Open Journal of Legal Science 法学, 2026, 14(1), 73-81
Published Online January 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.141010

Hans汉斯

跨境数据流动安全评估的整改机制

谭晓毅

澳门科技大学法学院，澳门

收稿日期：2025年11月28日；录用日期：2025年12月11日；发布日期：2026年1月8日

摘　要

数字经济已深度融入经济社会各领域，数据跨境流动成为产业发展的重要支撑，但安全风险与合规挑战并存。我国已建立数据出境安全评估制度，为数据跨境流动提供合规保障，但实践中部分企业因整改机制操作指引模糊，面临问题描述笼统、修改方向不明、反复提交等低效困境，不仅增加企业合规成本，也制约了数据要素的自由流动。本文结合企业实操经验，借鉴澳大利亚相关制度实践，聚焦整改机制的优化路径，构建兼具针对性、可操作性与协同性的整改方案，以期平衡数据安全监管与数字经济发展需求，为数字时代高质量发展提供制度支撑。

关键词

数据跨境流动，数据出境安全评估，整改机制，企业合规

Rectification Mechanism for Security Assessment of Cross-Border Data Flow

Xiaoyi Tan

Faculty of Law, Macau University of Science and Technology, Macau

Received: November 28, 2025; accepted: December 11, 2025; published: January 8, 2026

Abstract

The digital economy has been deeply integrated into all sectors of the economy and society. Cross-border data flows have become an important pillar for industrial development, yet they are accompanied by concurrent security risks and compliance challenges. China has established a security assessment system for data outbound transfers, which provides compliance safeguards for cross-border data flows. However, in practice, due to the vague operational guidelines of the rectification mechanism, some enterprises are plagued by inefficient predicaments such as ambiguous problem descriptions, unclear revision directions and repeated submissions. These issues not only increase

文章引用: 谭晓毅. 跨境数据流动安全评估的整改机制[J]. 法学, 2026, 14(1): 73-81.
DOI: 10.12677/ojls.2026.141010

enterprises' compliance costs, but also restrict the free flow of data as a key factor of production. Drawing on enterprises' practical experience and relevant institutional practices in Australia, this paper focuses on the optimization paths of the rectification mechanism and constructs a targeted, operable and collaborative rectification scheme. It aims to balance the needs of data security supervision and digital economy development, so as to provide institutional support for high-quality development in the digital era.

Keywords

Cross-Border Data Flow, Data Outbound Security Assessment, Rectification Mechanism, Corporate Compliance

1. 引言

随着全球化和数字化的发展，数据跨境流动越来越频繁。中国近年来出台了一系列数据安全相关的法律法规，比如《网络安全法》《数据安全法》《个人信息保护法》和《数据出境安全评估办法》(以下简称“《评估办法》”)等等，并建立数据出境安全评估、个人信息保护认证、标准合同等制度。其中《评估办法》第四条明确了四类需申报类型，要求对重要数据和达到一定量级的个人信息的跨境流动进行安全评估。[1]然而，现有安全评估机制在实践中面临多重挑战。截至 2025 年 3 月，国家互联网信息办公室收到各省、自治区、直辖市网信办报送的数据出境安全评估申报项目后依法决定是否受理，共完成数据出境安全评估项目 298 个，其中，44 个申报项目涉及重要数据，评估结果为不通过的 7 个，不通过率为 15.9%；44 个申报项目涉及 509 个重要数据项，评估后准予出境的重要数据项为 325 个，占申报数据项总数的 63.9%，复评通过率不足 10% [1]。在这个申报过程中，有不少企业因申报材料不完善或不合格被退回要求整改。当前我国数据跨境流动安全评估的整改机制在实践中呈现出程序框架明确但操作指引模糊的特征，企业因合同条款等申报材料不完善被退回整改时，普遍面临问题描述笼统、修改方向缺失、反复提交低效的困境，加重了企业合规成本和负担，阻碍数据跨境流动，影响业务的开展。因此，建构有效的整改机制是确保法律实施与兼顾数据安全和经济发展的关键。

本文通过分析当前安全评估制度的整改流程和要求，结合我国企业合规实践，借鉴澳大利亚的数据治理经验，旨在提高评估整改的透明度、适配度和高效性。而将数据安全纳入国家安全体系，研究整改机制如何平衡安全与发展，有利于为总体国家安全观提供微观支撑。通过研究优化整改机制，有利于提升评估整改效率，降低企业的合规成本，确保数据在跨区域流动的合规性与可控性，为我国在数字时代的高质量发展提供坚实保障。

2. 文献综述

本文要解决的核心问题是跨境数据流动安全评估整改中，如何破解问题描述笼统、修改方向缺失、

[1]《数据出境安全评估办法》，国家互联网信息办公室令第 11 号，2022 年 7 月 7 日发布，第 4 条规定：“数据处理者向境外提供数据，有下列情形之一的，应当通过所在地省级网信部门向国家网信部门申报数据出境安全评估：(一) 数据处理者向境外提供重要数据；(二) 关键信息基础设施运营者和处理 100 万人以上个人信息的数据处理者向境外提供个人信息；(三) 自上年 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；(四) 国家网信部门规定的其他需要申报数据出境安全评估的情形。”

反复提交低效的实践困境，构建兼具监管合规性与企业实操性的整改机制。现有研究主要围绕安全评估制度的构建、实施与优化展开探讨。在安全评估制度的整体研究方面，大部分国外学者对限制跨境数据流动持消极态度，如 Nigel Cory 提出数据本地化是一种错误观念和虚假承诺，其不能提供更好的数据隐私安全，反而会破坏网络安全。还提出应避免设置毫无意义或武断的白名单，因为监管机构无法维护其完整性或可信度，导致白名单随着时间的推移往往会退化为灰名单[2]。国内学者对于跨境数据流动监管规则的研究聚焦于研究我国应构建何种跨境数据监管模式。而整改机制作为安全评估制度中的配套监管机制，整改机制会直接影响到安全评估的标准、要求、总体耗时以及最终结果等，所以从学者们对安全评估制度的评析中可知学者对评估整改方面存在两种不同的态度，既有以风险导向的角度论述评估整改的重大意义和影响，支持“宁严勿宽”从而保护数据安全。以洪永淼、张明、刘颖为代表，认为跨境数据安全评估的核心是防范国家安全与公共利益风险，明确核心数据、重要数据的界定标准等方式构建评估机制[3]。而其它大多以合规与效率平衡的角度认为当前评估整改的机制设计会使企业的成本增加，耗时过长，影响企业开展业务，阻碍数据畅通。黄现清驳斥将数据作为传统资源如石油进行严格管控的理论，我国所采取的严格的管理方式限制了数据跨境流动，主张数据跨境流动应当在“自由流动”与“安全流动”之间寻找平衡[4]。现有研究聚焦评估制度，明确了评估的核心指标和监管框架，但对评估后的整改实施、流程优化、争议解决等事后闭环环节关注不足，即使部分研究提及整改，也仅将其作为评估制度的附属环节简要带过，未深入分析整改机制的操作逻辑和实践困境，更未对整改机制优化的核心问题提出解决方案。

在安全评估制度的专门研究方面，主要从数据评估标准界定、评估流程的时效、企业合规成本以及执法者的监管成本的角度研究该项制度的流程。丁晓东认为当前评估制度对数据标准界定十分泛化，缺乏精准评估会导致评估者“宁严勿宽”，造成不必要的评估和安全的反噬[5]。重要数据的界定标准不清可能导致企业把重要数据当成一般数据而遗漏申报或评估部门把一般商业数据宽泛解释成重要数据使得数据安全评估落入封闭、静态的安全认知陷阱。洪延青认为安全评估是当前主要的数据出境合规路径，采取事前审批和一事一议的模式与国际实践有很大的差异，会存在评估时效长、标准不清、流程和评估标准不透明等问题[6]，这些困境都会导致企业无法顺利通过数据评估，会被要求尽快整改，整改不当影响企业的正常业务开展，甚至违法违规面临行政处罚。丁伟、倪诗颖认为国内数据立法纷繁复杂，具体的操作流程混乱，数据安全评估的内容过多，加重了企业数据合规的成本[7]。大型企业或许可以通过专业的数据合规团队来解决风险评估问题，而正在兴起的中小企业要提高数据合规效率和降低合规成本成为数字企业发展的又一大难题。李凡认为当前制度执行设计上围绕数据本身构建会存在执法成本高难度大、数据处理者违法成本低难度小的难题，不利于长期持续有效的数据监管[8]。也即广且严的评估整改制度只适合于探索之初，需尽快调整。多数观点认为单一监管模式难以平衡安全与效率，尝试引入合作治理理论优化治理框架，强调监管机构、企业、第三方机构等多元主体平等协商、资源互补、协同共治，如由第三方参与评估和精准界定重要数据可提升企业合规效率，明确网信办主导、第三方支撑、企业自主合规的各主体职责等。周念利等提出对有高需求数据出境的企业而言，申报同类数据的频率较高，高频申报会造成合规成本较高，对于有大量跨境业务的企业高频申报没有简便处理方式([9], p. 2)，统一化的评估标准和整改要求对企业合规整改能力提出了很高的要求。对此，学界提出应用敏捷治理理论，即以快速响应、动态适配为核心，契合数字经济时代数据流动的动态性、创新性特征，如以出境评估门槛和同主体同类数据高频出境为分类标准，未达到此标准的通过签署标准合同或个人信息保护认证来出境数据，达到此标准的则需安全评估，但自贸区可建立白名单制度，采取事前备案和事后监管的监管机制并进行定期或不定期的抽查监督；以及应快速反馈，及时公布评估结果，慎用“禁止出境”这一评估反馈等([9], p. 3)。现有研究对安全评估制度的具体内容和方式指出了问题并提出相应的建议，合作治理、敏

捷治理理论应广泛用于跨境数据治理的整体框架研究和地方试点尤其是自贸区的实践中，已为解决多元参与主体冲突提供了理论基础和为跨境数据治理的高效性提供了思路，但未针对跨境数据提出整改设计方案，应用场景聚焦宏观环节而非整改实操，也未解决导致企业合规难以通过的反馈模糊、方向不明、反复低效的问题。这一研究缺口正是本文核心研究切入点，将合作治理、敏捷治理的理念融入至整改机制设计，尝试构建多元主体协同协商、流程动态优化、问题精准回应的方案。

3. 跨境数据流动整改机制的实践现状与困境

(一) 法律框架

《网络安全法》《数据安全法》《个人信息保护法》三部上位法的生效，初步确立了我国跨境数据流动的基本规则，即个人信息和重要数据本地化储存，而部分数据跨境流动必须进行安全评估。《评估办法》细化了这一规定，明确重要数据和达到一定量级的个人信息出境必须进行申报评估。同时，该《评估办法》第七条规定了省级网信部门材料完备性查验的职责以及国家网信部门作出受理决定并书面通知数据处理者的义务。[2]在省级网信部门查验数据处理者提交的申报材料前，数据处理者还需完成风险自评估报告。其中，在风险自评估环节和省级网信部门的材料完备性查验环节中均会涉及企业整改问题，企业自行查漏补缺而可能进行“盲人摸象”式整改，各地省级网信部门做法不一也可能因上级政策抽象笼统而理解不一致，也可能因趋于保守态度而对企业言辞含糊，导致企业的整改效率低下。《评估办法》第十一条和第十二条规定的是关于国家网信部门要求数据处理者补充或更正申报材料的程序，[3]这其中也会涉及国家网信部门通过补正合格材料的方式要求企业进行整改方可顺利出境。《评估办法》第十四条和第十七条规定了数据处理者的因有效期届满或情况变更时应当重新申报评估的义务 [4]，这其中明确规定了企业如需继续开展数据出境活动，必须按照要求整改，整改完成后重新申报评估，在评估过程中同样也会再次经历不符合要求的整改。在数据出境过程中，企业会遭遇来回反复的整改，以致最终耽误了跨境业务的发展。《评估办法》第二十条规定了该办法施行前已出境但不符合规定的数据活动应当在施行后六个月内完成整改 [5]。目前该部分企业的整改成效并未公开，是否像正在申报数据出境的企业一样陷于问题描述笼统、修改方向缺失、反复提交低效的整改困境并不清楚。从上述现行法律法规的概述中可知我国数据跨境流动安全评估的程序框架比较明确，但对企业合规整改的操作指引确实是模糊的，以致许多企业不是处于观望状态，就是承受着较高合规成本投入的负担。

(二) 实践现状

通过公开渠道查询到截止 2023 年 12 月 15 日，成功通过数据出境申报包括国家网信部门的审批或备

[2]《数据出境安全评估办法》第 7 条规定：“省级网信部门应当自收到申报材料之日起 5 个工作日内完成完备性查验。申报材料齐全的，将申报材料报送国家网信部门；申报材料不齐全的，应当退回数据处理者并一次性告知需要补充的材料。国家网信部门应当自收到申报材料之日起 7 个工作日内，确定是否受理并书面通知数据处理者。”。

[3]《数据出境安全评估办法》第 11 条规定：“安全评估过程中，发现数据处理者提交的申报材料不符合要求的，国家网信部门可以要求其补充或者更正。数据处理者无正当理由不补充或者更正的，国家网信部门可以终止安全评估。数据处理者对所提交材料的真实性负责，故意提交虚假材料的，按照评估不通过处理，并依法追究相应法律责任。”第 12 条规定：“国家网信部门应当自向数据处理者发出书面受理通知书之日起 45 个工作日内完成数据出境安全评估；情况复杂或者需要补充、更正材料的，可以适当延长并告知数据处理者预计延长的时间。评估结果应当书面通知数据处理者。”

[4]《数据出境安全评估办法》第 14 条规定：“通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：(一) 向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；(二) 境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；(三) 出现影响出境数据安全的其他情形。有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前重新申报评估。”第 17 条规定：“国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。”

[5]《数据出境安全评估办法》第 20 条规定：“本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。”

案的企业有 29 家，与国家网信部门和各地省级网信部门已经受理的千余件数据申报项目相比，数据出境申报的通过率仅为百分之一[10]。在评估结果为通过的这些企业中，其申报过程也并不是一帆风顺。例如，拜耳(中国)有限公司在向境外传输临床试验和药物警戒数据会涉及敏感个人健康信息和重要数据，对企业数据合规体系建设提出了高要求。这是生物医药领域数据出境经常面临的数据合规难题，而拜耳公司要整改的痛点可能就有数据分类复杂、合同条款缺失、跨部门协调等，所以为了整改评估成功，其不仅需要将混合的基因数据、患者隐私信息和科研数据采用匿名化处理和区块链技术明确区分个人信息和重要数据，还需要优化合同约定境外接收方数据泄露的应急回应机制和赔偿责任，甚至需要政策协同，利用北京自贸试验区的绿色通道机制，实行相关部门的联合预审，最终才能顺利出境数据，成为全国首个外资生物医药企业数据合规出境的案例[11]。而作为数据跨境电商领域标杆的焦点科技股份有限公司在向境外传输用户订单数据、物流信息以及 AI 模型训练数据时也同样面临数据类型混杂、技术措施不足、合规成本高的整改痛点。该企业通过采用隐私计算技术在境内完成模型训练后仅输出模型参数至境外、部署专用跨境传输通道、建立自动化合规申报系统、委托第三方机构分类分级数据等方式升级技术和优化流程[12]。上述整改措施无不涉及技术应用和部门协调，对于财力雄厚的大型企业而言是一笔不菲的时间和经济投入，但对于同样有数据跨境业务需求和面临整改的中小型企业而言则是可望而不可及。

(三) 问题聚焦

综上，我国跨境数据流动安全评估的整改机制主要存在的问题是过于严格和广泛的整改监管模式不仅对作为监管者的网信部门还是作为数据处理者的企业而言都是高初始投入且高持续成本，不利于数据产业的可持续发展。网信部门对企业数据合规的评估整改指引模糊主要体现在合同条款修改指引中的整改标准模糊、跨部门解释冲突以及条款动态更新指引缺位。相对地，企业在整改过程中也会面临问题定位难、材料补充难、时间成本高、沟通管道不畅等问题。

由于安全评估整改流程看似明确，但操作空间仍留有很大的空白。网信部门由于肩负维护国家安全和国家利益的职责，所以在提出整改要求时通常会采取保守的评估态度，以致将许多有数据出境需求的企业阻挡于外。比如，网信部门发送的整改通知常以条款不完善、风险防控不足等笼统表述退回材料，通知中并未说明需参照哪项技术标准或行业惯例，企业需自行参照生效法去推测，亦或是需通过多次沟通或第三方机构协助才能明确具体的量化标准。其中可能会多次修改反复提交仍未通过，企业与评估部门的沟通也依赖线下，缺乏实时反馈，整改耗时极长。甚至企业需补充的材料可能涉及商业机密或跨境获取难度较大时也没有变通采取替代解决方案。还有医疗跨境数据等特殊行业数据需同时满足多部门的法律法规，但不同部门之间对某一概念的解释可能存在冲突，企业需反复协调。甚至数据接收地的法律政策发生变更时，企业需自行修改合同条款以符合新要求。这些情况均由企业去承担成本和风险，其实过于强硬的整改监管模式并不利于维护数据产业的生态平衡，对企业释明的透明度、根据企业的自身情况提出整改要求的适配度、指引企业整改的效率并不高。

4. 可供借鉴之澳大利亚经验

我国跨境数据流动的评估整改机制目前在实践中存在透明度和适配度不高、低效性的问题，企业会面临问题描述笼统、修改方向缺失、反复提交低效的困境。严格统一的监管整改模式导致企业的合规成本高、监管资源消耗过大，且整改方案与企业实际业务场景适配性不足。目前学界关于跨境数据流动的研究大多集中在欧盟与美国的制度，而澳大利亚在数据跨境流动立法方面是较为中立的国家，既遵循国际组织的原则，又有其独到的经验，较为符合欧盟认可的数据跨境流动标准([13], p. 5)。相比之下，澳大利亚在数据评估中的协商式整改模式为解决此类问题提供了新思路，其构建了监管机构与企业的合作型治理关系，为破解我国监管刚性有余、弹性不足、透明度欠缺的困境提供了创新视角。

作为英美法系中注重监管实效的代表，澳大利亚并未采取欧盟立法严、执法刚的规则主义数据治理模式和美国市场化的数据监管机制，而是通过《隐私法》(Privacy Act 1988)构建了以协商为核心、以合规为目标的整改机制，形成了监管威慑与合规激励并存的治理平衡，这对我国平衡数据安全与产业发展具有特殊参考意义。正如学者陈永怡、孟彦辰指出“澳大利亚对健康医疗数据跨境流动的严格限制条件在一定程度上保护了该类数据的安全，但是过于严苛的本地化措施同时也在一定程度上阻碍了健康数据跨境流动带来的效益，且健康数据流动的风险并未完全消除。澳大利亚国内也认识到了过于严苛的个人数据保护所引发的问题，并在最近几年的司法判决中有所变化”([13], p. 6)。

在法律框架层面，《隐私法》是澳大利亚隐私保护的主要法律框架，与其他具体领域的法律共同构成了澳大利亚隐私和数据保护的全面法律体系。《隐私法》赋予专员一系列隐私监管权力，《隐私权监管行动政策》则解释了澳大利亚信息专员办公室(OAIC)的监管行动以独立性、问责制、相称性、一致性、及时性和透明度为原则，隐私评估包括基于风险的评估和基于合规性的评估，[6]基于风险的评估侧重于识别实体，根据相关立法如隐私原则向海外接收方披露隐私风险，所确定的隐私风险应直接与实体的一般合规义务相关，OAIC 可根据隐私风险评估结果提出建议来协助实体改善隐私做法和程序；基于合规性的评估的重点是确定数据披露实体是否遵守了已确定的立法义务或来自 OAIC 的明确指示，主要结果将是评估该实体是否符合或不符合相关立法下具体确定的义务，或 OAIC 之前向该实体提出的明确要求。评估类型将根据具体情况来确定([13], p. 6)。澳大利亚的协商式整改元素主要体现在 OAIC 投诉处理流程中的可强制执行的承诺。基于《2014 年监管权力(标准条款)法》(Regulatory Powers Act 2014)第 114 条 [7]规定，专员有权接受相关实体作出的书面承诺，并可在法院对被申请人执行，承诺内容主要包括采取特定行动以遵守《隐私法》、补救任何违规行为造成的损害如向个人道歉或赔偿、承诺某些未来合规措施如审查审计、人员培训以及实施合规监控和报告等。可执行承诺的具体适用于被申请人与专员发起的调查、数据泄露事件调查或 OAIC 进行的隐私投诉。在具体操作过程中，首先考虑提出可执行承诺的可能性，OAIC 必须评估承诺是否为此事提供适当的监管结果，或替代监管结果是否更合适。开始谈判承诺条款后，专员会考虑多项因素，包括承诺条款的要求、受隐私违规影响的个人利益、OAIC 采取执法行动的目标以及指导监管决定和行动的原则等。最为重要的是被申请人通常被要求提名一名负责监督承诺合规并向 OAIC 报告的书面代表，还要与 OAIC 协商聘请具有适当经验和资格的独立第三方审查行为或做法并就改善被申请人对《隐私法》的合规性提出建议。其中《隐私法》第 40 条明确规定了专员发起调查中的违规通知和整改协商权 [8]，其监管权力包括允许 OAIC 与企业合作以促进法律合规和保护隐私的权力，以

[6]Guide to privacy regulatory action, Office of the Australian Information Commissioner, https://www.OAIC.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action.

[7]Regulatory Powers (Standard Provisions) Act 2014, §114. Acceptance of undertakings “ 1) An authorised person may accept any of the following undertakings: (a) a written undertaking given by a person that the person will, in order to comply with a provision enforceable under this Part, take specified action; (b) a written undertaking given by a person that the person will, in order to comply with a provision enforceable under this Part, refrain from taking specified action; (c) a written undertaking given by a person that the person will take specified action directed towards ensuring that the person does not contravene a provision enforceable under this Part, or is unlikely to contravene such a provision, in the future. 2) The undertaking must be expressed to be an undertaking under this section. 3) The person may withdraw or vary the undertaking at any time, but only with the written consent of an authorised person. 4) The consent of an authorised person is not a legislative instrument. 5) An authorised person may, by written notice given to the person, cancel the undertaking.”

[8]Privacy Act, Act No. 119, 1988, §40A. Conciliation of complaints “1) If: (a) a complaint about an act or practice is made under section 36; and(b) the Commissioner considers it is reasonably possible that the complaint may be conciliated successfully; the Commissioner must make a reasonable attempt to conciliate the complaint. 2) Subsection (1) does not apply if the Commissioner has decided under section 41 or 50 not to investigate, or not to investigate further, the act or practice. 3) If the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must, in writing, notify the complainant and respondent of that matter. 4) If a notification is given under subsection (3), the Commissioner may decide not to investigate, or not to investigate further, the act or practice. 5) Evidence of anything said or done in the course of the conciliation is not admissible in any hearing before the Commissioner, or in any legal proceedings, relating to complaint or the act or practice unless: (a) the complainant and respondent otherwise agree; or (b) the thing was said or done in furtherance of the commission of a fraud or an offence, or the commission of an act that renders a person liable to a civil penalty.”

及在发生隐私侵犯的情况下使用的调查和执法权力，OAIC 在此权力安排下拥有双重身份，既是执法者，又是“合规教练”，其首选的监管方法是促进自愿遵守隐私义务，并与企业合作以确保能最大化保护隐私安全以及防止隐私泄露。例如，当个人或组织向 OAIC 提出隐私投诉时，OAIC 首先会尝试通过调解来解决纠纷。调解过程中，OAIC 会与投诉人和被投诉实体进行沟通，促进双方达成协议，以解决隐私问题。如果调解成功，被投诉实体可能会承诺采取一系列整改措施来纠正其隐私违规行为，这些承诺通常会形成书面协议。OAIC 会监督实体的履行情况，确保其按照承诺进行整改。如果调解不成功，OAIC 可能会启动正式调查程序。在调查和执法阶段，OAIC 也可能与被调查实体进行协商，以达成整改协议。OAIC 可以接受被调查实体的可执行承诺，要求其采取特定措施来纠正违规行为。调查结束后，OAIC 可以做出决定，要求相关实体采取整改措施，如果相关实体不遵守决定，OAIC 可以采取进一步的执法行动，对严重或不配合的违规行为，OAIC 会采取严厉的高额处罚，澳大利亚临床实验室(ACL)案则是一个足以震慑企业的鲜明例子。

这种协商式整改机制强调合作与合规，有助于减少法律程序的复杂性和成本，旨在鼓励企业主动纠正违规行为，同时保护隐私安全。与我国现行整改机制相比，澳大利亚的协商式整改在以下方面具有借鉴意义。第一，在透明度方面，OAIC 会定期发布报告，公开其监管活动和调查结果，以提升透明度。OAIC 年度报告强调其监管目标是促进合规而非单纯惩罚违规[14]，其官网开设合规协商资源中心，提供操作手册、视频教程和常见问题解答，贯彻合规伙伴理念，构建服务型监管形象。OAIC 对模糊的监管标准会发布数据评估指标解释，将抽象标准转化为可量化指标。第二，在高效性方面，OAIC 对合作的需整改实体优先采用可执行承诺，可设立 3-6 个月的整改观察期，允许企业因技术迭代、业务变化申请方案调整，还会通过引入第三方机构进行整改效果评估，加快问题解决，总体上既节省监管资源又提高合规效率。在 CII[9]的过程中，专员还会寻求有关各方合作。同时，OAIC 定期进行进度评估并提供合规工具包如数据分类指南模板，面对新兴技术的挑战，澳大利亚目前也在推动技术驱动的合规评估创新，探索使用新的监管工具和评估方法。第三，在适配性方面，可强制执行的承诺允许企业和监管机构互动协商，提出整改方案或替代措施来达到合规要求，促使企业迸发积极性，激励其提出适合自身企业规模和能力的措施，但绝不可低于法定要求。

但需注意，由于法律体系的差异和监管资源的约束，在本土化应用时需谨慎调整，比如我国成文法体系要求具体的整改依据不同于澳大利亚可使用衡平原则灵活解释法律，所以可在《数据安全法》和《评估办法》的实施细则中增设“协商整改特别条款”，明确监管机构可在法律框架内与企业协商约定具体合规措施。另外，不同于澳大利亚的人企情况，我国企业数量众多，全面推行一对一协商可能导致监管超载，所以可以对大中型企业实施深度协商，小微企业提供标准化智能化协商合规助手，分层实施降低监管成本。

5. 跨境数据评估的协商式整改机制构建

澳大利亚的协商式整改经验表明，分层协商可实现初始投入和可控的持续成本，通过柔性监管和多方协作，可在保障数据安全的同时促进产业经济发展。虽然这种整改模式可能会有监管力度不足、缺乏统一标准导致不公平、监管机构的工作效率低、企业可能拖延整改等批评意见，但是对于我国目前刚性有余、弹性不足的数据评估监管模式而言，仍存在合作沟通使整改计划更具可操作性、企业对整改目标和措施的认识清晰会更积极主动提升整改效率、充分表达企业诉求能保护企业利益、灵活适应数据行业

[9]CII是“Commissioner Initiated Investigations”的缩写，中文通常指“专员发起调查”。在澳大利亚隐私监管的背景下，CII指的是由OAIC的专员主动发起的调查，而不是基于个人投诉或外部转介启动的调查。专员发起调查通常涉及可能对个人隐私有重大影响的事件或行为，这些事件或行为可能没有通过常规的投诉渠道被报告。OAIC可能会通过媒体报导、公众关注、其他监管机构的转介或自身监控活动等方式发现这些潜在问题，并决定启动CII。

的发展变化等有利影响。

因此，我国可在透明度、适配度、高效性等方面优化现有的严格统一的评估整改模式，适当融入协商整改的元素，允许企业和监管机构协商提出整改方案或替代措施来达到合规要求。首先在监管标准方面，制定跨境数据评估指标的操作细则，允许企业在协商中提出个性化指标计算模型。其次在动态调整方面，可尝试合规信用评分方式，将协商整改表现与企业跨境数据白名单、税收优惠、信用积分等评判标准挂钩。再次在跨部门协调方面，明确跨境数据评估的主导监管机构，建立跨部门协商的一票否决协调机制，整改方案需经多部门联合听证。最后在高效性方面，我国可建立数据合规公共服务平台，通过政府购买服务方式为中小企业提供协商整改的第三方技术支持和方案设计服务等。

提出澳大利亚协商式整改机制并非简单复制其协商程序，而是构建监管弹性和法律刚性相统一的跨境数据治理模式。我国可以在《评估办法》中修订引入协商整改的前置程序，若企业在数据安全评估过程中触发了协商机制的启动条件如安全评估报告指出整改问题、企业对评估结论有异议及申请复核、监管机构发现整改不到位时要求重启等情形，企业可提交整改申请和相关数据材料，由第三方专业机构参与评估和审核材料，明确问题边界，继而监管机构组织多方包括企业、技术专家、法律顾问在内的协商会，明确整改标准，拟定整改方案尤其是适配企业的修改方向和时间节点，对于一般问题，由监管机构和第三方评估机构多数同意即可；对于重大问题如核心数据跨境整改，则须多方一致同意并由监管机构最终审批。若企业承诺执行的整改方案未通过则需重新协商。在整改方案通过并实施整改时，监管机构需全程跟踪，最后由第三方专业机构出具整改验收报告以及监管机构进行复核。验收通过后，监管机构需及时公示除涉及商业秘密以外的整改评估结果。此外，还应建立风险等级与协商深度相适配的整改机制，比如高风险场景强制协商、中风险场景可选协商，低风险场景快速整改。同时，依托全国监管平台开发利用在线协商板块，将澳大利亚的线下磋商会转型升级为智能合约式的协商系统，实现评估整改方案的算法辅助生成与自动合规校验。将合作治理和敏捷治理的核心理念融入评估整改机制，最终形成具有中国特色的数据协商整改治理模式。

在政府、市场与社会这三角关系的数据治理下，经澳大利亚的经验证明，通过构建监管者、被监管者以及第三方相互协作的协商机制，能够有效破解传统跨境数据监管中的“信息不对称”与“治理失灵”问题，有利于完善我国以政府主导、企业主责、社会协同为原则的数据治理体系，推动数据监管范式从对立博弈转向合作共治。

参考文献

[1] 中央网络安全和信息化委员会办公室网. 数据出境安全管理政策问答[EB/OL]. https://www.cac.gov.cn/2025-04/09/c_1745906286623776.htm, 2025-04-09.

[2] Cory, N. (2023) Comments to Attorney-General’s Department Regarding Australia’s Privacy Act Review. Information Technology & Innovation Foundation. https://itif.org/publications/2023/04/03/comments-to-attorney-generals-department-regarding-australias-privacy-act-review/

[3] 洪永淼, 张明, 刘颖. 推动跨境数据安全有序流动引领数字经济全球化发展[J]. 中国科学院院刊, 2022, 37(10): 1418-1425.

[4] 黄现清. 数字贸易背景下我国数据跨境流动监管规则的构建路径[J]. 西南金融, 2021(8): 74-84.

[5] 丁晓东. 数据跨境流动的法理反思与制度重构——兼评《数据出境安全评估办法》[J]. 行政法学研究, 2023(1): 62-77.

[6] 洪延青. 中国数据出境安全管理制度的“再平衡”——基于国家间数据竞争战略的视角[J]. 中国法律评论, 2024(3): 201-212.

[7] 丁伟, 倪诗颖. 数字贸易视野下我国跨境数据监管的发展困境及合作治理[J]. 北京邮电大学学报(社会科学版), 2023, 25(1): 67-76.

[8] 李凡. 商业数据跨境流动的规范重塑及合规治理[J]. 中国流通经济, 2023, 37(5): 71-80.

[9] 周念利, 于美月, 柳春苗. 我国自贸区(港)数据跨境流动试点制度创新研究[J]. 国际商务研究, 2023, 44(4): 86-97.

[10] 清华大学互联网产业研究院网. 数字产业观察丨每周要闻[EB/OL]. https://www.iii.tsinghua.edu.cn/info/1030/3893.htm, 2023-12-15.

[11] 大兴自贸办. 北京市数据出境“绿色通道”首家试用企业数据出境全部获批[EB/OL]. https://open.beijing.gov.cn/html//daxing/gzdt/2024/5/1715563660840.html, 2024-05-13.

[12] 南京自由贸易试验区. 跨境电商领域 + 数据安全, 全国首个案例落地[EB/OL]. https://njna.nanjing.gov.cn/zmq/zmqdt/202305/t20230519_3915596.html, 2023-05-22.

[13] 陈永怡, 孟彦辰. 澳大利亚健康医疗数据跨境流动法律规制研究及其对中国的启示[J]. 中国全科医学, 2024, 27(25): 3091-3099.

[14] Office of the Australian Information Commissioner (2024) OAIC Annual Report 2023-24. https://www.oaic.gov.au/__data/assets/pdf_file/0025/243592/OAIC_Annual-Report-2023-24_Digital.pdf