核心依据	审查触发条件	主管机制
中国	《数据安全法》（2021）	影响国家安全的数据处理活动；CII运营者重要数据出境	网信部门与行业主管部门联合监管，国家安全审查一票否决制
美国	第13873号总统令（2019）	“外国对手”所控制人员设计、供应的ICTS	商务部主导，可直接禁止交易或要求风险缓解协议
越南	《网络安全法》（2025，第116/2025/QH15号）	1至5级分类，涉及国安、国防、能源等领域的4至5级系统	公安部主导，系统运行前须完成强制网络安全鉴定

中国构建了以《数据安全法》为核心的综合性审查体系。第二十一条确立核心数据、重要数据、一般数据的分类分级保护制度；第二十四条对影响国家安全的数据处理活动实行国家安全审查；第三十一条对CII运营者重要数据出境设置严格红线，在华运营的云计算、大数据中心企业面临硬件与数据双重合规压力。

美国第13873号总统令宣布ICTS领域国家紧急状态，授权政府对涉及“外国对手”控制供应商的设备及技术实施直接禁令，审查不仅针对基础设施的物理部署，更溯源至技术来源地与实际控制权，行政裁量空间极大。

越南2025年《网络安全法》第八条将信息系统划分为五级，第九条界定“国家安全重要信息系统”涵盖军事、外交、能源、金融等核心领域；第十一条要求上述系统在投入运行前须通过公安部主导的“网络安全鉴定”，运行期间须配合突击检查与实时监控，属地化强制色彩突出。

三、行动清单

□ 对APEC各经济体部署资产及数据进行分类定级摸底；

□对照各国法律清单评估自身是否被认定为CII，重点参照越南《网络安全法》第九条所列领域目录及中国《数据安全法》第二十四条；

□审查供应链中是否存在被第13873号总统令认定为“外国对手”的高风险供应商，提前准备替代采购预案；

□针对越南等要求事前审查的经济体，在项目立项阶段即引入当地资质机构，确保满足第十一条强制鉴定要求；

□设立专职数据安全负责人，定期开展风险审计，以应对全球标准缺失带来的持续合规压力。

Q77

网络产品进入各成员经济体，通常可能涉及哪些安全认证、技术合规评估或准入要求？

答：

在APEC框架下，网络产品进入各成员经济体时，通常不会设定统一的“APEC通行证”，而是分别适用各经济体自身的认证、测试、备案和市场准入规则。整体上，最常见的产品安全认证、网络安全/隐私合规评估，以及针对高风险产品或服务的登记、审查或本地化要求。

一、通用认证：

产品安全与电磁兼容认证，尤其是带无线通信、终端接入、物联网功能的网络产品，通常要满足当地的电气安全、EMC、RF和语音规则。

网络安全认证或评估，一些经济接入要求第三方测试、漏洞评估、渗透测试、供应链安全证明，部分还将接受或搜集国际通行的安全认证体系。

隐私与数据保护认证，APEC体系里比较典型的边境隐私规则框架下的企业隐私认证思路，例如CBPR/PRP机制一类，用于证明企业的数据保护能力。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、常见技术评估：

数据跨境合规评估，如果产品会收集、传输或远程访问个人数据，通常会涉及数据最小化、目的限制、知情同意、跨境传输条件和接收方审查措施。

算法与内容安全评估，带来推荐、排序、生成、过滤或自动决策功能的产品，可能需要说明算法逻辑、风控措施、内容审核和用户退出机制安排。

供应链与机制更新审查，很多市场都会看是否存在后门、缺缺弱口令、补丁机制终止、日志留存不足、事件响应不足等问题。

三、常见准入要求：

备案、注册或通知，部分成员经济体对电信设备、无线设备、云服务、数字平台或高风险软件要求事前登记、上市通知或当地代表。

安全审查或主管机关批准，涉及关键基础设施、公共安全、国家安全或海量数据处理的产品，可能触发更强的审查程序。

本地化或附条件准入，少数经济接入对数据存储地点、审计接口、答复响应和本地合规主体提出要求。

Q78

云服务商的合规责任有哪些？（撰写人：郭小萱）

答：

一、核心提要

依据APEC隐私处理者认证体系（PRP），云服务商作为处理者，须严格在控制者授权范围内处理数据，建立完善内部治理机制，协助控制者履行对终端用户的隐私承诺，不得擅自超出指令范围使用数据。

APEC《隐私框架》（2015年版）要求云服务商在服务架构层面落实九项核心原则，安全保障（Security Safeguards）系其中硬性要求，须通过访问控制、加密及漏洞管理等技术手段将隐私保护内嵌于产品全生命周期。

跨境数据流通须借助隐私增强技术（PETs）化解合规摩擦：亚太各成员经济体监管差异显著，云服务商在处理跨境数据时，可运用差分隐私、联邦学习等前沿隐私增强技术（PETs）技术，在满足本地化监管要求的同时实现数据的合规流转，降低因司法管辖冲突引发的违规风险。

二、法规矩阵

根据APEC PRP项目要求及TELWG Recommendations for Cloud Transformation in APEC（云转型建议），云服务商需履行以下具体责任：

责任类型	具体内容
强化的安全保障责任(Security Safeguards)	书面安全政策：必须制定并执行涵盖受托处理个人信息的书面信息安全政策。
	物理、技术与行政控制：实施包括身份认证、访问控制（如密码保护）、数据加密、边界保护（防火墙/入侵检测）、审计日志记录及漏洞扫描在内的综合防护措施。
	员工合规培训：建立定期的培训机制和程序，确保员工签署安全政策并意识到隐私保护的义务。
问责制与透明度(Accountability)	违约通知义务：一旦发生数据泄露或隐私安全事故，处理者负有法定义务及时通知数据控制者。
	分包处理者管理：若将数据再次转包给第三方（Sub-processors），需通过合同确保第三方承担不低于原合同的合规责任，并对分包行为保持透明。
	测试与评估：需定期测试安全措施的有效性，并根据技术发展评估风险，更新防护策略。
跨境流动的合规对接(Cross-border Interoperability)	利用CBPR与PRP实现互认：APEC通过CBPR（控制者）与PRP（处理者）体系建立跨境流动信任机制。云服务商通过PRP认证可大幅降低其企业客户在亚太区域内进行数据跨境传输的合规摩擦。

三、专业洞察

针对AI与大数据行业，单纯的制度合规已不足够，必须结合前沿技术手段：（1）引入隐私增强技术：2026年APEC最新研讨会强调，云服务商应积极应用差分隐私(Differential Privacy)、联邦学习(Federated Learning)及同态加密(Homomorphic Encryption)，以在保障AI模型训练效能的同时，实现数据”可用不可见”，满足日益严苛的合规监管需求；（2）对齐国际云安全标准：APEC建议成员经济体鼓励云服务商采用 ISO/IEC 27017（云服务安全控制）和 ISO/IEC 27018（公有云PII保护）标准。这些标准提供了针对云环境的特定控制项，如明确物理选址、数据销毁机制等。

四、实务建议：出海企业的合规落地

□ 在技术研发与业务拓展团队中设立专门岗位，确保”隐私设计 (Privacy by Design)”理念嵌入AI算法开发全生命周期。

□ 利用如新加坡等经济体提供的PETs监管沙盒，在受控环境中测试新型隐私技术，提前降低监管合规的不确定性。

□ 发布并使用符合APEC要求的标准流程、风险评估模板和核对清单，提高与亚太地区大客户谈判时的信任水平。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q79

云服务商的合规责任有哪些？（撰写人：郭小萱）

答：

一、核心提要

工控系统与 IoT 设备并非一律必须先通过“当地安全测试”后方可落地。现行规则并没有针对所有此类设备设定统一、普遍适用的“本地测试前置”要求。

是否必须测试，关键取决于具体监管场景。如产品本身被纳入网络关键设备或网络安全专用产品目录，或其部署后的系统构成等级保护对象、关键信息基础设施，或者项目、行业主管部门明确要求检测、测评、验收，则应依法完成相应安全程序。

法律判断重点不在“是不是当地测试”这一表述本身，而在于是否触发强制性的产品准入、系统测评、风险评估或项目验收义务。因此，合规判断必须结合设备类别、部署行业、使用场景和落地方式具体分析。

二、法规矩阵与专业洞察

1.核心规则对照表

场景	是否可能需要安全测试	主要要求
一般工控设备、一般 IoT 终端	不当然需要	原则上无法律要求一律先做“当地测试”
属于网络关键设备、网络安全专用产品目录的产品	需要	应依法完成安全认证或安全检测，方可销售或提供
已部署运行的工控系统、IoT 平台	视情况需要	若构成等级保护对象，通常需履行定级、建设整改、等级测评等义务
用于关键信息基础设施的系统或设备	需要	运营阶段通常应开展网络安全检测和风险评估
行业主管部门、招投标文件、项目验收规范另有要求	需要	应按项目规则完成检测、测试或验收，否则可能影响交付和上线

2.洞察

从规范层级上看，工控系统与 IoT 设备的安全要求，通常分为产品准入、系统合规、持续运营、项目验收四个层面。如果是单体产品，重点看其是否被纳入法定目录；如果是已落地运行的系统，重点看是否进入等级保护或关键信息基础设施监管范围；如果是具体建设项目，还要看合同、招标文件、行业标准以及主管部门要求是否把安全测试作为交付前提。也就是说，实践中真正起决定作用的，不是“设备是不是工控或 IoT”，而是其所处的法律身份和落地环境。

因此，更稳妥的结论是：工控系统与 IoT 设备原则上并非当然必须通过所谓“当地安全测试”，但一旦进入法定目录监管、等级保护框架、关基保护框架，或者项目验收制度已经明确要求，则相关测试、检测、测评或评估就具有强制性。

3.实务案例

例如，某制造企业采购一批工业网关和传感终端接入生产线。若该批设备仅作为一般辅助设备使用，且未落入法定目录，也未进入重点监管系统，则通常不存在统一的“当地测试前置”义务；但若该项目接入的是企业核心生产控制网络，构成等保对象，或者属于能源、交通、通信等重点行业场景，则上线前往往就需要结合本地实际网络环境开展安全测评、漏洞检查、边界防护验证和验收测试。此时，测试要求就不再是可做可不做，而是合规落地的重要组成部分。

三、行动清单

- ☐ 先区分对象是“单体产品”还是“已部署系统”
- ☐ 核查产品是否属于网络关键设备或网络安全专用产品目录
- ☐ 判断系统是否构成网络安全等级保护对象
- ☐ 判断业务场景是否涉及关键信息基础设施
- ☐ 审查行业监管规则、主管部门要求是否有专项检测义务
- ☐ 核查招标文件、合同条款、验收标准是否将安全测试列为上线条件
- ☐ 结合本地实际部署环境评估是否需要补充风险评估、渗透测试或验收测试
- ☐ 形成书面合规结论，避免仅以“未要求当地测试”为由直接上线

Q80

若企业系统遭网络攻击，应如何进行处置？是否必须向监管机构报告？

（撰写人：左李福）

答：

一、核心提要

1.应急处置四阶段系合规前提：发现网络安全事件后，企业应依次完成“发现与隔离→研判与评估→报告与通知→溯源与恢复”四阶段处置。尤其在报告环节，多数亚太经济体已建立强制性报告制度，企业须在法定时限内向指定监管机构报告，迟报、瞒报或漏报将面临从罚款到刑事责任等多层次处罚。

2.亚太各国报告义务差异显著，需精准区分：中国、新加坡、澳大利亚、韩国、印度等国对网络安全事件设有强制性报告义务，时限从1小时到72小时不等；日本仅对涉及个人信息泄露的事件设强制报告要求，一般网络安全事件无通用报告义务；中国香港特别行政区是目前亚太地区少数尚未建立法定强制通报机制的司法管辖区，但自愿通报的“隐性压力”不容忽视。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

3.分层级初步报告与安全港保护：各国普遍允许企业先提交初步报告满足法定时限，后续补充详细信息。中国明确规定，采取合理必要防护措施并按期报告的，可视情从轻或免于追责，构成法定的“安全港”条款。

二、法规矩阵与专业洞察

1.网络安全事件快速处置流程——发现、隔离、研判、报告、恢复的闭环管理

企业在遭受网络攻击后均建议遵循以下五阶段标准化处置流程：

阶段一：发现与隔离（0-1小时）——系统检测到异常活动或收到攻击告警后，应第一时间采取隔离措施，切断受感染系统与主干网络的连接，防止横向移动和损害扩散。同时保存日志文件、网络流量数据、内存镜像等原始证据，确保证据链完整。该阶段还应立即向上级主管和信息安全负责人汇报，确保决策层第一时间知情。

阶段二：研判与评估（1-4小时）——技术团队对事件进行初步分析，判断攻击类型（如勒索软件、APT攻击、DDoS攻击等）、受影响系统的范围和敏感数据类型。根据各国法律规定的分级标准评估事件等级。例如，在中国，须依据《国家网络安全事件报告管理办法》中的《网络安全事件分级指南》判断属于“较大”“重大”还是“特别重大”级别；在新加坡，CII所有者在知悉后2小时内须判断事件是否属于法定报告范围。

阶段三：报告与通知（按规定时限执行）——这是合规义务最集中的环节。企业需在规定时限内向法定监管机构报告，同时在涉及个人信息泄露时通知受影响的数据主体。各国普遍允许先提交初步报告满足法定时限，后续再补充详细信息。

阶段四：溯源与恢复（持续进行）——在完成初步报告后，企业应开展深度溯源分析，查明攻击入口、攻击者身份及渗透路径，并修复相关漏洞。同时从备份中恢复受影响系统，重建业务连续性。

阶段五：总结与整改（事后）——事后进行全面复盘，更新应急预案，并根据监管部门要求提交整改报告。例如，中国要求网络运营者在事件处置结束后30日内提交事件处置总结报告。

2.洞察

(1)中国：“最严报告制度”下的安全港机制

中国自2025年11月1日起施行的《国家网络安全事件报告管理办法》，结合新修订的《网络安全法》（2026年1月1日施行），构建了亚太地区最为严格的网络安全事件报告制度之一。该办法将网络安全事件分为特别重大、重大、较大、一般四级，并以有限枚举方式给出分级定量指标。其突出特点在于：

分级分主体差异化时限：依《国家网络安全事件报告管理办法》（2025年）应按事件级别区分报告时限：特别重大/重大事件，CIIO须在30分钟内、中央国家机关须在1小时内、其他网络运营者须在2小时内报告；较大/一般事件，CIIO须在1小时内、中央国家机关须在2小时内、其他网络运营者须在4小时内报告。涉嫌违法犯罪的，还须在24小时内向公安机关报案。

明确的安全港条款：该办法第十一条明确规定，网络运营者“已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任”。这一条款为合规企业提供了法定的责任豁免空间。

分级定量指标清晰：核心数据泄露或个人信息泄露超过100万条即构成“较大事件”，直接触发报告程序；直接经济损失超过500万元同样构成较大事件，显著降低了报告门槛。

(2)新加坡：多层递进式报告与APT专项要求

新加坡《网络安全法》修正案于2025年10月31日正式生效，建立了多层递进式的报告机制。CII所有者须在知悉网络安全事件后2小时内向CSA提交初步报告，14天内提交补充报告；STCC所有者则须在2小时内初步报告、72小时内补充报告、30天内提交最终报告。修正案还特别要求对涉嫌由APT引起的事件、影响公众的事件、涉及零日漏洞利用或特定妥协指标的事件进行升级报告，在2小时、72小时或30天内分别履行不同的报告义务。

(3)中国香港特别行政区：自愿通报制度的“隐性高压”

中国香港特别行政区是亚太地区少数尚未建立法定强制通报机制的司法管辖区。私隐专员公署发布的《资料外泄事故的处理及通报指引》属于行政建议性质，鼓励资料使用者在发生“相当可能会对资料当事人造成实际损害的风险”的数据泄露事件时自愿向PCPD及受影响个人通报。政府曾计划修订PDPO引入强制通报机制并设定5个工作日的时限，但截至2026年初因考虑对中小企业的潜在影响而暂时搁置。

企业需高度警惕的是，尽管通报是自愿的，延迟通报可能被PCPD视为违反保障资料第4原则（DPP4）的初步证据。一旦被裁定违反DPP4，PCPD可发出具有法律约束力的执行通知；违反执行通知即属刑事犯罪，首次定罪可处最高5万港元罚款及两年监禁。因此，自愿通报制度下的“隐性高压”不容忽视。

(4)韩国：2026年立法密集更新

韩国2026年密集通过了多项网络安全立法更新，是亚太地区立法动态最为活跃的司法管辖区之一：

IT Network Act修正案（2026年3月12日国会通过，3月24日国务会议批准）：延迟或故意不报告黑客事件的企业将面临罚款增加；五年内因故意或重大过失发生两次以上安全事件的电信服务提供商，最高可处销售额3%的罚款。企业须指定高管担任CISO并设立信息安全委员会，信息安全管理体系认证标准将分级适用。

PIPA修正案（2026年2月12日国会通过、3月10日颁布，2026年9月11日生效）：最高行政处罚罚款从原先标准提升至企业总营收的10%。对重复发生个人信息泄露或对超过1,000万人造成损害的企业，将征收惩罚性纠正费。

政府调查权限扩大：修正案还允许政府在收到企业报告前，仅凭涉嫌安全事件即可启动现场调查，大幅降低了监管介入门槛。

(5)马来西亚：2026年网络安全法全面生效

马来西亚《2025年网络安全法》（ONSA）自2026年1月1日起正式生效，标志着该国在数字治理和数据安全领域迈出重要一步。该法明确了“关键信息基础设施”的定义，涵盖金融、能源、交通、通信、

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

医疗和政府信息系统。NCII实体须在初步6小时内向NACSA和行业主管部门报告，详细报告须在14天内提交。此外，PDPA还规定了数据泄露事件的报告义务——一旦发生重大数据泄露，企业须在72小时内向当局通报，并在7天内通知受影响用户。未报告网络安全事件的最高罚款为50万林吉特及10年监禁。

(1)印度：6小时超短时限

印度CERT-In指南要求所有实体在检测到网络安全事件后须在6小时内报告，涵盖数据泄露、凭证泄露、恶意软件入侵等各类事件。涉及勒索软件并伴有数据外泄的事件，建议在24-48小时内完成报告。这一6小时时限是亚太地区最短的报告时限之一。

1.实务案例：

澳大利亚Optus数据泄露事件

2022年9月，澳大利亚第二大电信运营商Optus发生大规模数据泄露事件，约980万客户（占澳大利亚总人口约40%）的个人信息遭泄露，包括姓名、出生日期、电话号码、电子邮件地址以及部分客户的驾照号码和护照号码。

事件发生后，OAIC立即对Optus提起民事诉讼，指控其违反《隐私法》的多个条款。OAIC在起诉书中主张，980万名受影响客户中的每一位均可视为一次独立违法，这意味着潜在最高罚款总额达到惊人的21万亿澳元。尽管最终罚款金额不会达到这一理论数字，但该案例充分说明：在数据泄露事件中，企业不仅面临监管机构的行政处罚风险，还可能因未能及时、充分地向受影响个人通报而承担额外的法律责任。该案还催生了澳大利亚《网络安全法》2024年新增的赎金支付强制报告义务（2025年5月30日起生效），要求年营业额超过300万澳元的企业在支付赎金后72小时内向ASD报告。

这一案例对亚太企业具有重要警示意义：在跨境运营中，企业须高度重视各国报告时限的差异，建立分层级报告机制。尤其在新加坡、马来西亚、菲律宾、泰国等设72小时时限的国家，以及印度等设6小时超短时限的国家，企业若未能按时履行报告义务，可能面临监管调查、巨额罚款乃至刑事责任。

三、行动清单

第一步：确认触发条件 —— 事件发生后，立即研判是否达到所在司法管辖区的法定报告门槛。在中国，重点关注是否触及“个人信息泄露100万条”“直接经济损失500万元”或“核心数据泄露”等分级标准；在澳大利亚，关注是否涉及“可能造成严重损害”的个人信息泄露或赎金支付。切勿因等待完整调查结果而延误初步报告。

第二步：分层级初步报告 —— 绝大多数司法管辖区允许先提交初步报告满足法定时限，后续补充详细信息。建议企业在发现事件后1-2小时内完成初步报告的基本信息收集和提交流程。在中国，可利用12387网络安全事件报告热线、官网、微信公众号、微信小程序、邮件、传真等六类渠道提交报告。

第三步：保存证据链 —— 保存日志文件、网络流量数据、内存镜像、通信记录等原始证据，确保证据链完整、可追溯。该等证据在后续监管调查、溯源分析和责任认定中至关重要。在日本等未明确要求保存日志的法域，保存证据同样是有效应对调查和降低责任风险的重要手段。

第四步：通知受影响个人 —— 在涉及个人信息泄露时，评估是否需要以及何时通知受影响的数据主体。在中国、韩国、泰国、菲律宾、马来西亚等国，通知个人通常是法定义务；在中国香港特别行政区，即使通报自愿，也强烈建议通知受影响的资料当事人。通知内容应包括事件性质、受影响数据类型、已采取的补救措施及后续联系方式等。

第五步：跨境事件协调机制 —— 对于涉及多个司法管辖区的数据泄露事件，建立跨法域报告协调机制。统筹安排各国通报的先后顺序和披露口径，避免因国内已通报而海外延迟通报引发的“双重标准”合规风险。特别关注不同法域报告时限的差异——如印度6小时、新加坡2小时、中国CIIO 1小时、菲律宾72小时、泰国72小时——以最短时限为准启动内部响应。

第六步：评估安全港资格 —— 在中国等设有安全港条款的法域，确保企业已采取合理必要的防护措施并按照应急预案进行处置。按期报告并有效降低事件影响的，可视情从轻或不予追究责任。建议在报告中主动说明已采取的防护措施和应急处置情况。

第七步：事后整改与总结 —— 事件处置结束后，按要求向监管部门提交详细的事件处置总结报告。在中国，须在30日内完成；在新加坡，CII所有者须在30天内提交最终报告。总结报告应包括事件原因、应急处置措施、造成的危害、责任追究、完善整改情况等内容，并据此更新网络安全事件应急预案。

第八步：定期演练与预案更新 —— 建议企业每半年至少组织一次网络安全事件应急演练，确保相关岗位人员熟悉处置流程和报告要求。根据演练结果和法规更新情况，至少每年度更新一次网络安全事件应急预案，确保预案始终与现行法律法规保持一致。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q81

各成员经济体通常如何管控加密技术的进出口？（撰写人：徐银萍）

答：

各国对加密技术的进出口管制通常基于国家安全、外交政策和技术竞争考量，但具体做法差异很大。为了方便快速了解，将主要经济体的核心做法整理成了下表：

经济体	监管核心特点	主要依据/清单	典型限制内容
中国	清单式许可管理：对特定商用密码实行进口许可和出口管制，大众消费类产品通常豁免。	商用密码进口许可清单、出口管制清单。	高性能安全芯片、密码机、加密VPN设备、量子密码设备等。
美国	内外有别，严格控制：历史上管制严格，现已放宽对多数商业加密产品的出口，但对特定国家和军用/高端技术仍严格限制。	《出口管理条例》(EAR)，原由《国际武器贸易条例》(ITAR)管制。	向古巴、伊朗、朝鲜等国的出口被严禁；对特定高性能加密技术实施管制。
欧盟	侧重网络安全合规：对进口产品的安全性和制造商责任提出强制性要求。	《网络弹性法案》(CRA，2027年全面生效)。	要求带数字元素的产品符合欧盟网络安全标准，否则不能上市。
俄罗斯	普遍许可，特定豁免：加密产品进出口通常需许可，但对部分商业用途设备有豁免。	联邦安全局技术鉴定是获取进出口许可证的关键环节。	特定商用广播、银行设备等可能获得豁免。
日本、韩国等	许可审批制：对加密设备或超过一定额度的交易实施许可证管理。	国内贸易管制法规。	日本对交易额超5万日元的密码出口要求许可证。

主要经济体的具体做法：

1. 中国：基于清单的“靶向”管理

中国的监管体系清晰，核心是两部清单和一项豁免。

· 法律基础：依据《商用密码管理条例》，对列入清单的密码产品实施进口许可和出口管制。

· 监管内容：具体管控对象非常明确，主要针对高性能和特定领域的密码产品，例如加解密速率超过10Gbps的安全芯片、密码机，以及量子密码设备等。

· 重要豁免：大众消费类产品（如手机、智能家居设备中使用的密码）不实行进口许可和出口管制，这平衡了安全与便利。

2. 美国：从全面管制到分类放松

美国的政策演变显著，反映了技术从军用转向民用的趋势。

· 历史与演变：加密技术曾被视为“军火”受严格管制。后逐步放宽，如将可自由出口产品的密钥长度提升至64位。

· 当前重点：管制重点转向防止高端技术流向特定国家（如古巴、伊朗、朝鲜等）以及用于军事、恐怖主义用途。

· 密钥恢复：历史上曾推广“密钥托管”或“密钥恢复”机制，以便执法部门在必要时访问数据。

3. 欧盟：通过产品安全标准进行间接管控

欧盟虽无专门的加密进出口许可清单，但通过强制的网络安全标准对进入其市场的产品进行管控。

· 核心法规：《网络弹性法案》要求所有在欧盟市场销售的“带有数字元素的产品”必须满足严格的网络安全要求，否则不能销售。

· 影响：这迫使所有制造商（无论产地）必须确保其产品的设计和全生命周期安全，实质上构成了技术性贸易壁垒。

4. 其他地区：普遍采用许可制

许多经济体对加密设备实施进出口许可证管理，但范围和严格程度不同。

· 俄罗斯：加密产品进出口需经联邦安全局技术鉴定并获取许可证，但对部分明确列出的商业设备（如特定广播、银行设备）给予豁免。

· 日本、韩国、印度：普遍对加密设备实施进口或出口许可证管理。

国际协调与区域规则

各国管制措施并非孤立存在，也受到国际协定影响。

· 多边协调：《瓦森纳安排》是一项重要的多边出口管制机制，其《基本清单》包含密码设备，成员国（包括美、日、韩、俄等）会据此调整本国出口控制政策。

· 区域协定：在《区域全面经济伙伴关系协定》等自贸协定中，各缔约方在承诺推动数据跨境自由流动的同时，也明确保留了出于基本安全利益采取管制措施的权力。这为各国实施加密技术进出口管制提供了国际法依据。

企业应对要点

从事相关国际贸易的企业应注意：

1.提前鉴定：在进出口前，主动向主管部门或专业机构确认商品是否受管制。

2.申请许可：如受管制，提前准备技术说明、最终用户证明等材料，依法申请许可证，中国法定的审批时间为45个工作日。

3.关注合规：出口至欧盟需提前确保产品满足《网络弹性法案》等网络安全标准。

4.利用试点：关注中国自贸试验区等地的特殊政策。例如，天津在特定条件下对不涉及国家安全的商用密码进口不采取限制措施。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q82

硬件产品的固件在何种情况下可能触发备案、公告、测试或重新认证等合规要求？ （撰写人：徐银萍）

答：

硬件产品固件的合规要求通常在产品发生功能变化、出现安全事件、法规更新或面向特定市场时被触发。

一、下面是具体触发场景及对应合规类型的梳理：

触发场景类别	具体情形举例	可能触发的合规要求类型
固件变更的性质与内容	固件更新导致产品主要技术参数、功能或性能发生变更。	备案、重新认证、变更许可
	固件修复漏洞、优化性能，但硬件、底层BIOS/固件或核心组件有更改。	重新认证、测试（升级认证）
安全事件与漏洞	产品发生与固件相关的安全事件或事故（如功能失效导致碰撞）。	事件报告、缺陷调查、召回
	发现并确认固件存在被主动利用的安全漏洞。	漏洞报告、公告、发布补丁

二、关键合规实践建议

除了应对上述触发点，主动建立以下合规实践能有效管理风险：

1.实施固件签名与完整性保护

对于关键信息基础设施、IoT设备或受强监管行业的产品，实施固件签名是证明固件完整性与来源可信的核心技术手段。建议建立自动化的企业级签名系统，替代易出错的手工操作，并确保使用符合规范的密码算法（如国密SM2/SM3）。

2.进行定期的合规性差距分析

面对国内外不断更新的法规（如欧盟CRA），建议定期针对产品线进行合规差距分析。重点评估：产品分类是否准确（默认、重要或关键）、支撑周期是否满足、现有流程是否能满足漏洞与事件报告的短时限要求。

3.关注供应链与合作伙伴合规

固件的合规性可能受限于供应链。需在合同中明确供应商的合规责任，并对关键组件供应商进行尽职调查。若产品依赖第三方认证组件（如通过红帽认证的硬件），需确保其认证在有效期内并可被正确“利用”或“传递”。

三、需要留意的情况

目前关于硬件固件合规的公开信息，存在一些普遍性的信息缺口：

1.高度特定行业要求：针对医疗设备、工业控制系统、航空航天等领域固件的特殊准入和测试要求，通常由行业监管机构另行详细规定。

2.各国市场准入差异：除欧盟CRA外，其他重要市场（如美国、日本）对特定类别硬件固件可能存在独特的备案或认证要求。

Q83

安全事件应急预案是否是强制要求？ （撰写人：李亚兵）

答：

在当前的全球网络空间治理语境下，企业若仍将网络安全事件应急预案视为一项“选配”或单纯的技术建议，将面临巨大的合规风险。无论是基于中国完善的法律体系，还是 APEC 的跨境隐私保护原则，亦或是欧盟等经济体的严厉监管，建立、演练并有效执行安全事件应急预案，已无可争议地成为企业必须履行的法定强制义务。

一、法律合规的绝对强制性

应急预案的强制性直接源于各国核心网络安全法典的明文规定，是对企业履行“勤勉尽责”义务的核心要求。

具体法条参考：

1、《中华人民共和国网络安全法》（2017 年实施）：

第 25 条：网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，应当立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

2、《中华人民共和国数据安全法》（2021 年实施）：

第 29 条：开展数据处理活动应当加强风险监测，发现数据安全漏洞、风险等缺陷时，应当立即采取补救措施；发生数据安全事件时，应当立即采取处置措施，并按照规定向有关主管部门报告；涉及个人信息的，还应依法履行告知义务。

3、APEC 隐私框架（Principle 7 – Security Safeguards）：

要求个人信息控制者应建立合理的安全保障措施，并确保其具备应对未经授权访问、披露或泄露的补救与响应机制（Retrievability and Correctibility）。这一原则是 APEC CBPR 认证中评估企业应急响应能力的核心依据。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、强制性义务的实务内涵与标准

监管机构在评估预案合规性时，已不再满足于“有没有纸质文档”，而是关注“是否有效且可执行”：

1、分级响应机制：预案必须针对不同级别的事件（如：一般事件、较大事件、重大事件、特别重大事件）设立清晰的技术和管理处置流程。例如，涉及100万以上个人信息泄露的事件，其报告层级和处置速度应远高于单一用户投诉。

2、法定报告时限：“立即报告”不再是一个模糊概念。中国相关地方细则已开始对“严重事件”提出小时级的报告要求；欧盟GDPR第33条更是明确，企业须在72小时内报告重大泄露。缺失预案导致报告延误，本身即构成新的合规违规。

3、定期演练的刚性要求：法律要求的不仅是“有预案”，更要求“预案有效”。《网络安全等级保护条例（征求意见稿）》明确重点保护对象应当每年至少进行一次应急演练。未进行演练的，可能被视为未履行法定保护义务。

三、实务案例

2023年，某知名跨境电商平台（企业A）遭遇SQL注入攻击，导致包含中国、新加坡两地用户在内的数十万条敏感信息（姓名、地址、卡号）泄露。监管机构介入调查。

调查发现：企业A的合规手册中虽然提及了“建立系统安全保护措施”，但并没有针对具体网络攻击场景（如勒索病毒、数据批量泄露）制定《应急处置操作手册》。更严重的是，该企业自成立以来从未举行过任何形式的网络安全突发事件模拟演练。

处理结果与启示：监管部门认定，该平台违反了《中华人民共和国网络安全法》第25条，属于“未制定应急预案”。鉴于违法行为导致了大量公民个人信息泄露的严重后果，监管部门依据该法第59条关于未履行网络安全保护义务的规定予以处罚。

该案例说明，建立、演练并有效执行安全事件应急预案，是企业的法定强制义务。即使企业采取了基础的技术防护，但是缺失法定且有效的预案，依然属于严重合规疏忽，无法规避监管制裁。

Q84

跨境运营的企业如何统一网络安全管理？（撰写人：李亚兵）

答：

在经济全球化与数字化的双重浪潮下，跨境企业正面临前所未有的合规挑战。其网络安全管理架构必须同时处理多国监管机构的严厉管辖，包括中国的数据本地化要求、欧盟的GDPR、以及APEC成员经济体间的自由流动诉求。成功的跨境安全管理不再是“一套标准走天下”，而是构建一个“逻辑统一、本地适配、动态合规”的整合管理体系。

一、跨境管理的合规边界与法理依据 统一管理的起点在于精准识别并映射各地区的法律要求。核心法理依据在于建立企业内部的“责任对等”机制，确保数据在不同分支机构间流动时安全不降级。

1、《中华人民共和国网络安全法》第37条、《中华人民共和国数据安全法》第31条：关键信息基础设施运营者在中华人民共和国境内收集和产生的个人信息和重要数据的出境，适用《中华人民共和国网络安全法》的规定；其他数据处理者在中华人民共和国境内收集和产生的个人信息和重要数据出境，应当通过国家网信部门组织的安全评估；法律、行政法规或者国家网信部门规定不需要进行安全评估的，从其规定。

2、欧盟《通用数据保护条例》（GDPR）第46条：允许在具备“适当保障措施”的前提下进行数据跨境传输，其中包括标准合同条款（SCCs）和约束性企业规则（BCRs）。

3、APEC跨境隐私保护规则（CBPR）：旨在通过一套公认的隐私保护准则，允许数据在成员经济体之间自由流动，前提是企业必须通过第三方认证，证明其具备统一且达标的保护能力和问责机制（Accountability）。

二、统一管理的四大实操路径

1、全局安全底座一体化（The Technical Baseline）：跨境企业应采用全球统一的身份认证（IAM）、多因素认证（MFA）和端点监控系统（EDR）。无论员工在深圳、香港特别行政区还是新加坡办公，均接入同一套零信任架构，确保总部SOC对全球资产的实时监控和异常阻断能力。

2、认证驱动的合规对齐（Certification as Alignment）：积极推动企业总部通过APEC CBPR认证或ISO/IEC 27001。CBPR认证意味着企业建立了跨成员经济体的统一隐私标准，成员国监管机构对该认证的认可将大幅降低企业在各地的单独合规沟通成本。

3、数据本地化与逻辑隔离（Physical/Logical Balance）：针对中国等有严格数据本地化要求的地区，企业应采用“物理本地、逻辑统一”的架构模式。即涉及核心业务或敏感数据，优先在本地部署（如私有云、受限租户云），确保不违反当地法律；仅通过受限的、经过安全审计的API实现总部的审计和跨区业务协作。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

4、应急联动的同步化：必须建立全球性的安全事件应急演练。例如，新加坡研发中心的漏洞不仅要报告当地监管局，更要同步给全球SOC，防止攻击利用跨区连接在全网蔓延。

Q85

跨境运营中，企业在处理安全日志传输时通常需遵循哪些数据合规要求？

（撰写人：左李福）

答：

一、核心提要

1.日志留存义务存在显著差异：中国采取强制性留存规则（不少于6个月），日本无明确法定留存义务但关键社会基础设施运营者（CSIPs）须留存以供报告，韩国通过PIPA框架对包含个人信息的安全日志施加实质留存要求，新加坡则要求采取合理安全措施保护数据但无特定日志法定留存期限。

2.跨境传输合规路径呈现“机制多元化”特征：中国采用安全评估、标准合同、认证三轨并行制；日本以“同等保护实体+充分性认定+同意”为核心；韩国实行“明示同意+法定豁免+认证”机制；新加坡遵循“同意+必要传输义务”规则。APEC CBPR认证在亚太地区获得广泛互认，成为企业提升跨境合规效率的重要工具。

3.执法力度持续强化：韩国PIPC自2023年修订PIPA后，行政罚款计算基准改为“实体全部收入”，已开出多起针对国内外企业的跨境数据传输巨额罚单；新加坡PDPA 2025修订强化了数据泄露通知时效（72小时）和数据保护官（DPO）强制化要求；中国2026年1月1日施行的修订版《网络安全法》进一步落实了数据分类分级保护制度及数据出境安全评估等要求，违规处罚力度大幅提升。各法域执法趋严态势明显，企业面临多重合规挑战。

二、专业观察

1.中国：强制性日志留存与数据出境三轨制

2026年1月1日施行的修订版《网络安全法》延续并强化了网络安全等级保护制度。根据该法第二十三条，网络运营者须履行五项安全保护义务，其中第三项明确要求“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”。这一强制性规定意味着在中国境内运营的企业，无论规模大小，均须建立日志记录和留存机制，留存期限最低6个月。

在跨境传输层面，中国形成了“安全评估—标准合同—认证”三轨并行的制度体系。2025年10月出台的《个人信息出境认证办法》（《办法》）标志着三种个人信息出境制度的全面落地。《办法》明确认证机制适用于：不涉及关键信息基础设施运营者、不涉及重要数据、自当年1月1日起累计向境外提供个人信息在10万人至100万人之间（或敏感个人信息不满1万人）的情形。

专业建议：企业在处理安全日志跨境传输时，应首先完成数据分类分级，识别日志中是否包含个人信息（如IP地址、设备标识符）或重要数据。如属此类数据，须根据传输体量和数据性质选择合适的出境路径，并注意在境内指定代表或专门机构以便于监管沟通。

2.日本：宽松的日志留存与灵活的跨境机制

日本的网络安全法律体系以《网络安全基本法》为基本框架，APPI为数据保护核心法律。值得特别注意的是，日本法律并未强制要求留存网络安全日志，仅有针对关键社会基础设施提供者（CSIPs）的信息共享义务。此外，若网络攻击导致或可能导致个人数据泄露，则触发向PPC的报告义务，实践中需留存日志以满足报告要求。根据《刑事诉讼法》，调查机构可要求电信服务提供商留存特定通信记录最长60天。在跨境传输方面，日本作为全球CBPR论坛创始成员之一，其CBPR认证机制已在多国获得互认。获得全球CBPR认证的企业可在日本与其他CBPR成员经济体之间直接进行个人信息跨境传输，无需额外审批。这一机制大大简化了跨国企业在亚太区域内的数据流通合规流程。

专业建议：虽然日本无强制日志留存义务，但从风险管理的角度，建议企业建立完善的日志管理体系，尤其对于处理个人数据的业务场景。考虑申请APEC CBPR/全球CBPR认证，以提升跨境数据传输的合规效率。

3.韩国：严格的域外适用与巨额罚款风险

韩国PIPA是亚太地区数据保护立法中最严格的框架之一，其域外适用范围的宽泛解读令人关注。PIPC于2024年4月发布的指引明确PIPA适用于：向韩国数据主体提供商品或服务、处理行为对韩国数据主体产生重大影响、在韩设有营业场所的外国实体。这意味着即使企业未在韩国设立实体，只要向韩国用户提供服务并处理相关数据（包括安全日志中的个人信息），即须遵守PIPA。

2023年PIPA修订后，行政罚款计算基准从“与违法行为相关的收入”改为“实体的全部收入”（扣除与违法行为无关部分），最高可达全部收入的3%。2025年1月，PIPC在跨境数据传输案件中对Kakao Pay处以59亿韩元罚款，对苹果处以24亿韩元罚款，创下新高。这些案件凸显了PIPC对外国实体跨境数据合规的高度关注。

专业建议：企业在韩国运营或向韩国用户提供服务时，安全日志中的个人信息跨境传输须获得数据主体明示同意（区别于默示同意）。同时，如符合以下任一条件——年营收超过1万亿韩元、日均处理超100万韩国数据主体个人信息、被PIPC要求——须在韩国指定国内代表。

4.新加坡：精细化的技术治理与快速响应

新加坡2025年对PDPA的重大修订聚焦三大核心变革：DPO强制化、数据泄露通知时效化（72小时）、管辖范围全球化。在技术治理层面，新加坡金融管理局（MAS）发布的《金融机构AI风险管理指南》首次要求将PDPA“告知同意”原则嵌入模型训练日志，这一做法代表了从“合规导向”向“技术硬约束”的监管范式跃迁。

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

PDPC于2025年7月对Ezynetic公司的执法案例极具警示意义——因使用“p@ssword1”等弱密码导致近20万条个人数据泄露，被处以17,500新元罚款。此案虽金额不大，但传达了监管的核心关切：企业是否落实了最基本的“合理安全措施”。

专业建议：在新加坡运营的企业应确保日志管理系统的安全性达到“合理安全措施”标准，包括但不限于访问控制、加密存储、定期漏洞评估。建议任命DPO并建立72小时内响应数据泄露事件的应急机制。

三、行动清单

☐ 完成数据分类分级盘点：全面梳理安全日志中包含的数据类型，识别是否涉及个人信息（IP地址、设备标识符、行为轨迹等）或重要数据（系统漏洞信息、安全事件详情等），此为判断各国合规要求适用的前置条件。

☐ 评估各法域日志留存义务差异：针对企业运营所涉及的亚太国家，逐一核实是否存在法定日志留存义务及具体期限要求（如中国要求不少于6个月），确保各地日志管理策略符合当地法律。

☐ 确定跨境传输的合规路径：根据传输数据类型、数量、目的地国家，在中国、日本、韩国、新加坡等国现有的合规机制（安全评估、标准合同、认证、同意等）中选择适用的路径，确保多法域合规路径的协调统一。

☐ 获取必要的用户同意：在日志跨境传输涉及个人信息时，按各国要求获取同意（特别注意韩国要求“明示同意”而非默示同意），并在隐私政策中明确披露跨境传输的目的、接收方及数据保护措施。

☐ 评估APEC CBPR/全球CBPR认证适用性：如企业在多个亚太经济体间频繁传输数据，可考虑申请全球CBPR认证。目前日本、韩国、新加坡等均认可该认证作为跨境传输合规机制，认证后可在成员经济体间直接进行数据传输。

☐ 指定境内代表（如适用）：在中国和韩国运营的外国企业，如满足相关门槛（韩国为年营收超1万亿韩元或日均处理超100万韩国数据主体个人信息），须在当地指定代表机构或代表人员。

☐ 建立数据泄露应急响应机制：确保具备在72小时内（韩国、新加坡）或合理期限内（中国、日本）向监管机构报告数据泄露事件的能力，日志系统应能够支持事件溯源和影响评估。

☐ 保留合规记录以备监管审查：包括跨境传输的同意记录、安全评估报告、标准合同签署文件、认证证书、数据泄露报告记录等，保留期限建议覆盖各国法定的诉讼时效或监管追溯期。



作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q86

在智能制造场景下，各经济体对智能制造数据有哪些特殊监管要求？生产运营数据、设备运行数据与质量数据等通常在何种情况下会被纳入重点监管范围？（撰写人：薛菁）

答：

一、核心提要

APEC框架下数据监管呈现明显的“主权化+分层治理”特征。

中国：以《中华人民共和国数据安全法》为核心，建立数据分类分级制度，通过《数据出境安全评估办法》监管重要数据。

美国：以出口管制（EAR/ITAR）及特定行业网络安全（如CMMC）为主，侧重受控技术与国防相关数据。

日本、新加坡：强调“受信任的数据流动机制”。

关于纳入重点监管的情形：数据通常在涉及国家安全、关键产业（半导体、能源等）、关键信息基础设施（CII）、重要/核心数据分类、或涉及受控技术与大规模跨境流动时进入重点监管范围。

关于数据类别关注重点：生产运营数据关注供应链稳定性；设备运行数据关注控制权与远程运维风险；质量与工艺数据关注技术秘密与知识产权。

二、法规矩阵与专业洞察

合规模块	典型法律/依据	关键要求
中国工业数据监管	《中华人民共和国数据安全法》；《数据出境安全评估办法》、《工业和信息化领域数据安全管理办法（试行）》	建立一般、重要、核心数据分类分级；重要数据出境需开展安全评估。
美国出口与安全监管	Export Administration Regulations (EAR); International Traffic in Arms Regulations (ITAR); Cybersecurity Maturity Model Certification (CMMC) Program	对受控技术数据实施出口限制；在国防采购体系中对承包商数据安全提出分级要求。
数据本地化限制	越南《网络安全法》（Law No. 24/2018/QH14）；Decree No. 53/2022/ND-CP	在特定主体和条件下要求数据本地存储及设立本地机构。
数据共享与流通政策	日本 Data Free Flow with Trust (DFFT)；新加坡 Trusted Data Sharing Framework	推动在可信机制下的数据共享与利用（包括工业与非个人数据）

三、行动清单

□ 建立数据资产地图

明确智能制造场景中的数据类型（生产、设备、质量），并结合所在经济体规则进行分级（如识别重要数据、技术秘密等）。

□ 开展跨境数据合规评估

对涉及跨境传输的数据（如生产配方、设备参数、质量报告），依据适用法律（如中国数据出境规则、美国出口管制）进行预判。

□ 加强关键系统安全控制

对工业控制系统相关数据，实施访问控制、身份鉴别、日志记录、密码保护等技术措施（依据数据分类等级匹配）。

□ 规范第三方与远程运维访问

对境外设备厂商或服务商访问设备运行数据的行为，设置最小权限控制并保留审计日志。

□ 实施数据脱敏与最小化原则

对涉及敏感工艺参数、地理信息或核心技术的数据，在共享或跨境前进行脱敏或降精度处理。

Q87

智能硬件采集用户数据是否需额外披露？（撰写人：何杨）

答：

一、核心提要

注意采集敏感数据需额外披露相关信息、个人信息处理规则须公开展示。

二、法规矩阵与专业洞察

智能硬件采集用户个人信息，除常规隐私政策告知外，针对特定场景必须履行额外、显著、单独的披露及授权义务，各项要求均有明确法律规定支撑，具体内容如下：

1.根据《个人信息保护法》第七条规定，处理个人信息应当遵循公开透明原则，明示处理目的、方式和范围；该法第十七条进一步要求，处理前需以显著方式、清晰易懂的语言，完整告知处理者信息、数据种类、保存期限及用户权利行使途径；《网络数据安全管理条例》第二十一条也明确，个人信息处理规则需集中公开展示、醒目易读。

2.基于同意处理一般信息的，需符合《个人信息保护法》第十四条自愿明确同意的要求，且依据该法第十六条，不得捆绑授权，不得以用户拒绝非必要采集为由拒绝提供基础服务。

3.对于生物识别、医疗健康、行踪轨迹等敏感个人信息，依照《个人信息保护法》第二十九条、第三十条，必须单独告知个人并取得单独同意，同时额外说明处理必要性及对用户权益的影响。

4.开展自动化决策的，需遵守《个人信息保护法》第二十四条，保证决策透明，提供便捷的退出渠道。

5. 采集目的发生变更的，应重新告知并取得同意；向第三方提供个人信息的，应依《个人信息保护法》

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

第二十三条单独告知接收方身份、联系方式、处理目的与方式及信息种类并取得单独同意。欧盟GDPR、新加坡PDPA等亦就采集目的与第三方共享设有相应透明告知义务。

综上，智能硬件数据采集并非仅依托隐私政策笼统告知即可，高风险、非必要、敏感类数据采集，均需单独履行额外披露义务，严守个人信息保护相关法律法规要求。

Q88

跨境电商店铺推荐算法在各经济体通常受哪些监管要求？

（撰写人：薛菁）

答：

一、核心提要

店铺推荐算法通常受四类规则约束：

1）个人信息/画像使用；

2）广告与商业推荐披露；

3）平台对商家的透明与公平；

4）自动化决策或不公平/误导性做法控制。不同经济体侧重点不同，中国偏“算法专门化”，日本偏平台透明与商家公平，美国偏FTC反欺骗执法，新加坡、韩国、澳大利亚更多落在一般数据保护与消费者保护框架内。

进入重点监管的典型触发情形通常包括：

使用个人信息进行画像推荐；影响消费者交易决策的排序或展示；把付费推广伪装成自然推荐；对商家流量分配、搜索排序或上架资格产生实质影响；以及基于完全自动化处理作出对个人有显著影响的决定。

二、法规矩阵与专业洞察

经济体	现行有效官方依据	核心要求
中国	《互联网信息服务算法推荐管理规定》《中华人民共和国个人信息保护法》《中华人民共和国电子商务法》	主要处理个人数据跨境流动中的隐私与责任，不直接规定店铺推荐算法的排序逻辑，但《互联网信息服务算法推荐管理规定》第十六条要求以显著方式告知用户算法推荐服务情况，并公示其基本原理、目的意图与主要运行机制
美国	Federal Trade Commission Act；FTC关于“dark patterns”的官方材料	禁止unfair or deceptive acts or practices；数字广告与推荐中的重要信息披露要清晰显著；不得把广告伪装成自然内容，不得用“暗黑模式”操纵消费者
日本	Act on Improving Transparency and Fairness of Digital Platforms (Tentative translation)	指定平台须披露交易条款及搜索排名显示基本的基本决定事项；并建立投诉处理和争议解决机制
新加坡	Personal Data Protection Act 2012 (PDPA)；	若跨境电商平台用个人数据驱动店铺推荐，通常落入PDPA
韩国	Personal Information Protection Act (PIPA)	个人有权拒绝接受完全自动化处理作出的决定，或要求解释；因此店铺推荐算法如达到“完全自动化处理并产生显著影响”的程度，会进入PIPA规则

三、行动清单

□先识别推荐机制属于哪一类

把店铺推荐区分为自然排序、个性化推荐、赞助/付费推荐、广告投放和评价加权，否则很容易把不同法域下的义务混写。中国法对个性化搜索和自动化决策要求最直接；日本法更关注平台对商家的透明与公平；美国更多是广告/误导问题。

□单独审查“是否使用个人数据画像”

一旦推荐算法使用浏览、点击、交易、位置、设备等个人数据，通常就会进入中国PIPL、新加坡PDPA、韩国PIPA等规则。

□把“广告/付费推荐”与“自然排序”清晰区分。

美国FTC的官方材料都把清晰披露、不得误导作为重点；中国《电子商务法》也要求电商广告遵守广告法。把商业推广伪装成自然结果，是高风险点。

□对商家侧准备一套可说明的排序规则。

日本Transparency Act已明确把“搜索显示排名的基本决定事项”列为应披露示例；中国算法规定也要求公开基本原理、目的意图和主要运行机制。平台至少应能解释核心排序因子和申诉纠错路径。

Q89

各经济体针对物联网设备的无线电认证分别设立了何种监管机制？

（撰写人：王孝冉）

答：

物联网设备的无线电认证（Radio Certification / Type Approval / Radio TypeApproval）是指监管机构或认可的合格评定机构对物联网（IoT）设备进行无线电频谱使用合规性审查和批准的过程，目的是确保设备在合法使用无线电频谱的同时，不会造成有害干扰、电磁兼容问题或健康安全风险。亚太经济合作组织（APEC）共有21个经济体，涵盖澳大利亚、文莱、中国、中国香港特别行政区、中国台北、

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

印度尼西亚、日本、韩国、马来西亚、墨西哥、新西兰、巴布亚新几内亚、秘鲁、菲律宾、俄罗斯、新加坡、泰国、美国、加拿大、智利和越南。物联网（IoT）设备作为无线电频谱的主要使用者，其无线电认证（Radio Certification/Type Approval）是市场准入的核心环节，涉及无线电频谱管理、电磁兼容（EMC）、干扰控制及安全要求。各经济体虽均参与APEC电信设备合格评定相互承认安排（TEL MRA），但仍保留独立的监管机制，以适应本地频谱规划与风险管理需求。

经济体	监管机构	主要认证机制	IoT设备关键要求	备注
澳大利亚	ACMA	SDoC + RCM标记	低风险SRD（Wi-Fi/Bluetooth等）自行符合，无需预先批准	支持e-labeling，与新西兰高度协调
文莱达鲁萨兰国	AITI	强制型式批准（Dealer Type Approval）	所有无线电设备需预先评估（Level 1-3），SRD为Level 1	证书有效5年
加拿大	ISED	混合模式（认证/SDoC）	高风险需列入Radio Equipment List，低风险SDoC	—
智利	SUBTEL	自我声明 + QR码（多数SRD）	2025年起多数SRD转为自我声明（医疗设备除外）基于FCC/CE报告简化	永久有效
中国	MIIT / SRRC	混合模式（SRRC认证 + 进网许可）	IoT无线设备需SRRC认证，部分低风险豁免	—
中国香港特别行政区	OFCA	自愿/强制认证（HKTEC）	多数设备自愿，高功率发射器强制	—
日本	MIC	强制认证/型式批准（Giteki标记）	低功率SRD可能简化或豁免风险分级	—
印度尼西亚	MCDA/ Kominfo	强制第三方认证	所有设备需预先测试+批准QR码标记，无SDoC	—
韩国	MSIT / RRA	混合模式（KC认证/声明）	IoT设备需注册，低风险SDoC	—
马来西亚	MCMC	强制认证（SIRIM批准）	所有设备需批准（计划转向混合模式）	无SDoC
墨西哥	IFT	强制批准	支持MRA，e-labeling	无SDoC
新西兰	RSM	SDoC + RCM/R-NZ标记	按风险级别符合标准，与澳大利亚协调	—
巴布亚新几内亚	NICTA	混合模式（型式批准 + 简化SDoC）		—
秘鲁	MTC	型式批准/同等认证	辐射功率>10mW需批准（基于FCC/CE），低功率豁免，永久有效	—
菲律宾	NTC	Type Acceptance（RCE）	IoT无线设备多为RCE强制认证	—
俄罗斯	Rossvyaz / RFC（EAEU框架）	FAC认证/声明 + RFC结论	结合EAC标记，无线IoT需额外射频合规	—
新加坡	IMDA	混合模式（ESER/SER/GER注册+声明）	IoT设备多为简化注册	—
中国台北	NCC	混合模式（风险分级认证/声明/豁免）	IoT/Smart Home设备需LP0002等标准测试	—
泰国	NBTC	混合模式（设备标准检查与认证）	无线设备需NBTC通知合规	—
美国	FCC	混合模式（Part 15认证/SDoC）	IoT无线设备多为有意辐射器需认证，无意辐射器SDoC	—
越南	MIC	型式批准/合格评定	IoT无线设备需符合EMC/无线标准，部分SDoC（2026年起更新EMC规范）	—

Q90

各经济体如何对电动车数据（电池、定位）进行监管否构成敏感数据？

（撰写人：王孝冉）

答：

电动车（EV/NEV）数据主要包括电池数据（BMS系统中的SOC电量、健康状态、温度、电压、充电历史等技术参数）和定位数据（GPS、行车轨迹、实时位置等）。这些数据通过车联网、App或充电桩收集。APEC经济体中，电动车的定位数据在绝大多数经济体中被视为个人数据，且常被归类为敏感数据（或需更高保护），因其可揭示个人行为、习惯和隐私（精确/连续轨迹尤其敏感）。电动车的电池数据通常为技术/非个人数据（匿名时），但若与VIN、车主、App或位置关联，即成为可识别个人数据；少数情况下（健康推断或生物识别关联）可能被视为敏感。

整体来看，电动车数据主要受各国个人信息保护法/隐私法管辖，强调同意、目的限制、最小化收集、跨境传输安全评估和数据本地化。CBPR为部分成员提供互认框架，但EV数据监管仍以本地法为主，无统一APEC专用EV数据法规。

下面对APEC经济体对电动车数据主要监管措施、在各国是否构成敏感数据列表归纳：

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

经济体	主要监管框架	电池数据监管	定位数据监管	是否敏感数据？（电池 / 定位）	备注
澳大利亚	Privacy Act 1988 (APP)	通用隐私法适用；无强制上报	个人数据（若可识别）；需同意/目的限制	否（技术时）是（习惯揭示时）	位置数据若与个人关联即受保护；EV隐私风险报告增多
文莱达鲁萨兰国	PDPA（有限）	通用隐私法；无EV专用	个人数据	视情况 / 是	执法较弱
加拿大	PIPEDA	个人数据（若可识别）；无强制上报	敏感上下文（位置+习惯）	否 / 是（上下文敏感）	弱于GDPR中国EV数据担忧突出，但统一适用PIPEDA
智利	LPPD (2024年生效 2026 全面实施)	个人数据；敏感数据定义含健康/私密	敏感数据（私生活揭示）	视关联 / 是	新法加强敏感数据保护
中国	PIPL + MIIT NEV数据规定	强制实时上报国家平台（安全监督）；数字ID追溯（2026）；碳足迹报告	强制上报；重要数据/敏感个人信息	技术为主，但关联后是 / 是（精确轨迹为敏感）	最严格；跨境传输需安全评估；重要数据本地化
中国香港特别行政区	PDPO	个人数据	个人数据	否 / 是	与中国内地不同，较灵活
印度尼西亚	PDP Law（新兴）	通用隐私法	个人数据	视情况 / 是	执法发展中；EV基础设施重点
日本	APPI	个人数据；同意要求	个人数据；敏感处理需同意	否 / 是（特殊照顾类可能）	同意严格；跨境转移需同意
韩国	PIPA	个人数据；明确同意	敏感/位置数据需单独同意	否 / 是	全球最严之一；敏感数据高标准
马来西亚	PDPA	个人数据	个人数据	视情况 / 是	同意+目的限制
墨西哥	新联邦个人信息保护法（2025更新）	个人数据；敏感数据加强	敏感处理	视情况 / 是	加强未成年人/科技数据保护
新西兰	Privacy Act 2020	个人数据	个人数据（合理隐私期待）	否 / 是	与澳协调；位置数据受关注
巴布亚新几内亚	数据保护法（新兴）	通用	个人数据	视情况 / 是	有限监管
秘鲁	PDPL	个人数据	个人数据	视情况 / 是	同意+安全义务
菲律宾	Data Privacy Act	个人数据	个人数据	视情况 / 是	GDPR影响
俄罗斯	联邦个人信息法 + 本地化要求	个人数据；本地化	个人数据	否 / 是	国家安全审查严格
新加坡	PDPA	个人数据；同意	个人数据（上下文敏感）	否 / 是	商业友好；EV充电数据适用
中国台北	PDPA	个人数据	个人数据	视情况 / 是	敏感类别明确
泰国	PDPA	个人数据；同意	个人数据	视情况 / 是	执法有限；中国EV渗透高
美国	CCPA/CPRA（州法为主）+ NHTSA	个人数据（CA审查connected vehicles）；无联邦强制	敏感个人信息（精确地理位置）	否 / 是（CCPA明确）	CPPA重点审查EV；联邦安全+州隐私
越南	PDP Law（2025）+ Data Law	个人数据	敏感数据（位置服务）	否 / 是	新法加强；位置/行为监测为敏感

Q91

工业互联网平台的跨境数据流动风险有哪些？（撰写人：何杨）

答：

一、核心提要

注意数据泄露风险、数据违规出境、第三方服务商安全短板。

二、法规矩阵与专业洞察

工业互联网平台承载着研发设计、生产工艺、设备运维、供应链管控等关键工业数据，其跨境数据流动涉及多主体、跨地域、多环节流转，兼具数据安全、合规监管、国家主权、产业供应链等多重风险，事关企业生产经营、产业核心竞争力乃至国家经济安全。

第一，在数据安全与隐私保护层面，跨境传输链路、平台系统漏洞、第三方合作环节均存在安全隐患，极易引发核心工业数据窃取、泄露、篡改与伪造等问题，还会滋生数据非法滥用、商业间谍窃取、勒索病毒攻击等安全事件，同时触碰个人信息跨境保护红线，引发隐私侵权风险。

第二，在合规与法律层面，全球各国数据监管规则碎片化差异显著，数据本地化存储、跨境传输审批、重要数据管控等要求各不相同，叠加境外监管机构长臂管辖、工业重要数据界定模糊等问题，企业极易触

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

犯多国数据监管法规，面临高额行政处罚，同时大幅推高跨境合规管控成本。

第三，在国家数据主权与安全层面，关键领域工业数据属于国家战略数据资源，违规跨境流动会直接威胁关键信息基础设施安全，加剧地缘政治博弈带来的贸易壁垒风险，甚至造成核心技术外泄，削弱国内产业竞争力。

第四，境外云服务商、第三方配套厂商等供应链主体存在安全短板，工业数据标准不统一、平台互操作性不足等技术问题，叠加企业内部数据分类分级管控缺失、跨境治理体系不完善、应急处置能力薄弱等管理短板，进一步放大了跨境数据流动的全链条风险，形成系统性安全隐患。

Q92

各经济体下，AI质检系统产生的数据需要遵循哪些数据保护相关规则？

（撰写人：范晓荧）

答：

一、核心提要

数据本地化与跨境合规：在APEC区域内运营AI质检系统时，核心生产数据与个人信息须本地存储，跨境传输前必须完成安全评估或认证，严禁未经脱敏的原始数据直接出境。

分类分级与匿名化处理：制造业数据需严格分类，涉及员工生物特征或客户信息的应视为“敏感个人信息”；输入AI模型前，必须通过去标识化技术切断数据与特定主体的关联。

供应链责任穿透：企业作为数据控制者承担首要责任，需与第三方服务商签署数据处理协议（DPA），明确责任边界，并确保其具备同等安全保护能力。

二、法规矩阵与专业洞察

监管维度	中国(CN)	印度尼西亚(ID)	新加坡(SG)	美国(US)
核心法律依据	《数据安全法》	《个人数据保护法》(PDP)	《个人数据保护法》(PDP)	核心法律依据
存储与本地化	重要数据本地存储	存储与本地化	重要数据本地存储	存储与本地化
跨境传输机制	安全评估/认证	跨境传输机制	安全评估/认证	跨境传输机制
AI/质检场景规则	训练数据脱敏	AI/质检场景规则	训练数据脱敏	AI/质检场景规则

APEC经济体对制造业AI质检数据的监管呈现“本地存储刚性化、跨境流动契约化、处理过程匿名化”的特征。各法域虽监管侧重不同，但均要求企业在利用AI提升质检效率的同时，确保数据全生命周期的安全可控。

中国的“双重属性”监管：AI质检采集的图像或IoT数据若能关联特定生产线或操作员，即被视为“个人信息”或“重要数据”。企业必须建立“数据出境安全评估”与“算法备案”的联动机制。

印尼的“强本地化”壁垒：印尼PDP法对关键领域的数据出境施加严格限制，外资制造业企业通常需在本地部署私有云或边缘计算节点。

新美“治理导向”：两国不强制数据落地，但要求建立完善的AI治理框架。新加坡强调AI质检结果需有人工复核，美国加州则要求披露是否将数据用于画像分析。

三、行动清单

□ 数据分类分级：梳理AI质检采集的数据，识别个人信息（如操作员ID）及重要数据（如核心工艺参数），建立分类台账。

□ 本地化与脱敏：在受限经济体（如中国、印尼）部署边缘计算节点；输入AI模型前，实施去标识化或匿名化处理。

□ 履行跨境申报：依据所在地法律（如中国的标准合同备案、印尼的政府批准）完成合规手续，严禁擅自传输原始数据。

□ 签署DPA协议：与供应商、云服务商签署数据处理协议，明确数据所有权归属企业，服务商仅为处理者。

□ 建立告知机制：若涉及员工绩效自动化决策，需披露算法逻辑，并提供申诉渠道。

Q93

企业在多个APEC 经济体使用同一智能设备系统，需要满足哪些跨境合规要求？

（撰写人：范晓荧）

答：

一、核心提要

数据分类与分级是前提：在部署智能设备系统前，必须对采集的数据进行分类（如个人数据、重要数据、核心数据）。不同经济体对“重要数据”的定义差异巨大，例如中国对测绘、金融数据有严格本地化要求，而新加坡则侧重于个人数据的保护与流动。企业需建立统一的数据分类标准，以应对不同法域的合规要求。

隐私保护与数据主体权利的协调：APEC经济体普遍采用隐私保护框架，但具体要求不同。例如，欧

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

盟GDPR（虽非APEC成员，但影响广泛）要求数据主体拥有“被遗忘权”，而APEC隐私框架则强调数据的流动与保护平衡。企业需确保智能设备系统能够响应不同法域的数据主体权利请求（如访问、更正、删除等）。

本地化与跨境传输机制的适配：部分经济体（如中国、俄罗斯）要求数据本地化存储，而另一些（如美国、新加坡）则允许自由流动。企业需根据各法域的法律要求，选择合适的跨境传输机制（如标准合同条款、认证、白名单等），并确保智能设备系统的技术架构能够支持这些机制。

二、法规矩阵与专业洞察

经济体	核心法律依据	关键合规要求	数据本地化要求
中国	《网络安全法》 《数据安全法》 《个人信息保护法》	关键信息基础设施运营者（CIIO）需通过安全评估；处理个人信息达到国家网信部门规定数量的需申报数据出境安全评估；重要数据需本地化存储。	严格：重要数据和CIIO的个人信息必须在境内存储，确需出境的需通过安全评估。
美国	《澄清合法使用境外数据法》（CLOUD Act）、各州隐私法（如CCPA）	联邦层面无统一数据跨境法律，但受CLOUD Act影响，政府可要求企业提交境外数据；各州隐私法（如加州CCPA）侧重消费者隐私权利。	无统一要求：但受行业监管（如金融、医疗）影响，特定行业有数据存储要求。
新加坡	《个人数据保护法》（PDPA）	允许数据跨境，但需确保接收国提供与PDPA实质上同等的保护水平；企业需采取合理措施保护数据。	无强制要求：但需确保跨境数据的安全性。
澳大利亚	《1988年隐私法》（Privacy Act）及《隐私修正案（强制性数据泄露通知）法2017》	允许跨境，但需确保接收国提供“实质上同等”的保护；若发生数据泄露，需及时通知受影响个人和监管机构。	无强制要求：但需确保跨境数据的安全性。

三、行动清单

□ 完成数据映射 (Data Mapping)：

根据每个部署智能设备系统的APEC成员经济体的法律要求，建立统一的数据分类标准，识别智能设备系统中涉及的所有数据流，明确哪些数据属于“个人敏感信息”或“重要数据”（参考《GB/T 35273 个人信息安全规范》或当地标准）。

□ 选择合规传输机制：

根据每个部署智能设备系统的APEC成员经济体的法律要求，选择合适的跨境传输机制（如标准合同条款、认证等），并确保智能设备系统的技术架构能够支持这些机制。

□ 启动 APEC CBPR 认证（如适用）：

若业务主要集中在日本、新加坡等CBPR成员经济体，申请加入CBPR体系，以获得跨境数据流动的“白名单”待遇。

□ 实施本地化措施：

针对强制本地化的法域（如中国），建立本地数据中心，或使用本地云服务，确保重要数据不跨境。数据如需回传至境外总部，需通过当地的数据出境安全评估。

□ 建立应急响应机制：

针对APEC成员不同的数据泄露通知时限（如澳大利亚要求72小时，中国未明确规定具体时限但要求“立即”），制定分级响应预案

□ 定期监控与更新：

定期监控数据流动情况，确保持续合规；同时，关注各APEC成员经济体法律的更新，及时调整合规策略。

Q94

APEC主要经济体对IoT产品在当地建立“数据镜像”均设立了何种监管规则？

答：

APEC主要经济体针对物联网产品在当地建立“数据镜像”，一般并没有统一专门规则，而是分别纳入各自的个人信息保护、网络安全、数据本地化和跨境传输监管框架中；实务上最常见的是要求先看镜像数据是否涉及个人信息或敏感数据，再看是否属于基础行业数据、是否需要本地存储或安全审查，以及镜像后的远程访问、集中运维或境外回传是否会触发跨境传输合规义务，因此企业通常不能只把“数据镜像”部署理解为技术问题，而必须按当地数据合规规则整体设计。

Q95

APEC主要经济体对制造业AI项目（如预测性维护）的数据用途披露分别设立了哪些监管要求？逻辑有何差异？　　（撰写人：何杨）

答：

一、核心提要

韩国对高风险AI有更严格的监管要求、其他经济体多为建议披露、在未来各经济体对AI合规立法或更具体。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

二、法规矩阵与专业洞察

APEC 21个成员经济体围绕制造业AI项目（含预测性维护）的数据用途披露，基本以本国现有数据保护立法为核心基础搭建监管框架，同时结合AI应用的特殊性，辅以专项AI监管规则或行业实操指引，确保数据用途披露合规与AI技术创新有序推进。

在APEC 21个成员经济体的AI监管规则体系中，针对个人信息及敏感个人信息场景形成了相对统一的合规逻辑：若制造业AI应用的处理范畴涵盖个人信息乃至敏感个人信息，各经济体普遍要求AI运营主体依法、清晰、明确地披露数据的具体合规用途，切实保障数据主体的知情权、同意权等合法权益，确保数据处理全流程符合合规要求，防范个人信息泄露与滥用风险。

而就非个人信息处理的制造业AI业务场景而言，各经济体的监管要求呈现出差异化特征，多数成员并未针对此类场景设置强制性的专项合规义务。其中，韩国针对高风险Ai单独设定了更为严苛的法定合规流程与管控责任，形成了刚性监管约束，强化对数据用途的全流程监管。而其余APEC经济体如美国，则多采用框架化监管模式，以行业自律指引、合规操作建议等柔性治理方式推行监管要求，未出台统一的强制化合规规范，整体监管尺度更具灵活性与行业自主性，为制造业AI技术的创新应用预留了合理空间。



更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

Q96

如何判断AI模型的数据训练（数据收集和整理、训练）和内容生成是否侵犯版权？（撰写人：孟昕）

答：

AI大模型的广泛应用，正在重塑信息产生的方式与内容创作方式。与此同时对于AI大模型的训练数据以及生成内容引发了很多著作权相关的讨论。

《生成式人工智能服务管理暂行办法》第七条规定，生成式人工智能服务提供者（以下称提供者）应当依法开展预训练、优化训练等训练数据处理活动，遵守以下规定：

（一）使用具有合法来源的数据和基础模型；

（二）涉及知识产权的，不得侵害他人依法享有的知识产权；

（三）涉及个人信息的，应当取得个人同意或者符合法律、行政法规规定的其他情形；

（四）采取有效措施提高训练数据质量，增强训练数据的真实性、准确性、客观性、多样性；

（五）《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律、行政法规的其他有关规定和有关主管部门的相关监管要求。

目前司法实践中关于训练数据未经著作权人许可使用拥有著作权的作品的案例存在较大分歧。

目前司法实践中并没有关于训练数据未经著作权人许可使用拥有著作权的作品统一的判例。理论层面，主要存在以下几种观点：

1.AI在训练、优化训练等训练数据处理活动中使用他人享有著作权的训练素材，属于合理使用，不构成侵权。

2.AI在训练、优化训练等训练数据处理活动中使用他人享有著作权的训练素材是对相关作品思想、规律的统计抽象和特征提取，并非表达性使用，不构成侵权。

3.AI在训练、优化训练等训练数据处理活动中使用他人享有著作权的训练素材，不属于合理使用，相关行为构成侵犯复制权、改编权和信息网络传播权，对于合理使用不应扩大解释。

无论是训练阶段还是输出阶段，AI模型是否构成著作权侵权，仍应遵循"接触＋实质性相似"的传统判断路径，具体分为以下四步：

4.是否构成作品：确认相关内容构成《著作权法》所保护的作品；

5.接触判断：如果作品已经公开发布，通常推定具有接触可能性；

6.实质性相似判断：根据思想–表达二分法判断是否构成实质性相似；

7.抗辩事由：审查是否存在合理使用、法定许可等抗辩事由。

AI模型的合规训练，要在训练数据的收集、整理及模型实际训练各环节均使用具有合法来源或者获得许可的数据，并充分尊重他人依法享有的知识产权。若在上述过程中未经权利人许可，擅自复制、存储或使用受著作权保护的作品，可能侵犯相关权利人的复制权等权利。此外，在内容生成阶段，若AI模型的输出内容与训练数据中的受保护作品构成实质性相似，且能证明或合理推定模型在训练阶段存在对相关作品的"接触"，则可能构成著作权侵权；若相关行为落入法定的合理使用范畴，则可能不侵权。

需要特别提示的是，目前司法实践对于人工智能训练阶段的数据使用以及生成内容的输出，能否适用合理使用抗辩，尚未形成明确且一致的裁判标准，相关规则仍处于发展过程中，存在较高的不确定性。因此，企业不宜将“合理使用”作为当然适用的免责依据或主要抗辩路径，而应基于审慎原则，优先通过取得授权、控制训练数据来源、完善合规机制等方式，主动防范潜在著作权侵权风险。

Q97

Ai模型的数据训练和内容生成侵犯版权，应如何承担责任？（撰写人：韦征）

答：

一、核心提要

处理AI版权侵权需区分“训练输入端（Input）”与“生成输出端（Output）”，责任承担逻辑通常如下：

1.训练输入端（模型开发商/训练主体）：

核心争议：使用受版权保护的作品进行大规模数据挖掘（TDM）是否构成合理使用。

倾向判断：若未经授权使用且未能满足法定例外（如新加坡的计算数据分析异常、美国的合理使用原则），开发者可能面临直接侵权责任。

2.生成输出端（模型服务商/使用者）：

内容归责：当输出内容与受版权保护的作品构成“实质性相似”时，若模型未能提供必要的技术过滤，服务商可能承担间接侵权（或帮助侵权）责任。

用户责任：一般用户若仅为提示词输入者，通常难以直接承担版权责任，除非其主观上诱导模型生成特定侵权内容。

二、法规矩阵与专业洞察

1.APEC成员的监管路径大致分为三类，企业需根据目标市场的法系进行合规评估：

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

监管模式	代表成员	特征与逻辑
明确例外型	新加坡	通过《版权法》引入“计算数据分析（CDA）”例外，允许在符合条件下进行AI训练，降低了开发商的合规门槛。
个案司法驱动型	美国	缺乏统一立法，主要依赖法院在AI版权诉讼中的判例（如实质性相似原则）来界定训练数据的合法性。
专项规制型	中国	通过《生成式人工智能服务管理暂行办法》等规定，要求提供者承担数据来源合规性审查义务，并强调知识产权保护。

2.洞察

(1)“实质性相似”是最终防线：无论训练数据是否合法，若AI输出内容在表达形式上与原作品过于接近，侵权事实极易成立。

(2)合规趋势：区域内正从“野蛮扩张”转向“许可机制”。Adobe、财联社等机构与创作者建立授权池的模式，正成为降低法律风险的主流趋势。

(3)责任链条延长：法规不仅针对开发者，对AI应用的分发平台（如应用商店、云服务商）的“通知–移除”责任要求也在提高。

三、行动清单

针对AI技术开发与应用，建议采取以下防御性行动：

1. 训练阶段（Input Compliance）

建立训练数据集的“溯源档案”，确保数据采集来源合法，剔除明确标明“禁止爬取”或版权存疑的内容。在支持TDM（文本与数据挖掘）例外原则的地区（如新加坡），严格按规定执行，确保不将数据用于非法定用途或向第三方泄露源文件。此外，针对关键语料库，积极探索与版权方达成商业许可协议，以锁定法律确定性。

2. 内容生成阶段（Output Management）

在模型中植入内容过滤机制，通过指纹比对技术监测输出内容是否命中受保护的作品库。同时在服务条款（TOS）中明确版权归属及免责声明，告知用户若利用模型生成侵权内容需承担相应法律后果。另外，可提供生成式AI标识，告知用户输出内容为AI生成，降低因AI冒充人类创作带来的道德风险与法律追究。

3. 争议处理机制

设立专门的版权投诉渠道，快速响应权利人的下架请求（符合各成员经济体的“避风港原则”）。密切关注APEC各成员针对AI法律修订的动向（特别是有关“生成内容版权归属”的立法讨论），及时调整产品策略。

Q98

云端软件及相关服务（即通过网络提供软件功能或技术支撑的服务形态），应如何通过知识产权进行全面保护？

（撰写人：冷勇达）

答：

云端软件所涉及的知识产权主要包括著作权、专利权及商业秘密、商标权。若要实现全面保护，也应围绕这四类权利展开。

（一）计算机软件著作权保护

著作权保护的是代码本身的“表达形式”。根据《民法典》第一百二十三条[《中华人民共和国民法典》第一百二十三条 民事主体依法享有知识产权。知识产权是权利人依法就下列客体享有的专有的权利：（一）作品；]、《著作权法》第三条[《中华人民共和国著作权法》（2020修正）第三条 本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果，包括：（八）计算机软件；]及《计算机软件保护条例》第十四条，软件著作权自开发完成之日起自动产生[《计算机软件保护条例》第十四条 软件著作权自软件开发完成之日起产生。]。我国实行自愿登记制度，登记证书是证明权利归属的初步证据，无须另行举证。侵权认定遵循“实质性相似+接触”原则，通常需对源程序、目标代码及逻辑结构进行比对，判断侵权是否成立。

特别警示：开源协议合规风险。企业必须建立开源代码使用审批和审计机制。务必警惕GPL、AGPL、SSPL等具有‘传染性’的许可证。特别是在SaaS模式下，对AGPL/SSPL协议代码的使用必须极其审慎，因其可能将‘网络使用即分发’认定为触发开源义务的条件，从而要求企业公开整个衍生服务的源代码。建议法务与技术团队联合审查所有代码依赖项。

（二）专利权保护

依据《专利法》第二条[《中华人民共和国专利法》（2020修正）第二条 本法所称的发明创造是指发明、实用新型和外观设计。

发明，是指对产品、方法或者其改进所提出的新的技术方案。]、第二十五条[《中华人民共和国专利法》（2020修正）第二十五条 对下列各项，不授予专利权：（一）科学发现；（二）智力活动的规则和方法；（三）疾病的诊断和治疗方法；（四）动物和植物品种；（五）原子核变换方法以及用原子核变换方法获得的物质；（六）对平面印刷品的图案、色彩或者二者的结合作出的主要起标识作用的设计。对前款第（四）项所列产品的生产方法，可以依照本法规定授予专利权。]，数据处理方法、AI算法、系统性能改进逻辑等可申请发明专利；图形用户界面（GUI）可申请外观设计专利。核心算法应尽早申请发明专利，独创的SaaS交互界面应申请GUI外观设计专利。

（三）商业秘密保护

对于部署在云端、难以反向工程的后端技术，商业秘密保护是有效手段。依据《反不正当竞争法》第

更多免费行业报告 并购家 www.ipoipo.net

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

十条，商业秘密须具备“不为公众所知悉、具有商业价值”并“采取相应保密措施”三个要件。保护对象包括未公开的源代码、数据模型、架构配置及客户名单等。企业必须对内实施权限分级和日志审计，对外签署保密协议（NDA）及竞业限制协议，以满足法定保密要件。

（四）商标权保护

商标保护品牌辨识度，降低获客成本。根据《商标法》第八条[《中华人民共和国商标法》第八条 任何能够将自然人、法人或者其他组织的商品与他人的商品区别开的标志，包括文字、图形、字母、数字、三维标志、颜色组合和声音等，以及上述要素的组合，均可以作为商标申请注册。

产品名称、Logo、服务口号等均可注册。SaaS兼具技术与服务属性，需跨类别注册保护：核心类别包括第42类（SaaS、云计算）、第9类（可下载软件）及第38类（通讯功能）。

Q99

针对算法及模型权重，可采取哪些保护措施，以抵御窃取风险？

（撰写人：孙霖）

答：

一、核心提要

确立以“商业秘密”为核心的法律防御：相比专利或著作权，算法模型权重因其不可读性，最契合商业秘密（Trade Secret）的保护路径。必须满足“秘密性、价值性、保密措施”三要素，以获得 APEC 各成员经济体法律的广泛支持。

构建“技术+合同”的双重隔离带：核心防御不在于单纯的代码加固，而在于对模型访问权限的颗粒度控制，以及与核心研发人员、合作伙伴签署涵盖“算法溯源”条款的深度保密协议。

部署主动式侵权追踪：面对“窃取后洗白”的风险，应在模型中植入“数字水印”或“指纹”，确保在发生数据泄露或被第三方非法商用时，具备法律层面的可追溯性和排他性证据。

二、法规矩阵与专业洞察

1. APEC 主要成员经济体法律要求对比

维度	美国 (USMCA/DTSA)	中国 (反不正当竞争法/算法规定)	新加坡/东盟参考 (APEC 框架)
主要法律依据	《商业秘密保护法》(DTSA)	《反不正当竞争法》及《互联网信息服务算法推荐管理规定》	《商业机密法》及 APEC 隐私/跨境数据流框架
对模型权重的界定	明确视为受保护的商业信息，只要具备商业价值	视为“经营信息”或“技术信息”备案制强化了监管合规	侧重于数据资产的商业机密保护
维度	美国 (USMCA/DTSA)	中国 (反不正当竞争法/算法规定)	新加坡/东盟参考(APEC 框架)
保护核心要求	合理的保密措施 (Reasonable Measures) 是法庭支持的前提	必须证明采取了相应保密措施（如加密、权限管控）	强调“受信任的数据共享”与违约追偿
窃取救济方式	禁令救济、高额惩罚性赔偿。	行政处罚与民事赔偿并重；严重者涉及刑事。	侧重于经济赔偿与恢复名誉。

2. 洞察

在 APEC 框架下，算法和模型权重的法律属性更倾向于——商业秘密。

权重（Weights）的特殊性：源代码可以被混淆，但权重是一系列浮点数。一旦泄露，对方无需理解逻辑即可直接部署。因此，法律层面的“秘密性”认定至关重要。

法规趋势：随着APEC对数字经济（Digital Economy）的重视，跨境执法协作正在加强。这意味着在新加坡泄露的权重，如果在中国或美国被非法使用，通过商业秘密侵权诉讼获取跨境救济的成功率正在提升。

3. 实务案例

案例：A科技公司研发了一款高效图像识别模型，其核心权重被离职员工私自拷贝并提供给竞争对手B公司。

结果分析：若A公司仅签署了通用劳动合同，未对模型权重进行物理隔离（如放在隔离服务器）或逻辑标记（如数字水印），法庭可能认为A公司未尽到“合理保密义务”。

若A公司部署了访问审计日志，并在模型中植入了特定随机扰动的“指纹”，则可确凿证明B公司产品中的权重源自A公司，从而在诉讼中占据绝对优势。

三、行动清单

针对算法及模型权重的防窃取风险，建议落实以下行动：

☐ 资产梳理：将核心算法模型权重列入“特级商业秘密”清单，明确资产边界。

☐ 物理与逻辑隔离：实施内网研发环境与外网物理隔离，禁止使用个人存储介质拷贝模型文件。

☐ 访问控制（IAM）：针对模型仓库实施最小权限原则，所有访问与下载行为需有动态审批和日志审计。

作者
序
目录
APEC数字经济总体环境
APEC数据保护与隐私法规
APEC跨境数据流动
APEC人工智能法律与监管
APEC算法治理与自动决策系统
APEC数字贸易
电子商务与平台经济
APEC网络安全与技术合规
APEC产业应用场景
制造业、IoT、电动车、跨境电商等
APEC知识产权与数字内容

☐ 技术埋点：在发布版模型权重中植入不可感知的数字水印，作为资产权属的“基因证明”。

☐ 法律协议加固：在入职、离职及第三方合作协议中，明确约定“模型权重”属于敏感职务成果，离职后保密义务永久有效。

☐ 模型加密部署：在边缘侧或云端部署时，采用模型混淆、加密壳或 Trusted Execution Environment (TEE) 等硬件加固技术。

☐ 跨境合规审查：若涉及 APEC 成员间的跨境研发协同，需确保数据出境符合当地网络安全法要求，避免因违规操作导致法律保护失效。

☐ 应急响应预案：建立模型泄露应急预案，一旦发现异常流量或市场出现疑似竞品，立即启动证据固定流程。

Q100

企业如何应对海外市场的版权、内容合规投诉？

（撰写人：陆雪儿）

答：

一、核心提要

企业需整合技术工具与法律机制搭建全周期合规架构，覆盖版权登记、内容审核、投诉响应全链路，将风险防控重心由事后处置转向事前预防。

研究属地国避风港规则，通过及时移除侵权内容和合规响应流程降低主体责任风险，平衡合规成本与法律风险。

企业应针对AI生成内容、用户生成内容等新兴内容，结合本土规则与海外版权相关原则，优化内容治理技术，回应前沿立法要求。

二、法规矩阵与专业洞察

司法管辖区	核心法律依据	程序要求	平台责任
美国	DMCA《版权法》	需含侵权链接或描述、权利人法定声明等	通知删除机制为主，合规反通知后平台需24小时内恢复内容
欧盟	《数字单一市场版权指令》欧盟版权指令、人工智能监管体系	成员国需保障72小时内响应时效	主动监管与前置义务强化
澳大利亚	Copyright Act 1968	通知需包含侵权细节与补救要求	反通知后需终止临时禁令

该表从司法辖区维度对美国、欧盟及澳大利亚的版权与内容合规投诉规则进行比较，揭示出不同法域在法律依据、程序要求及平台责任配置上的差异，不同法域呈现出由事后响应向事前控制、由单一通知机制向多层责任体系演进的趋势。企业在应对海外版权与内容合规投诉时，应基于上述差异构建分区域合规策略，重点完善权利证明管理、响应时效控制及平台责任履行机制，从而实现跨境合规风险的系
统性管控。

三、行动清单

☐ 完成核心内容在海外市场的版权登记，固化权利凭证。

☐ 制定并实施严格的内部审核流程，确保所发布内容符合当地法律要求。

☐ 建立快速响应机制以在收到投诉后能迅速采取行动。

☐ 定期进行法律风险评估，识别潜在风险点并制定应对策略。

☐ 记录投诉处理过程并定期评估合规策略的有效性。

更多免费行业报告 并购家 www.ipoipo.net

编后记

这套蓝皮书的缘起，其实很简单：太多出海的企业，带着相似的困惑找到我们——“这个行业我们能不能在当地百分之百控股？”“数据能不能传回国内？”“被列入实体清单该怎么办？”问题具体而琐碎，却往往关乎生死。我们由此意识到，比起体系庞大的教科书，出海企业更需要一部能随手翻到答案的“手边书”。于是，有了“问答”这一体例。从选题到成稿，数十位深圳律师、公司法务、高校研究员以及境内外法律界专家学者历时数月，字斟句酌，拒绝纸上谈兵，力求“查明”到位，只为让读者读到的，是可以信赖的答案。

我们要特别致谢：感谢深圳市福田区司法局、深圳市律师协会、中共深圳市福田区律师行业委员会的悉心指导，感谢深圳市律师协会福田区律师工作委员会、深圳市律师协会国际交流与合作工作委员会、深圳市律师协会福田区律工委国际与港澳台中心、河套国际法律查明中心搭建的平台，感谢每一位在本职工作之余伏案执笔的法律界同仁，也感谢为我们答疑释惑的境内外专家与合作伙伴。这本书的每一页，都凝结着集体的心血。

我们也必须坦诚：法律是流动的。数字与人工智能领域的规则日新月异，亚太各国的立法、判例与执法口径亦在不断更新。尽管我们已尽最大努力核实每一处细节，仍难免挂一漏万，甚至存在有待商榷之处。期待未来能与各位业界同行在更多场合，共同见证与探讨相关领域的最新发展。

法治，是最好的营商环境；专业，是最稳的出海底气。谨以此蓝皮书，献给每一家在亚太乘风破浪的中国企业，也献给每一位以专业为舟的法律人。

路虽远，行则将至。

FT亚太涉外法治丝路计划

《亚太数字经济与人工智能法律问答指南（蓝皮书）》编委会

二〇二六年八月