企业数据跨境安全合规指引

2024

中国信息协会信息安全专业委员会
中国网络安全产业联盟数据安全工作委员会
安恒信息技术股份有限公司

版权声明

前言

在全球数字经济蓬勃发展的今天，数据掌控力已成为全球数字经济的竞争重点，跨境数据流动成为各国关注热点。我国陆续发布实施了《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》等法律法规，确保国家安全和个人隐私得到充分保护的前提下促进数据跨境流通。

在国际化背景的大趋势下企业出海已成为企业发展战略选择，以拓宽市场、分散风险并获取新的增长动力。随着企业出海业务的增加，数据跨境活动日益频繁，如何确保企业数据跨境流动的合规合法是企业出海必须面对的重要问题。

本报告聚焦企业在全球化背景下的数据安全需求，通过分析数据跨境的风险、合规要求和典型案例，为企业提供数据跨境安全合规指引，确保在国际市场中的合规和安全运营。

第1章分析企业在出海过程中数字化的需求，利用大数据、人工智能、云计算、物联网、工业互联网等数字化技术，企业能够更精准地分析市场趋势，优化供应链管理，提高运营效率。伴随而来的数据跨境风险亟需应对，通过案例展示不合规和安全问题对企业带来的巨大影响。

第2章简要介绍国外数据跨境管理要求。通过分析美国、欧盟、日韩及新加坡等主要经济体的数据跨境流动法规，为企业提供不同地区的数据合规指引。

第3章详细介绍我国数据跨境安全管理要求，阐述数据出境安全评估、个人信息保护认证、个人信息出境标准合同等合规路径的实施细则，为企业提供合规运营实操指南。

第4章介绍我国自贸区在数据跨境流动先试先行实践，北京、上海、粤港澳大湾区等地区通过数据出境负面清单、提供数据跨境服务等措施，探索便利化的数据跨境流动安全管理机制。这些实践帮助企业在特定地区、特定行业满足数据跨境合规处理。

第5章通过典型场景分析，如敏感数据流通、供应链安全、网络攻击防护等，提出应对这些场景的安全策略，帮助企业识别潜在的风险点，并采取有效措施保障数据安全。

第6章提出数据跨境安全保障综合方案，强调合规监管、数据安全服务平台以及隐私计算技术的应用。这为企业在数据跨境流动过程中提供了系统化的安全解决方案。

第7章总结企业在数据跨境合规与安全的重要性，提出建立“政市企”多层服务机制、加快数据跨境基础设施建设、强化安全措施等建议，为企业在全球数字经济中安全高效地跨境运营提供明确的指引。

在编写本报告的过程中，得到了众多专家、学者和业内人士的指导和帮助。在此表示衷心感谢。同时欢迎广大读者提出宝贵意见和建议，以不断优化和完善报告内容。

目录

CONTENTS

企业数据跨境安全合规指引

2024

第一章
企业出海与数字化需求

企业出海趋势

在全球化从市场扩张转向深度融合和创新驱动的背景下，中国企业的全球化发展不仅仅是将产品和服务输出到国外市场，更是在全球范围内整合资源，优化价值链，以提升效率和竞争力。虽然全球化为企业提供了增长机遇，但也带来了复杂的国际环境挑战。例如，各国的政策法规差异、地缘政治的不稳定、文化差异以及供应链的风险，成为我国企业出海时面临的主要障碍。

随着数字技术与产业变革加快推进，各国积极推进数字化转型，对数字贸易开放发展的规则环境与监管协调提出更高要求，数字贸易规则成为国际经贸规则重构和各方博弈的焦点。国务院发展研究中心2023年9月发布的《数字贸易发展与合作报告》显示，全球数字贸易发展新态势表现为跨境数字服务贸易继续保持增长、附属机构数字服务贸易持续调整、跨境电商进入相对缓慢增长阶段。2022年，全球数字服务贸易规模为3.82万亿美元，同比增长3.9%，ICT（信息通信技术）服务继续领跑细分数字服务贸易增长，区域数字服务贸易增长出现分化，跨国公司数字领域投资保持较快增长。

企业出海行业特点

近年来，越来越多的中国企业积极布局海外市场，寻求更广阔的发展空间。特别是高科技、制造业、互联网、新能源和汽车等领域的企业，海外营收和占比有了显著的提升。通过跨国并购、海外研发中心的建立、国际营销网络的扩展等方式，实现了产品和服务出海，提升海外市场的竞争力。

信息技术企业

随着信息技术的不断发展，伴随企业出海过程，云计算、大数据、人工智能等企业信息技术服务市场也逐渐走向全球，成为其中的重要组成部分。

在国际市场拓展方面，华为和中兴通讯是中国信息技术行业的杰出代表。华为凭借其在5G技术、通信设备和企业解决方案领域的领先优势，成功进入了欧美、亚洲和非洲多个国家的市场。公司通过建立全球研发中心、与国际运营商合作及投资海外市场，稳固了其全球通信解决方案的市场地位。中兴通讯通过提供全方位的通信设备和服务，与多个国家的电信运营商建立了合作关系，并在全球市场中占据了一席之地。阿里巴巴通过其云计算平台不断扩展国际业务，并在亚洲、欧洲和美国等地建立了多个数据中心。腾讯通过其全球化战略，尤其在游戏和社交平台领域，通过收购、投资及合作，拓展其在海外市场的影响力。这些企业利用技术创新和全球网络布局，成功提升了在国际信息技术市场的竞争力。腾讯云通过与当地企业的合作，快速进入东南亚、北美和欧洲市场。在大数据和人工智能方面，百度、讯飞等通过其人

工智能平台，向全球客户提供智能语音、图像识别等服务。

伴随数字化转型的加速，企业服务市场将迎来更多机遇。信息技术创新帮助企业推出更加先进和多样化的服务产品。同时，通过与国外企业深度合作，提升服务质量和客户满意度，增强国际市场的竞争力。

金融科技企业

金融科技产业涵盖了移动支付、在线贷款、财富管理、保险科技等多个领域。我国企业在这些领域通过技术创新和商业模式的输出，迅速扩大了国际市场份额。

在移动支付领域，金融科技巨头如蚂蚁集团和腾讯金融科技，通过支付宝和微信支付等产品，在东南亚、欧洲和北美市场迅速普及。蚂蚁集团与多个国家的本地支付服务提供商合作，提升跨境支付的便利性和普及率。腾讯金融科技则通过微信支付在日本、韩国和东南亚等地取得显著市场份额，提升了中国移动支付产品的国际影响力。

在网络贷款领域，陆金所和拍拍贷等企业通过大数据和人工智能技术，为海外市场提供便捷的在线贷款服务。陆金所通过与东南亚和非洲的本地金融机构合作，推出适应当地市场需求的贷款产品。拍拍贷则在拉丁美洲市场推出了一系列针对中小企业和个人的贷款服务，帮助解决传统金融体系难以覆盖的借贷需求。

在财富管理领域，蚂蚁财富和腾讯理财通等平台在全球范围内提供多元化的财富管理产品。蚂蚁财富通过与国际知名金融机构合作，引入全球优质理财产品，满足海外用户的投资需求。腾讯理财通则通过其强大的社交平台，向全球用户推广个性化的财富管理服务，提升了财富管理平台的国际影响力。

在保险科技领域，众安在线和水滴互助等企业在保险科技领域取得了显著成果。众安在线通过其自主研发的保险科技平台，向海外市场输出创新的保险解决方案。水滴互助则在东南亚和印度市场推广其互助保险模式，帮助更多用户获得便捷、低成本的保险服务。

随着5G技术和人工智能等新技术的普及，金融科技产业将迎来新的发展机遇。通过技术创新，推出更多具有国际竞争力的金融科技产品。同时，通过对当地市场的深度了解，进一步提升产品和服务的多样性和可靠性，增强国际市场的影响力，并为全球金融科技产业的发展注入新的活力和动能。

电商和零售企业

我国电商企业如已经成为全球电子商务市场的重要参与者。通过技术创新和商业模式的输出，这些企业在全球多个国家和地区建立了自己的电商生态系统。

在国际市场拓展方面，阿里巴巴通过全球速卖通等平台进入欧洲、俄罗斯和拉丁美洲市场，提供便捷跨境购物服务；京东通过与国际品牌合作、物流网络扩展及投资海外电商平台，在东南亚和欧美市场建立稳固业务基础。两家公司利用强大供应链和技术创新拓展全球电商版图。

此外，拼多多和 Shein 等新兴电商平台在全球市场增长强劲。拼多多积极布局跨境电商业务；Shein 以低价快时尚模式在欧美市场崛起，成为全球快时尚重要玩家。同时，华润万家等中国零售企业通过并购和国际合作在亚洲和欧美地区扩大影响力，推动中国零售品牌全球化进程。

随着全球电子商务市场的不断扩大，将面临更多发展机遇和挑战。通过提升物流和供应链管理能力，提供更加优质的用

户体验，电商企业有望进一步巩固和扩大国际市场份额。例如，通过大数据和人工智能技术的应用，精准分析消费者需求，提供个性化服务，提升客户满意度和忠诚度。

医药和生命科学企业

我国医药企业在医药研发、医疗设备和健康管理等方面进展显著，正逐步向全球市场拓展。

在医药研发方面，华海药业、复星医药、恒瑞医药、石药集团、药明康德和百济神州等企业通过仿制药、创新药物研发和全球市场布局，在欧美市场表现突出。它们通过并购、合作和自主研发获得国际认证，积极参与全球医药产业链，在癌症治疗、仿制药及合同研究服务等领域赢得全球市场份额。

在医疗设备方面，迈瑞医疗和联影医疗通过提供高质量、价格合理的医疗设备，赢得全球客户信任。迈瑞医疗产品已销往全球 190 多个国家和地区，联影医疗通过创新技术提升国际市场竞争力。

随着全球医疗需求不断增加，医疗企业应发挥好本土产业链、研发和技术创新优势，推出更多具有国际竞争力的产品和服务。同时，通过加强知识产权保护，提升自主创新能力，增强在国际市场的竞争力和影响力。

智能制造企业

以智能制造、绿色制造和服务型制造为代表的新型制造模式企业，通过技术创新和产业升级，积极参与全球产业链的竞争。

围绕智能制造，海尔和美的通过引入智能制造技术，提升了生产效率和产品质量。在海外设立生产基地和研发中心，增强了国际市场的竞争力。

围绕绿色制造，远景和宁德时代是绿色制造的代表企业。远景通过其全面的新能源解决方案，成为全球领先的绿色制造企业。宁德时代则通过提供高性能的电池产品，赢得了全球电动汽车厂商的青睐。

围绕智能硬件，小米、传音在智能手机领域成绩显著。安克创新、科沃斯等在智能电子领域展现强劲增长联发科技提供系统芯片(SoC)解决方案的公司，服务于全球移动通信和智能设备市场。

全球对环境保护和可持续发展愈加重视，绿色制造和智能制造将成为主流。企业可以通过技术创新和产业升级，推出更加智能、环保和高效的制造解决方案。并且通过参与全球产业链的分工与协作，提升在国际市场的竞争力。

汽车企业

汽车制造和汽车科技企业通过技术创新和产业升级，逐步在全球市场占据重要地位。比亚迪和蔚来是电动汽车领域的代表企业。比亚迪通过其高性能的电动汽车产品，赢得了全球消费者的青睐。蔚来则通过其创新的电池换电技术和智能驾驶系统，成为全球电动汽车市场的重要参与者。此外，汽车科技领域也取得了显著的进展。百度通过其自动驾驶技术，向全球汽车厂商提供智能驾驶解决方案，帮助汽车厂商实现智能化管理和控制。

全球对新能源汽车和智能驾驶技术需求仍在不断增加，汽车与汽车科技企业将迎来更多机遇。通过技术创新和国际合作，推出更加先进和环保的汽车产品和技术解决方案，企业将进一步提升在国际市场的竞争力和影响力。

企业出海区域特点

一般来说，企业出海的目标市场包括发达国家和新兴国家。发达国家如北欧、西欧、日本、韩国及澳大利亚等地，普遍拥有完善的法律制度和发达的基础设施，且消费者购买力强，市场秩序规范。这些因素虽然为企业提供了良好的市场环境，但也意味着更高的准入门槛和激烈的市场竞争。在这些地区，企业必须提供高质量、具创新性的产品和服务，才能满足当地消费者对品质的严苛要求。此外，进入这些市场的过程中，企业必须注重与当地合作伙伴的协作，并确保自身运营符合相关法律规范，展现出强大的国际化运营能力和适应不同文化与市场的本地化策略。

在“一带一路”战略的背景下，新兴市场如东南亚、中东、南亚及中南美洲变得更加具有吸引力，尽管这些地区的产业基础相对薄弱，政策法规存在不稳定性，但“一带一路”倡议的推动为这些国家和地区提供了新的发展机遇。该战略通过推动基础设施建设、加强区域经济合作和促进贸易往来，极大地改善了新兴市场的投资环境，为企业在这些地区的拓展创造了良好的条件。此外，这些市场的经济增长迅速、人口红利显著，市场潜力巨大，吸引了大量企业，尤其是中小企业，前往投资和拓展业务。

对于中小企业而言，新兴市场竞争相对较少，“一带一路”带来的政策支持为其提供了难得的机会。企业在进入这些市场时，除了要注意本地化战略的实施，还需利用“一带一路”提供的国际合作平台，与当地政府、行业组织及相关企业建立紧密的合作关系，通过双赢的合作模式，提升市场占有率。通过积极参与当地的基础设施建设和产业链整合，企业可以不仅利用政策优势，更能借助区域合作带来的市场扩展机遇，获得政策优惠和资金支持，提升自身的竞争力。

无论是进入竞争激烈的发达国家，还是选择潜力巨大的新兴市场，企业都必须具备清晰的市场定位、深刻的本地化理解和灵活的运营策略，全面分析目标市场的消费者行为、市场动向和竞争环境，从而制定科学合理的市场进入与发展计划。同时，企业还需综合评估自身资源配置的能力、国际化团队的建设水平，以及跨境运营中的风险管理体系，以确保全球业务的稳健发展和长期持续性。这些准备工作是保障企业在全球化进程中减少风险、提高成功率的关键，在新市场中建立稳固的业务基础，并实现长期的可持续发展。

企业出海安全挑战

企业出海面临诸多风险与挑战，包括不同国家的法律与合规要求（如数据保护、税务、劳动法等）、文化差异带来的市场适应难题、供应链管理中的不确定性，以及复杂的跨境数据流动和安全风险。

市场准入和法律风险

企业出海面临不同国家的政策法规环境，包括税收法、劳动法、环境保护法等，企业需要投入大量时间和资源来熟悉并遵守这些法律法规。

一些国家设置了外国企业市场准入门槛，例如技术标准、认证要求、行业规范等，要求企业符合相关标准才能进入市场。此外，国际贸易政策的不确定性，如关税政策的变动、贸易协定的重新谈判以及反倾销等问题，都可能影响企业的海外经营。

供应链风险

企业在海外面临的供应链挑战包括物流成本控制、供应链的稳定性和效率、以及适应当地的供应链管理规则。海外市场的远距离物流和复杂的关税体系可能导致成本增加和运输延误。企业需要建立健全的供应链网络，保证原材料供应和产品的及时交付。在遇到国际贸易摩擦、自然灾害等不可控因素时，供应链的灵活性和应急管理能力也是企业成功的关键。

供应商的选择和管理直接影响到产品质量和供应稳定性。在海外市场，企业需要寻找可靠的供应商，建立长期合作关系。有效的供应商管理可以确保生产线的稳定运行，满足市场需求。全球范围内的政治、经济和自然风险增加了供应链的不确定性。例如，贸易战、自然灾害和政治动荡可能影响到供应链的运转。企业需要制定有效的风险管理策略，包括多元化供应商来源、建立紧急响应机制等，以应对各种不可预见的风险事件。

随着数据在业务运营和决策中的关键角色日益凸显，数据同时成为供应链管理中的重要环节。通过信息技术数字化建设，企业能够实现供应链的全面优化和智能化管理。数字化技术如物联网、大数据分析和人工智能，使企业能够实时监控物流运输、预测市场需求、优化库存和供应计划，从而降低成本、提高效率、加强供应链的灵活性和响应能力。数据驱动的供应链管理不仅提升了运营效率，还帮助企业更快速地适应市场变化和客户需求，从而在竞争激烈的全球市场中保持竞争优势。

全球化运营挑战

企业在全球化发展的过程中，跨文化、跨区域的全球运营将是全新的挑战。信息技术部门作为现代企业运营的数字化基石，需要做好当地技术人员管理、全球团队建设、运维管理等多个方面的保障。

为支持全球业务发展，企业在不同国家和地区建立技术团队，面临诸多挑战。企业在海外市场的品牌认知度和吸引力较弱，海外市场的薪酬水平和福利待遇差异，都会导致招聘高素质信息技术人才的挑战，特别是在技术要求较高的领域。由于在文化、工作习惯和沟通方式上存在差异，要求企业管理者具备较强的跨文化沟通和管理能力。远程工作和全球协作需要依赖高效的协作平台和技术工具，如视频会议系统、项目管理软件和即时通讯工具，确保团队成员之间的信息沟通和项目进展的透明度。

运维管理是中国企业全球化过程中面临的又一大挑战。全球网络架构和数据安全是关键问题。不同国家和地区在网络安全法规和数据保护政策上存在差异，企业需要在遵守当地法律法规的同时，确保全球信息技术系统的安全和稳定运行。例如，不同国家和地区对数据跨境流动和存储提出了严格要求，企业需要制定合规的运维策略，防止数据泄露和安全事件的发生。企业需要建立跨国的运维支持团队，提供24/7的技术支持和服务，确保全球各地用户的技术问题能够及时响应和解决。这不仅要求运维团队具备高水平的技术能力，还需要在全球范围内建立高效的服务网络和响应机制。

企业出海数字化需求

数字化平台建设

在数字化技术推动下，企业出海正在经历从劳动密集型、资本密集型的产品出口到技术驱动型、思维创新型、品牌先导性的升级之路。业务模式的数字化转型与数字化平台建设可以帮助企业应对全球运营的复杂性和不确定性。

首先，企业在全球多个市场运营时，数字化平台能够帮助企业实时监控和管理分散的业务点。通过统一的数字化系统，企业可以高效整合各区域的运营数据，优化资源配置和运营效率。其次，供应链的稳定性是直接影响企业全球扩展的重要因素，特别是在多变的国际环境中。数字化平台能够对供应链进行实时监控，预测潜在风险，保障供应链的连续性和稳定性，从而帮助企业应对全球范围内的物流和生产调度问题。再次，在出海过程中，文化差异和市场需求的不同使得产品和服务的本地化设计成为必须。通过数字化平台，企业可以深入分析各地的市场数据，快速调整营销策略和产品设计，以更好地适应本地市场。最后，数字化平台通过大数据分析和人工智能技术，为企业提供深度的市场洞察和预测，帮助管理层在全球市场中做出更加精准的决策，快速响应市场变化，提升竞争力。

推动企业出海数字化转型，能够简化跨境业务流程。通过整合利用全球资源，如公有云、SaaS服务及供应商的解决方案，企业能够轻松进行跨境支付和签订电子合同，从而降低交易成本并缩短交易时间。此外，数字化供应链管理可以让企业实时监控物流动态，优化库存管理，减少供应链中断的风险。通过云计算和大数据分析等数字化平台，企业不仅能增强数据处理能力，还能实现灵活的资源配置，确保业务的连续性以及应对市场突发变化的能力。

数字化不仅能够帮助企业提升运营效率、降低成本，还为企业提供了创新的商业模式和新的增长机会。借助数字化手段，企业能够在全球范围内构建更具竞争力的业务架构，加速国际化进程。同时，数字化为企业带来了更多的业务拓展可能性，进一步推动了企业全球化战略的实现。

通过数字化平台，企业能够实现全球市场的在线营销、客户服务和数据分析，更好地了解和满足不同国家和地区消费者的需求。长期主义要求平台持续投入和更新，以应对市场变化和技术进步，同时建立信任和稳定的客户基础。国际化战略则要求平台支持多语言、多货币支付和地域化内容管理，以提升用户体验和市场适应性。因此，海外数字化平台不仅是企业全球化战略的执行工具，更是推动长期发展和市场扩展的重要驱动力。

数字化互联互通

针对中小型企业出海数字化建设，优先采用IT“轻资产”模式，采用公有云服务和软件即服务(SaaS)的模式，将业务系统和数据部署在海外市场的本地云平台上，从而快速响应当地的业务需求。这种模式的灵活性在于按需使用的特性，企业可以根据实际需求随时启动或关闭服务，实现“即开即用”的便捷，从而快速适应市场的变化，优化成本结构，并最大化业务的敏捷性。

利用公有云和SaaS 服务，企业还能够借助这些服务商在海外各地区的合规能力，保障信息安全，同时享受到持续的技术更新和维护，降低对本地信息技术支持的依赖，使企业能够以更加高效和成本效益的方式在国际市场竞争和成长。

数字化的核心目标需要确保海外与国内业务之间的无缝连通性，保障数据的安全互联互通，以及实现高效的跨境团队协作和沟通。远程员工需要一个安全的连接通道，帮助企业强化网络安全，同时简化了企业总部信息技术部门的管理工作。对云服务和云上应用采用零信任访问控制，确保只有经过验证和授权的用户才能访问敏感数据，进一步加强企业数据的安全性和保障业务连续性。

数字化供应链管理

随着企业的出海成长，在海外设立办公室、研发中心贴近当地的消费者，或通过建设或并购等方式扩展当地生产能力。在此阶段，信息技术基础设施的建设和优化显得尤为关键。

信息技术部门需要与业务计划同步，确保数字化基础能够支持海外业务的顺畅运行。这包括系统的快速部署和交付，以及日益严格的运维标准。信息技术系统的稳定性直接影响到日常业务和供应链的数字化流程，也意味着海外扩张之路是否坚实。因此，构建一个具有弹性的信息技术架构至关重要，以便能够迅速适应业务的发展需求。关键在于确保连续性和可靠性，特别是在海外环境中，一旦发生问题，应对和修复的时间窗口可能非常有限，因此需要保持可预期的运维能力。

这时建议采用云网融合的数字化架构，企业可以最大化利用各项资源。这个架构需要在满足安全合规要求的同时，提供稳定的网络连接，强化了管理和运维效率。为全球分布的员工群体带来了高效的协同工作能力，使团队协作无论距离远近都能畅通无阻，极大提升工作效率和企业的整体竞争力。

在海外拓展阶段，打造好数字化供应链的基础，企业可进一步整合全球资源，实现规模效应和协同效应，提高运营效率，增强全球市场的响应速度和创新能力。最终，通过这样的全球化战略，企业不仅增强了自己的国际竞争力，也促进了全球市场的互联互通与经济一体化。

数据跨境风险与案例

在企业出海过程中，数据安全是一个不容忽视的问题。大数据环境下，数据高度汇聚，跨境数据泄露风险增大。同时，平台跨境数据接口的多样性和复杂性使得安全风险暴露面大幅增加。在数据出海数据活动中，确定数据的流通流向以及追踪其使用轨迹变得异常困难，而数据跨境主体的多元性和流程的复杂性进一步导致安全责任的划分变得模糊不清。人工智能等新技术新应用的引入为数据安全带来了新的风险和挑战。此外，出海数据资产的梳理工作变得尤为复杂，出海数据分类分级标准的统一也面临诸多困难，这使得跨境主体在面临出海数据时，不得不面对更大的数据风险。

隐私泄露风险。大数据环境加大了用户隐私泄露的风险。一些敏感数据的所有权和使用权并没有明确界定，基于大数据的分析未考虑到其中涉及的个人隐私问题。在数据采集、存储、传输、处理过程中无法有效保护个人隐私，大数据的智能化应用也会增加商业信息和政府敏感信息泄露的风险。大数据环境中多源数据的汇聚，通过数据之间的关联更容易获得隐私信息，增加隐私泄露威胁。

存储安全风险。海量和多源异构数据的集中存储，对大数据分析平台提出了更高要求，对海量数据的处理，以及大规模的分布式数据存储和集群管理。数据大集中的后果是复杂多样的数据存储在一起，很可能会出现将某些生产数据放在经营数据存储位置的情况，致使企业安全管理不合规。数据存储管理安全防护措施难以保护复杂多样的大数据存储，容易造成数据失窃和篡改。

数据基础设施风险。数据基础设施是大数据安全运行的基础，防止攻击者通过非授权访问、在网络基础设施传输过程中破坏数据完整性、造成信息泄露、拒绝服务攻击、网络病毒传播等方式对数据基础设施造成安全威胁。随着基础设施和网络节点数的增加，网络安全风险增大，攻击者利用传输协议的漏洞进行数据窃取、数据拦截。

网络攻击风险。大数据技术容易成为黑客的攻击手段，通过最大限度地收集和关联分析得到更多有用信息，大数据分析使黑客的攻击更加精准。大数据成为高级可持续攻击的载体。传统的检测是基于单个时间点进行的基于威胁特征的实时匹配检测，而高级可持续攻击（APT）是一个实施过程，无法被实时检测。利用大数据发起僵尸网络攻击，可能会同时控制上百万台傀儡机并发起攻击。大数据的价值低密度性，使得安全分析工具很难聚焦在价值点上，黑客可以将攻击隐藏在大数据中，给安全服务提供商的分析制造很大困难，误导安全防护目标信息提取和检索的攻击，导致安全监测偏离应有方向。

长臂管辖合规风险。全球数据跨境流动和数据监管未形成统一，由于各国国情和各种因素的差异，立法框架仍存在差异，导致数据跨境企业可能受到双重法规限制。从全球范围来看，长臂管辖对数据全球数据流通正产生重大影响。例如，欧盟《通用数据保护条例》（GDPR）规定，任何向欧盟境内的数据主体提供商品或服务并涉及个人数据处理的公司所收集的信息均受欧盟管辖。为此，数据处理国通过数据立法进一步应对长臂管辖的影响。我国《数据安全法》规定“非经中华人民共和国主管机关批准，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华人民共和国境内的数据”，《个人信息保护法》规定“非经中华人民共和国主管机关批准，个人信息处理者不得向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息。”。

数据违规处罚案例

企业在全球化扩展时必须优先考虑合规性，特别是在跨境数据传输和用户数据处理方面，以避免高额罚款和信誉损失。Facebook（Meta）、Amazon、Google等全球科技巨头都因不同程度的违规行为遭受了巨额罚款，凸显了数据合规的重要性。

1. Facebook/Meta-2.65亿欧元（2022年，爱尔兰数据保护委员会）

在2022年，爱尔兰数据保护委员会对Meta（Facebook母公司）罚款2.65亿欧元。该事件涉及用户的个人数据被非法抓取并泄露给第三方，包括超过5亿用户的电话号码和其他个人信息。爱尔兰数据保护委员会认定Facebook未能采取充分的技术和组织措施来保护用户数据，违反了GDPR的相关规定。

2. Facebook/Meta-10亿欧元罚款威胁（2023年，欧盟隐私监管机构）

Meta在2023年面临了巨额罚款，可能高达10亿欧元，原因是其违反GDPR规定，继续将欧洲用户的数据传输至美国。欧洲数据保护委员会认定Meta未遵守欧洲对数据跨境传输的隐私保护要求，此案进一步凸显了跨境数据流动和隐私保护的紧张关系。

3. WhatsApp（Meta子公司）-2.25亿欧元（2021年，爱尔兰数据保护委员会）

WhatsApp因未能向用户充分说明其与Facebook共享数据的方式，被爱尔兰数据保护委员会罚款2.25亿欧元。该事件涉及对数据处理透明度的严重违反，特别是用户在不同平台之间的数据共享权利，WhatsApp未能提供足够清晰的信息来遵守GDPR透明度和用户同意的要求。

4. Amazon-7.46亿欧元（2021年，卢森堡数据保护委员会）

2021年，卢森堡数据保护委员会对亚马逊（Amazon）处以7.46亿欧元的罚款，这是迄今为止GDPR最大的罚款。该

案涉及亚马逊的广告定向方式，被认为违反了GDPR的隐私规定，尤其是在未获得用户明确同意的情况下，使用个人数据进行个性化广告。

5. Google–1亿欧元（2020年，法国CNIL）

法国的数据保护机构CNIL在2020年对Google处以1亿欧元罚款，原因是Google未能正确管理网站上的cookie设置，违反了用户同意条款。CNIL指出，Google在没有得到明确同意的情况下存储cookie，这违反了GDPR中对透明度和数据收集同意的规定。

6. Clearview AI–2000万欧元（2021年，多个欧盟国家）

ClearviewAI因非法收集和处理公民的面部识别数据而遭到多个欧盟国家的调查和罚款。该公司从公开的社交媒体图片中提取面部信息，未获得数据主体的同意，严重违反了GDPR的隐私保护规定。在多个案件中，ClearviewAI被罚款2000万欧元或更多。

7. BritishAirways–2000万英镑（2020年，英国ICO）

英国信息委员会办公室（ICO）对BritishAirways因数据泄露事件开出2000万英镑的罚单，尽管初始拟罚金额为1.83亿英镑。该事件影响了超过40万名客户的数据，包括信用卡详细信息、客户姓名和联系方式。ICO指出，BritishAirways未能采取适当的安全措施来保护客户的数据，这是该公司违规的主要原因。

8. H&M–3500万欧元（2020年，德国汉堡数据保护局）

2020年，德国汉堡数据保护局对时尚零售商H&M处以3500万欧元罚款，原因是H&M非法监控员工的私人生活。调查发现，H&M收集了大量有关员工个人生活的信息，并将这些数据用于工作评估。该行为严重违反了GDPR对数据收集和处理的规定，尤其是在员工隐私保护方面。

9. Marriott International–1830万英镑（2020年，英国ICO）

Marriott因数据泄露事件被英国ICO罚款1830万英镑。该事件影响了超过3.39亿名全球客户的个人数据，包括信用卡信息、护照号码等敏感数据。数据泄露源于Starwood酒店集团的数据库漏洞，但由于Marriott在2016年收购了该集团，并未及时修复安全漏洞，因此被认定为负有责任。

案例凸显了欧盟GDPR在数据隐私保护领域的严格性，数据透明度、用户同意和跨境数据传输问题是这些违规行为的核心焦点。跨国企业需要采取充分的措施来确保个人数据的安全和透明使用。

重要数据泄露事件

2021年底，我国发生了首例涉及高铁运行安全的危害国家安全案件。一名国家铁路集团的员工非法向境外人员提供高铁运行的敏感数据和技术信息，涉及中国高铁的运行安全。这些信息的泄露可能会对国家基础设施的安全构成严重威胁。案件涉及的违法行为被认定为危害国家安全，凸显了交通领域基础设施在国家安全体系中的重要性。

该案件反映了在现代化交通和信息技术发展背景下，数据安全对于国家关键基础设施的重要性，以及相关人员在敏感岗位上的责任。案件审判引起了广泛关注，显示出中国对涉及国家安全的非法数据传输行为的严格打击和零容忍态度。如果数据处理者需要将在我国境内收集和产生的重要数据提供给境外，必须进行数据出境风险自评估，向网信部门提交数据出境安全评估的申请。

健康数据泄露事件

在美国政府承包商Maximus发布的一份报告中，揭示了一起重大的数据泄露事件。据称，大约800万至1100万份健康数据记录被公之于众。这次数据泄露引发了广泛关注，特别是因为Maximus作为一家管理医疗补助和医疗保险以及许多其他政府项目的承包商，负责处理大量与联邦医疗项目相关的数据。这些数据通常由政府职能部门委托给外部组织进行采集、存储和利用，而其初始控制权归属于政府职能部门。如果受托组织未经授权就公开这些数据，就构成了违约和违法行为。一旦数据泄露，受托组织应当承担起数据安全责任。

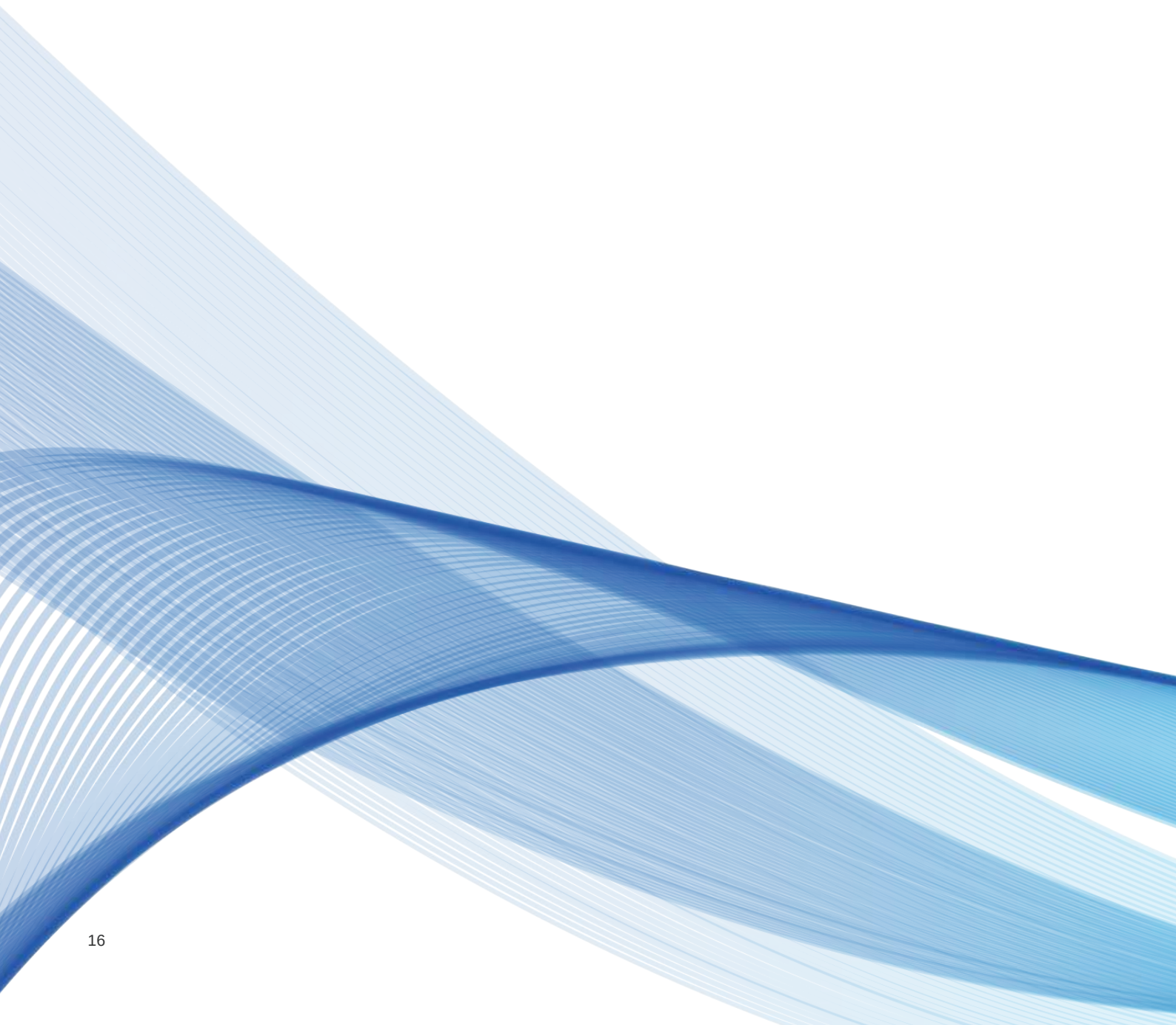
事件的具体起因可能是由于网络攻击或安全漏洞，导致这些敏感数据被不法分子获取。此次数据泄露不仅威胁到了受害者的隐私，还可能对他们的身份安全带来风险，甚至可能导致身份盗窃或欺诈行为的发生。事件暴露了在政府承包商和医疗数据处理领域中，加强数据保护和网络安全的重要性。

软件供应链攻击

2023年3月，全球著名的通讯软件服务商3CX遭遇了一次网络攻击。这次攻击在很多关键特性上与2020年广为人知的SolarWinds供应链攻击极其相似。在这次事件中，攻击者主要针对了3CX的一款VoIP电话系统应用软件。这款软件的客户遍布全球，涵盖了超过60万家组织以及2.5万个渠道合作伙伴，其中包括美国运通、麦当劳、可口可乐、NHS、丰田、宝马和本田等知名企业。然而，这次3CX的网络攻击有其独特之处，网络安全公司Mandiant指出，这次3CX的攻击实际上是由早期的供应链攻击造成的。据Mandiant的研究人员透露，他们监测到攻击者篡改了金融软件公司Trading Technologies发布的一款软件包，这是他们首次见证一起软件供应链攻击引发了另一起软件供应链攻击。这次事件再次凸显了企业网络安全的重要性，尤其是对供应链安全的关注。此外，事件也提醒我们，必须采取必要的安全措施来保护敏感数据，特别是在处理供应链数据时，必须严格遵守相关法规和合同约定，以确保数据的安全和合规。同时，我们也应当警惕，一次供应链攻击可能会引发更多的供应链攻击，构成一连串的安全威胁。

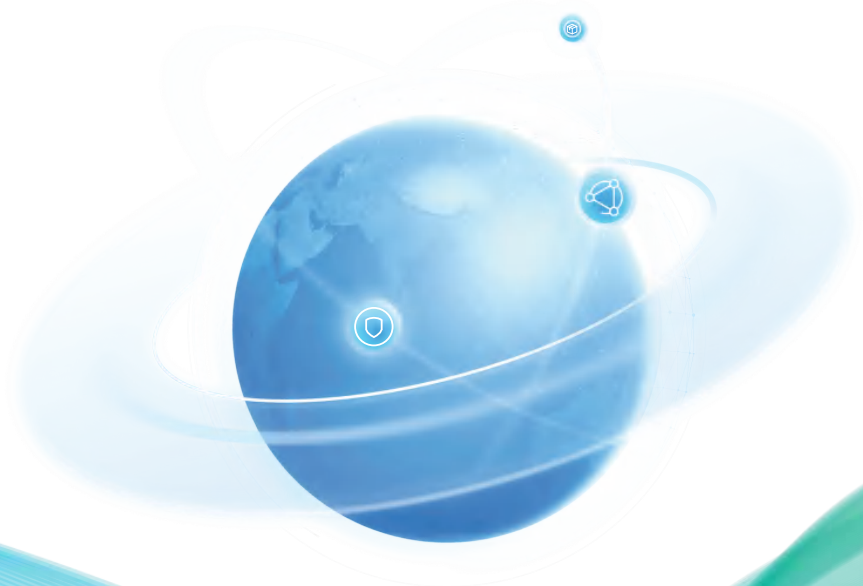
综上，数据安全问题不仅会影响企业的声誉和经济利益，更可能阻碍企业的海外扩张。在某些国家和地区，如果企业不能满足当地的数据安全法规要求，可能会被禁止进入市场，或者在进入市场后受到重罚。因此，对于计划出海的企业来说，必须将数据合规与安全作为重要的考虑因素之一。

企业数据跨境安全合规指引 2024



第二章
国外数据跨境管理要求

各国数据跨境流动管理方式存在显著的差异。从技术和产业发展角度，数据技术发达的国家，倾向于凭借其技术优势，在跨境数据流动中获取更多数据红利，因而其数据跨境法律法规就更显宽松。美国在全球数字经济中居于领先地位，基于数字贸易与数字技术领域的优势，倡导全球数据自由流动。欧盟、英国、新加坡和日本等数字经济发展较为成熟的地区和国家采取的是数据流动与数据保护平衡的模式。



欧盟数据跨境流动要求

根据欧盟《非个人数据自由流动条例》（Regulation on the Free Flow of Non-personal Data）与《通用数据保护条例》（GDPR），以充分性认定、个人信息保护认证、标准合同条款等建立信任机制等方式，欧盟致力于欧洲一体化市场，推动其成员国内部数据的自由流动，其他国家只有在具有与欧盟同等保护水平的条件下，才允许将数据传输出境。“充分性认定”是欧盟核心的个人数据出境管控制度，由欧盟委员会负责对欧盟以外国家或地区的数据保护立法实施、执法能力、监管机构设置和国际条约等因素进行综合评估，最终确定数据自由流动的“白名单”国家。欧盟这一机制促使其他国家按照GDPR的要求进行数据保护，以便本国企业能够与欧盟企业正常进行数据流动，有助于欧盟引领全球的数据合作。

欧盟《通用数据保护条例》（GDPR）于2018年5月25日正式生效，为个人数据的收集、处理、存储和传输建立了一个框架，要求以安全的方式处理所有个人数据，对不遵守这些要求的企业的罚款和处罚。

针对个人数据跨境传输机制，GDPR规定了三种方式。首先，制定“充分性认定”程序，确保第三国的数据保护标准与欧盟标准具备同等保护能力，将个人数据从欧盟传输到第三国。这意味着向第三国的数据传输与欧盟内部数据传输方式一致，从而便利欧盟数据的跨境自由流动。充分性保护认定要求第三国的数据保护标准要基于“基本等效”的欧盟标准，为对第三国的数据保护法律框架的全面评估，欧洲数据保护机构制定了数据安全能力评估所需的要素清单。其次，制定企业与企业之间的“标准合同条款”（SCC），作为将欧盟公民个人数据跨境传输到欧盟境外所采用的合同模板。第三，制定“约束性企业规则”（BCR），作为在欧盟成立的公司遵守的数据保护政策。

由此，从欧盟向非欧盟国家转移个人数据，转移目的地获得欧盟委员会的充分性认定，指的是欧盟认为对于个人数据有充分保护的国家或地区，个人数据可以直接转移到这些国家，而无需采取保护措施，这一规则主要适用于经认定的特定国家。对于未在上述白名单上的国家、地区或国际组织的商业实体，需通过采取保护措施得到充分保护，其中最重要的是签署欧盟SCC和主要适用于跨国公司或组织内部数据跨境传输的有约束力的公司规则（BCR）。

美国数据跨境流动要求

尽管美国没有联邦层面统一的数据与隐私安全保护立法，美国联邦国会和州立法机构都颁布了各种数据隐私安全法律，适用于不同领域的事项，包括个人数据在的某些应用场景（如将数据信息用于营销、就业人员的筛选）、某些行业（如金融机构、医疗保健服务提供者）、某些数据类别（如身份证号码、驾驶执照信息）或特定的侵害行为（如身份盗用、儿童的在线隐私）。

在消费者保护领域,《联邦贸易委员会法》（Federal Trade Commission Act）禁止企业针对消费者的不公平和欺骗性的行为。联邦贸易委员会（FTC）依据此法审查企业在保护客户数据隐私方面是否使用了不公平或欺骗性的做法。

在健康医疗领域，《健康保险携带和责任法案》（HIPAA）对广泛的医疗保健相关活动的隐私进行监管，适用于受保护的健康信息（PHI），PHI包括与病人健康有关的医疗信息、医疗记录、与医疗服务提供者的对话、医疗账单信息等等。

在金融领域，《公平信用报告法》（FCRA）和《公平和准确信用交易法》（FACTA）规范了信用报告信息保护要求，信用数据如果被违法利用可能会造成严重后果，FCRA确保消费者知道信用报告机构如何收集和使用个人信息。消费者有权在其报告与雇主共享之前表示同意与否，对个人信用报告实施安全冻结以限制披露，并向侵犯其权利的企业寻求赔偿。FACTA还加强了管理信用报告的组织在检测和防止身份盗用方面的义务。

在教育领域，《家庭教育权利和隐私法》（FERPA）通过要求教育机构加强对学业记录的保护和增加学生和家长的权利来保护学生的学术信息的隐私和安全，减少学生因为在高难度课程表现不佳而被污名化的风险。FERPA适用于从美国教育部接受联邦资金的教育机构所保存的任何学术记录。

在州立法层面，为了解决美国缺乏联邦层面全面隐私保护的问题，《加州消费者隐私法案（CCPA）》于2020年1月实施，以加强对消费者的隐私权利和数据安全的保护，对企业遵循义务做出了规定。该法案被认为是美国国内最严格的隐私立法，开启了美国统一隐私立法的高潮。CCPA实施以来，包括谷歌和Facebook在内的科技公司面临非常严格的隐私保护要求，包括披露他们收集的关于消费者的个人信息的类别和具体要素、收集信息的来源、收集或出售信息的业务目的以及与之共享信息的第三方的类别等等。同时，基于CCPA的“长臂管辖”原则，即使中国企业在美国没有公司实体，也有可能要遵守CCPA的规定。

其他州的数据隐私立法还有《特拉华州在线隐私和保护法》、《伊利诺伊州知情权法案》、《新泽西州个人信息和隐私保护法》、《华盛顿州生物识别隐私法》、《纽约金融管理局网络安全条例》等。

2010年11月，美国发布第13556号行政命令《受控非密信息（CUI）》，确立了管理受控非密信息的政府计划，对基础设施、国防、出口管制、金融、情报等非涉密信息类型进行监管。制定“受控非机密信息”列表，通过《出口管制条例》（EAR），对非个人数据采取严格出境管理措施。

2024年2月28日，拜登政府依据《国际紧急经济权力法》（IEEPA）发布了《关于防止受关注国家获取美国人大量敏感个人数据和美国政府相关数据的行政令》（以下简称《行政令》），美司法部同日发布关于该行政令的情况说明，并于次日发布《行政令的拟议规则预通知》进一步细化阐述，防止受关注国家访问收集涉及美国政府的敏感数据以及有关美国人的敏感信息。新规和系列动作反映了拜登政府从主导“数据自由流动”的跨境政策转变为以国家安全为由的“数据安全流动”。中美之间潜在数据流动规模巨大，围绕数据和技术领域的竞争也最为激烈，显然中国是该项政策最关键和最重要的管制目标。该行政令及后续政策将对我国数据跨境政策实施以及技术和产业发展造成影响，也可为我国数据基础制度框架提供参考。

在国际贸易协定方面，2016年美国推动的《跨太平洋伙伴关系协定》（TPP）主张允许为数据主体利益而进行的数据跨境传输，以破除许多国家所设置的数据本地化存储等市场准入壁垒。2018年，美国出台了《澄清境外数据合法使用法案》（CLOUD Act），扩大了美国政府直接调取境外数据的权利，并给其他国家调取美国境内个人数据设置“符合资格的外国政府”审查门槛。美国积极推行由亚太经合组织（APEC）主导的跨境商业个人隐私保护规则体系（CBPR），致力于促进APEC各经济体之间无障碍的跨境数据传输与流通。

美欧数据跨境流动要求

自2000年《欧美安全港框架》以来，欧美数据跨境规则不断演进，从跨境数据安全风险中持续改进规则协议。《欧美安全港框架》旨在满足欧盟《数据保护指令》（指令95/46/EC）相关要求，美国企业向美国商务部自我认证遵守相关原则与要求，即可接收从欧盟传输来的个人数据。2013年，奥地利律师Maximilian Schrems对Facebook Ireland Ltd提起投诉，并提交爱尔兰数据保护专员，试图禁止Facebook Ireland Ltd依据安全港框架将其个人数据转移到美国，认为美国法律没有确保对其个人数据进行充分保护以免受美国政府的监视活动。2015年10月，欧盟法院发布SchremsI决定，宣布安全港框架无效，认为安全港框架违反《数据保护指令》（指令95/46/EC），侵犯欧盟公民的个人数据根本权利。

在SchremsI案之后，2016年欧盟委员会通过第2016/125号决定，批准隐私盾协议，视为一项“充分性决定”，确定美国“确保对欧盟数据主体提供足够的数据隐私保护”。在《欧美隐私盾协议》共享框架下，美国设立独立的隐私盾监察员，负责监督国家安全干预。美国还向欧盟提供关于为国家安全目的访问数据的限制和保障措施的详细承诺。

首先，美国企业承担更强义务。虽然参加隐私盾是自愿的，但一旦美国企业提交参加隐私盾的自我确认书，就应当完全遵守相关隐私原则并公开隐私政策以及执法部门获取个人数据的请求等。此外，美国企业声明其符合并遵守隐私盾要求

的自我确认书至少每年提交一次，否则会被除名。在监督和执法方面，美国商务部、联邦贸易委员会、交通部等负责监督参加隐私盾的美国企业履行义务，做出相应处罚和制裁，如联邦贸易委员会可依据《联邦贸易委员会法》第45条，认定违规企业构成不正当竞争，给予罚金、除名等严厉处罚。

第二，对美国政府进行网络监控、获取个人信息的明确限制。美国政府获取欧盟公民个人信息明确限于以下六个目的：一是侦测、反击外国势力的特定行动；二是反恐；三是反制核扩散；四是网络安全；五是侦测、反制对美国和同盟军事力量构成的威胁；六是打击国际犯罪威胁，包括逃避刑事制裁的行为。美国方面承诺不再进行大规模的任意监控。此外，美国设立一个独立的隐私盾监察员，负责处理涉及政府部门监控、获取个人信息的投诉。

2020年7月16日，欧盟法院在“Schrems II 案”中认为美国的监控立法违反了《欧盟基本权利宪章》，也没有为欧盟个人提供有效的司法救济，因此欧美之间的“隐私盾”协议无效。另外，就目前广泛使用的数据保护标准合同条款（SCCs）的合法性问题，欧盟法院认为其继续有效，但需结合具体情况采取额外补充措施；在使用标准合同条款等保障措施进行数据传输时，也需确保提供了“与欧盟同等的保护水平”，否则数据保护机构可以暂停或终止相关数据传输。

2023年7月，欧盟委员会通过《欧美数据隐私框架》充分性决定，旨在推动跨大西洋商业往来，并确保与欧盟法律一致水平的数据保护，为美国组织从欧盟/欧洲经济区向美国进行数据传输提供可靠的机制。《欧美数据隐私框架》体系由两个部分组成。美国商务部发布的《欧美数据隐私框架原则》，明确参与框架的美国实体所需遵守的要求，事实上与隐私盾内容重合性较大。从GDPR角度看，《欧美数据隐私框架》可视为将参与框架的美国实体作为一个特殊的群体予以充分性认证，从而可以为美国企业适用GDPR提供豁免。同时，制定了框架配套文件《关于加强美国信号情报活动保障的行政令》及其他相关规范美国情报机关活动的文件。

欧盟对《欧美数据隐私框架原则》做出的充分性决定将在很大程度上减轻跨大西洋数据传输的合规难度。根据《欧美数据隐私框架原则》取得认证的组织无需再采取任何其他数据跨境传输合规机制（例如标准合同条款或具有约束力的组织规则），即可将个人数据从欧盟转移至美国。位于欧盟的数据提供方在将个人数据跨境传输至取得《欧美数据隐私框架原则》认证的接收方时，开展转移风险评估将不再是强制义务。

在管理机制层面，《欧美数据隐私框架》认证机制由美国商务部国际贸易管理局进行管理，由美国联邦贸易委员会和美国交通部负责执行。欧洲委员会将通过定期检查监督数据隐私框架，并确保美国方面执行的合规性。欧盟和美国还设有定期联合审查的条款。如果美国未能履行承诺，欧洲委员会可以暂停数据隐私框架。

在机制实施层面，个人可以向其所在欧盟成员国的国家数据保护机构提交投诉，然后通过欧洲数据保护委员会转交给美国。投诉的初步调查由美国公民自由保护官员进行。必要时，个人也可以向新成立的数据保护审查法庭提出申诉，该法庭是一个独立机构，由不属于美国政府的个人组成，可以做出具有约束力的法律决定。

英美两国建立“数据桥”。英国议会于2023年9月21日制定了充分性认定条例，该条例将于10月12日生效。根据这一法规，英国企业将可以在不需额外机制、传输影响评估以及其他附加传输保障措施的情况下，将能够将个人数据传输到获得“欧盟-美国数据隐私框架的英国扩展”认证的美国组织。在官方文件中，这一决策通常被称为"数据桥"，即指允许英国的个人数据自英国传输至其他国家，而无需进行额外的数据保障措施。数据桥不具有互惠性，因此它不允许数据从其他国家自由地流向英国。对于数据桥的评估需要考虑国家对个人数据的保护、法治情况、对人权与基本自由的尊重以及监管机构的运作模式。数据桥的构建有利于确保源自英国的个人数据能够实现自由且安全的跨境交换、方便共享关键信息以促进与生命安全相关的研究、减少数据共享方面的障碍等。

其他国家数据跨境要求

新加坡数据跨境要求

新加坡推动智慧国家战略，加大了对电信业和数据中心建设。制定《个人数据保护法》以及相关法规，建立和完善了个人信息保护制度，确立了一系列规范跨境数据流动的准则，设定数据跨境流动的条件等。数据跨境流动管理规则有助于将数据汇聚和流动到新加坡，打造成为国际数据融合的重要中心城市。

新加坡数据跨境制度要求在通常情况下，个人数据应在国内存储，数据跨境传输受到特定的条件和要求的限制。与欧盟白名单制度类似，规定只有当接收国的数据保护法律和标准与新加坡保持同等保护水平时，才允许进行跨境数据传输。这种机制确保了在数据跨境流动时，数据主体的个人信息依然受到足够的保护。此外，强调数据安全性和透明性，要求数据处理方在处理个人数据之前履行充分的信息告知义务，以明确解释数据的用途和处理方式。

新加坡数据跨境流动主管部门包括个人数据保护委员会和信息通信部下设的信息通信与媒体发展局。具体而言，个人数据保护委员会职责包括建立个人数据保护机制、进行监管和政策实施，要求监管对象（包括各种私人组织，涉及数据获取、使用、储存、传输和跨境转移）建立完善的数据传输机制、审核机制，并设立相应的问责工具。信息通信与媒体发展局主要在技术等方面为个人数据保护委员会的监管和政策实施提供支持。此外，鉴于不同专业领域（例如医疗、教育、金融等）的数据内涵更加丰富，保护难度更大，因此，对于这些领域的数据流动，个人数据保护委员会与各专业领域的主管部门合作，制定相关咨询指南并共同进行监管。

日韩数据跨境要求

截至目前，亚洲仅有日本、韩国两个国家通过欧盟数据保护的“充分性认定”程序。2019年1月，欧日先后认定双方的个人数据保护措施相当。首先，日本通过“补充规则”解决与欧盟在个人数据保护上的差异，包括扩展对敏感数据的定义范围、保障数据个人权利的行使、向日本以外的第三方传输的数据将受到更高级别的保护。其次，承诺以国家安全和刑事执法为目的获取欧盟数据将被限制，受到独立监督和有效的补救机制。第三，同意在已有的数据保护机构个人信息保护委员会建立“争议处理机制”，以处理日本使用欧盟数据时产生的投诉。

2021年12月20日，韩国通过欧盟数据保护的“充分性认定”程序，意味着韩国企业可不受限制地将在欧盟收集的个人数据引入国内。为了通过欧盟的“充分性认定”程序，韩国修订了韩国的《数据保护法》，整合数据保护相关法规，增强韩国个人数据保护委员会机构的管辖力。在《数据保护法》内容，对标GDPR数据保护管理要求。例如，修正案规

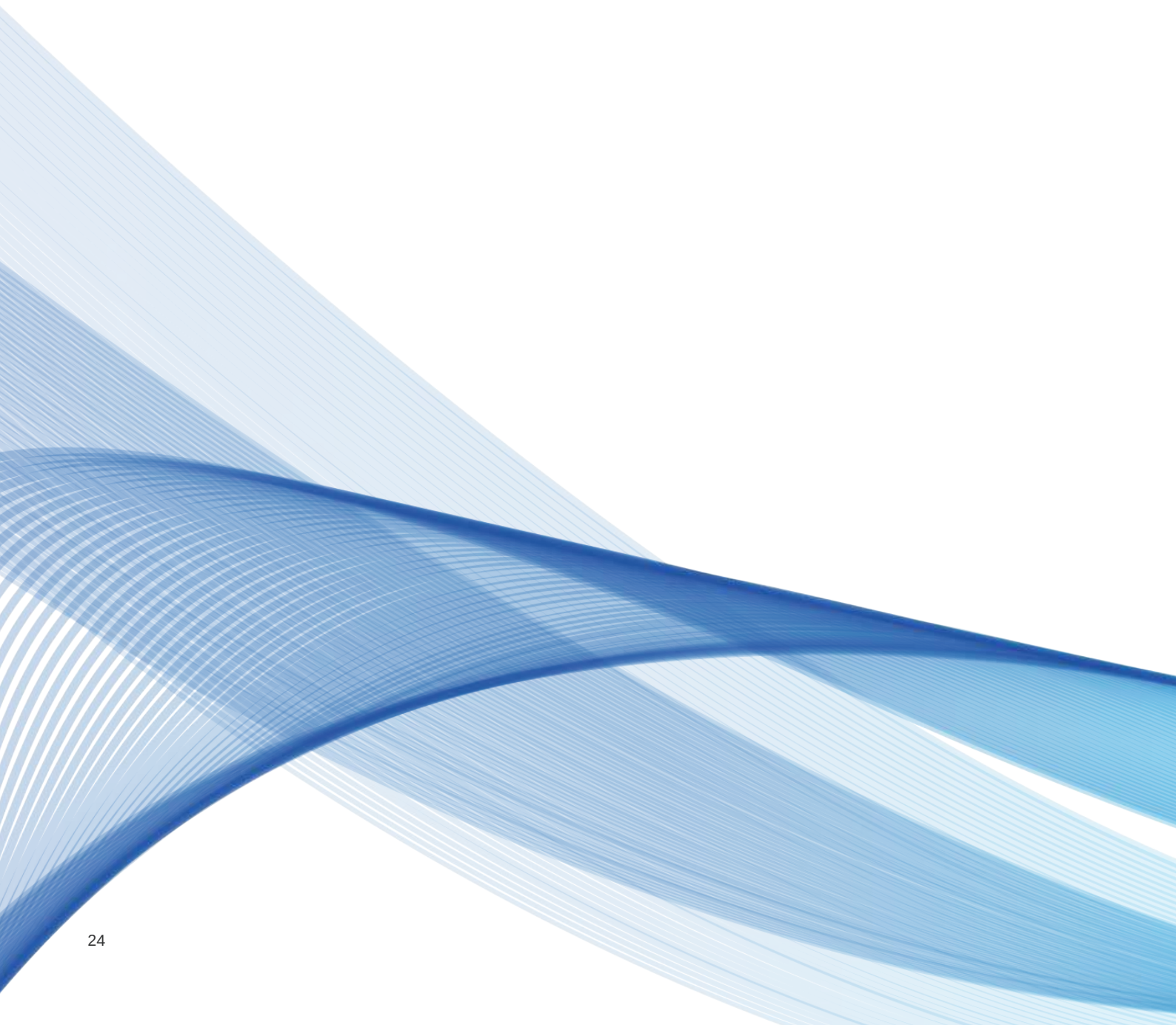
定违反数据保护法律要求将可能产生对企业总销售额3%的行政罚款，重者可处刑事处罚或监禁。又如，引入“假名化”概念，增强数据流动性。在未经数据主体同意的情况下，出于符合公众利益的科学目的，韩国允许数据处理者处理假名化的信息。

俄罗斯数据跨境要求

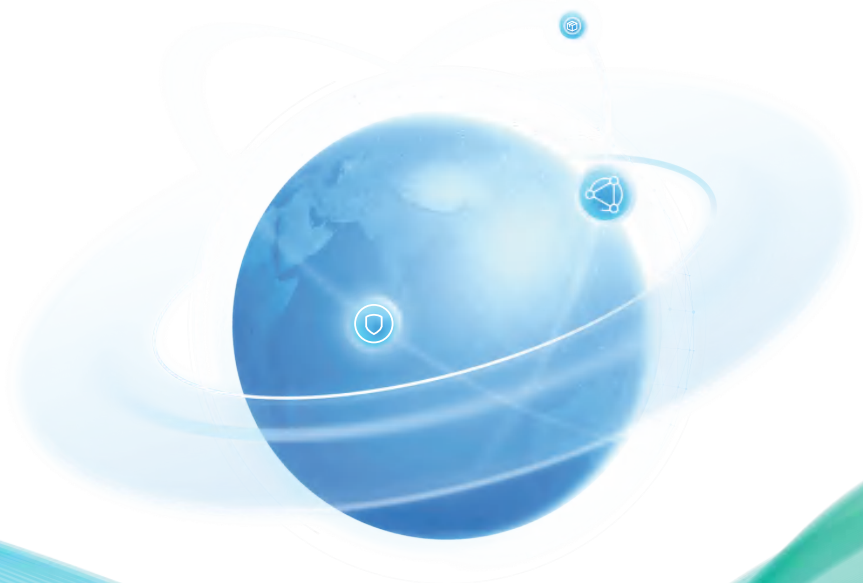
俄罗斯、印度、巴西、南非等国家的数据跨境规则，建立强监管“本地化”模式。采取属地原则以限制重要数据出境，形成了优先考虑安全保护的“本地化”政策模式。俄罗斯在《关于信息、信息技术和信息保护法》和《俄罗斯联邦个人信息法》中，加强了对信息跨境传输的监管，确立了数据本地化存储的基本规则。俄罗斯对个人数据出境控制相当严苛，一是俄罗斯联邦公民个人信息和数据库需要存放在俄罗斯境内；二是对俄罗斯公民个人数据的处理活动必须使用位于俄罗斯境内的数据库；三是处理数据前履行信息告知的义务。俄罗斯同样存在与欧盟相似的“白名单”制度，要求数据接收国必须符合同等保护要求才可进行跨境数据传输，否则，只有在个人数据主体已书面同意其个人数据出境、个人数据主体作为合同当事人履行合同等前提条件下，才可传输数据出境。

此外，在国际贸易协议中也有体现跨境数据流动要求，从促进国际贸易发展角度出发，“问责制”成为国际规则或贸易协议的主导方向。例如，经济合作与发展组织（OECD）在2013年制定的《关于隐私保护与个人跨境数据流动的指南（2013）》以及亚太经济合作组织（APEC）在2012年建立的“跨境隐私规则体系”，都采取了“问责制”的原则，即通过设立一定的准入标准和规则，以企业自律方式实施跨境数据的流动管理。

企业数据跨境安全合规指引 2024



第三章
我国数据跨境管理要求



数据跨境合规要求

2017年以来，我国逐步建立完善数据跨境法律法规要求，加强积极推动数据依法有序自由流动，相继出台《网络安全法》《数据安全法》《个人信息保护法》《数据出境安全评估办法》《促进和规范数据跨境流动规定》《网络数据安全管理条例(草案)》等法律法规，对数据出境活动作出明确规定。

《网络安全法》第三十七条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。《数据安全法》第三十一条规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，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运营中收集和产生的重要数据的出境安全管理办法，由国家网信部门会同国务院有关部门制定。

《个人信息保护法》第三十八条规定，个人信息处理者因业务等需要，确需向中华人民共和国境外提供个人信息的，应当具备下列条件之一：通过国家网信部门组织的安全评估；按照国家网信部门的规定经专业机构进行个人信息保护认证；按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；法律、行政法规或者国家网信部门规定的其他条件。中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。个人信息处理者应当采取必要措施，保障境外接收方处理个人信息的活动达到本法规定的个人信息保护标准。

综上，我国数据跨境要求主要围绕重要数据和一定规模上的个人信息。这是为了切实保护人民群众利益，维护国家网络和数据安全，促进数据依法有序自由流动。数据出境安全管理不是对于所有数据，只限于重要数据和个人信息，这里的重要数据是针对国家而言，而不是针对企业和个人。

为落实法律规定要求，国家互联网信息办公室公布了《数据出境安全评估办法》和《个人信息出境标准合同办法》，联合国家市场监督管理总局公布了《关于实施个人信息保护认证的公告》，基本构建了数据出境安全管理制度。此外，国家互联网信息办公室先后公布了《数据出境安全评估申报指南》、《个人信息出境标准合同备案指南》等文件，对数据处理者申报安全评估、备案标准合同的方式、流程及需提交的材料等具体要求作出了说明。

2024年8月，国务院常务会议审议通过了《网络数据安全管理条例(草案)》。会议指出，要对网络数据实行分类分级保护，明确各类主体责任，落实网络数据安全保障措施。要厘清安全边界，保障数据依法有序自由流动，为促进数字经济高质量发展、推动科技创新和产业创新营造良好环境。参考2021年11月公开征求意见的《网络数据安全管理条例（征求意见稿）》条例，对数据跨境安全管理提供更加明确的要求。

数据处理者向境外提供数据应当履行以下义务，包括：不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范围、方式和数据类型、规模等向境外提供个人信息；不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据；采取合同等有效措施监督数据接收方按照双方约定的目的、范围、方式使用数据，履行数据安全保护义务，保证数据安全；接受和处理数据出境所涉及的用户投诉；数据出境对个人、组织合法权益或者公共利益造成损害的，数据处理者应当依法承担责任；存留相关日志记录和数据出境审批记录三年以上；国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示；国家网信部门认定不得出境的，数据处理者应当停止数据出境，并采取有效措施对已出境数据的安全予以补救；个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。非经中华人民共和国主管机关批准，境内的个人、组织不得向外国司法或者执法机构提供存储于中华人民共和国境内的数据。

向境外提供个人信息和重要数据的数据处理者，每年编制数据出境安全报告，向设区的市级网信部门报告上一年度以下数据出境情况，包括：全部数据接收方名称、联系方式；出境数据的类型、数量及目的；数据在境外的存放地点、存储期限、使用范围和方式；涉及向境外提供数据的用户投诉及处理情况；发生的数据安全事件及其处置情况；数据出境后再转移的情况；国家网信部门明确向境外提供数据需要报告的其他事项。

在数据跨境技术要求方面，提出建立数据跨境安全网关，对来源于境外、法律和行政法规禁止发布或者传输的信息予以阻断传播。任何个人和组织不得提供用于穿透、绕过数据跨境安全网关的程序、工具、线路等，不得为穿透、绕过数据跨境安全网关提供互联网接入、服务器托管、技术支持、传播推广、支付结算、应用下载等服务。

促进和规范数据跨境流动规定

2024年3月22日，国家互联网信息办公室发布《促进和规范数据跨境流动规定》，对现有数据出境安全评估、个人信息出境标准合同、个人信息保护认证等数据出境制度的实施和衔接作出进一步明确，适当放宽数据跨境流动条件，适度收窄数据出境安全评估范围，在保障国家数据安全的前提下，便利数据跨境流动，降低企业合规成本，充分释放数据要素价值，扩大高水平对外开放，为数字经济高质量发展提供法律保障。数据跨境旨在促进数字贸易，2023年7月国务院发布的《关于进一步优化外商投资环境加大吸引外商投资力度的意见》中提出，要探索便利化的数据跨境流动安全管理机制。

《促进和规范数据跨境流动规定》在促进数据自由流动与强化数据安全保护之间建立了平衡，主要对下列内容进行了规定：一是明确重要数据出境安全评估申报标准。二是明确免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。三是设立自由贸易试验区负面清单制度。四是调整应当申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境活动条件。五是延长数据出境安全评估结果有效期，增加数据处理者可以申请延长评估结果有效期的规定。

重要数据出境安全评估

重要数据是指一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据。《数据安全法》规定，国家数据安全工作协调机制统筹协调有关部门制定重要数据目录，加强对重要数据的保护。各地区、各部门应当按照数据分类分级保护制度，确定本地区、本部门以及相关行业、领域的重要数据具体目录，对列入目录的数据进行重点保护。但是，目前仍存在重要数据识别规则不清晰的问题，对数据跨境流动造成障碍。为此，《促进和规范数据跨境流动规定》，数据处理者应当按照相关规定识别、申报重要数据。未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。

在国家标准层面，GB/T43697-2024《数据安全技术 数据分类分级规则》在2024年3月21日发布，并将于2024年10月1日正式实施。根据数据的敏感性、重要性和潜在风险，将数据分为核心数据、重要数据和一般数据三个级别。在数据分级的过程中应综合考虑数据的领域、群体、区域、精度、规模、深度、覆盖度和重要性等多个要素。该标准进一步聚焦重要数据范围，定义为“特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据”。仅影响组织自身或公民个体的数据一般不作为重要数据。

该标准附录G明确了重要数据识别指南，各行业主管和地方政府也在陆续出台或更新本行业本地区的重要数据目录，对于已经有了重要数据目录的行业和地区，企业就必须开展重要数据识别和申报数据出境安全评估。此外，自贸区政府具有先试先行的权利，通过设立可及时调整更新的负面清单，为区内企业创造更加便利的数据跨境管理环境。

数据出境豁免条件

根据《促进和规范数据跨境流动规定》，以下六种数据出境活动免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：

一是国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的。

二是在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的。

三是为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店

预订、签证办理、考试服务等，确需向境外提供个人信息的。

四是按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的。

五是紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的。

六是关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。其中，第三种至第六种条件所称向境外提供的个人信息，不包括被相关部门、地区告知或者公开发布为重要数据的个人信息。

针对境外数据入境再出境、个人作为一方的国际合同、跨境人事管理、紧急救助等场景的豁免，消除了对跨国企业各种常规事务中个人信息跨境的阻碍，便于跨国企业进行全球统一人事管理。针对个人信息（非敏感个人信息），每年10万人以下个人信息（不包含敏感个人信息）跨境也被豁免，能够减轻了不用处理大量个人信息的企业的负担。另一方面，在实务操作上要聚焦数据使用目的，看是否符合“履行合同所必须”等豁免条件。

2024年9月，广州互联网法院发布了跨境数据纠纷十大典型案例，这也是首次披露跨境数据违规案例。其中，“王某与某咨询公司、某国际酒店公司个人信息保护纠纷案”，是个人信息跨境处理行为的合法性审查的典型案例。

基本案情是王某通过某咨询公司运营的微信公众号购买了某国际酒店公司住宿服务，并在某国际酒店公司的移动应用APP上预定了境外酒店。预定过程中，王某点击勾选了某国际酒店公司的《客户个人数据保护章程》，并提交了姓名、国籍、电话号码、电子邮箱地址、银行卡号等个人信息。事后，王某发现依据《客户个人数据保护章程》规定，其提交的个人信息将被传送共享至全球多个地区和接收主体。王某认为两公司跨境处理中国公民个人信息行为违反相关规定，遂向广州互联网法院提起诉讼。

广州互联网法院生效判决认为，被告公司为消费者预定域外酒店服务收集案涉个人信息，此种情况下的个人信息出境，属于履行合同必需，不须单独同意。经审理查明，被告公司在其《客户个人数据保护章程》中，未遵循公开透明原则，真实、准确、完整告知其处理规则，未能依法正确履行告知义务。另查明，被告公司基于商业营销目的，还向位于美国和爱尔兰的某第三方公司传输处理相关个人信息，该处理行为及其处理目的超出履行合同必需，也未向王某充分告知并取得其单独同意，属于违法处理行为，侵害了王某的个人信息权益，应当承担民事侵权责任。

该案例具有典型意义，未来可以作为是否数据出境合规豁免条件的参考。数据跨境流动已经成为全球资金、信息、技术、人才等资源要素交换、共享的基础，个人信息的跨境流动关乎个人、社会和国家利益。当前，跨境互联网平台的个人信息处理章程普遍存在信息收集范围表意不清、信息处理方式含糊不明等问题。

跨境个人信息处理的主要合法性基础是个人同意和履行合同所必需，无论基于上述何种合法性理由，个人信息处理者均应当依法履行告知义务。从个人同意的角度，本案中被告的《客户个人数据保护章程》属于一揽子的笼统告知，而非增强告知。对于类似的笼统告知，用户或消费者的点击勾选，不能产生“单独同意”的效力。结合本案，如果跨境个人信息处理行为超出笼统告知的处理目的，又不具备个人同意以外的其他法定的合法性基础，个人信息处理者必须履行增强告知义务并获得个人单独同意，从而确保个人信息知情权和决定权的实现。从履行合同必需的角度看，如果跨境个人信息处理的收集范围、处理方式、处理目的等确属履行合同所必需的，则不需要个人的单独同意。

本案明确了个人信息跨境处理的合法性审查规则，为丰富全球个人数据跨境流动的实践探索提供司法范本。

自贸区负面清单制度

自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单。

自由贸易试验区内数据处理者向境外提供负面清单外的数据，可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。负面清单出台前，自由贸易试验区内的数据出境活动按照国家数据出境安全管理有关规定执行。

“负面清单”是外商投资领域的专用词汇，“数据跨境流动的负面清单”指不纳入数据跨境流动安全管理的数据的范围，需经省级网络安全和信息化委员会批准后，报国家网信部门、国家数据管理部门备案。

该条实施以来，天津、北京、上海等地自贸区已出台符合自贸区产业需求和典型应用场景的数据出境负面清单。各地自贸区实际情况不同，特别是对外贸易的具体业务不同，因此对自贸区给予了充分的自由度，允许所有的自贸区定制负面清单，显示了开放的政策趋势。

数据出境安全评估

评估流程

根据网信办发布的《数据出境安全评估办法》及《数据出境安全评估申报指南》中的要求， 数据出境安全评估主要包括以下环节。

1、申报材料准备。数据处理者申报数据出境安全评估，需要准备《数据出境安全评估申报书》、与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件、数据出境风险自评估报告以及其他相关材料。

2、向省级网信部门申报。数据处理者申报数据出境安全评估，应当通过数据出境申报系统提交申报材料，系统网址为https://sjcj.cac.gov.cn。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的，采用线下方式通过所在地省级网信办向国家网信办申报数据出境安全评估。

3、完备性查验（5个工作日）。省级网信办在数据处理者提交申报材料之日起5个工作日内完成申报材料的完备性查验，并向数据处理者告知查验结果。通过完备性查验的，省级网信办将申报材料提请国家网信办受理；未通过完备性查验的，省级网信办向数据处理者告知未通过完备性查验原因。

4、是否受理（7个工作日）。国家网信办自收到省级网信办提交的申报材料之日起7个工作日内，确定是否受理并书面通知数据处理者。

5、组织评估（45个工作日）。国家网信部门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。

6、是否补充/更正材料。要补充或者更正申报材料的，数据处理者应当按照告知要求及时补充或者更正材料。无正当理由不补充或者更正申报材料的，国家网信办可以终止安全评估。情况复杂或者需要补充、更正材料的，国家网信办可以适当延长评估时间，并告知数据处理者预计延长的时间。

7、书面通知评估结果。开展评估完成后，国家网信办向数据处理者出具评估结果通知书。数据处理者应当按照数据出境安全管理相关法律法规和评估结果通知书的有关要求，规范相关数据出境活动。

8、申请复评（15个工作日）。数据处理者对评估结果有异议的，可以在收到评估结果通知书15个工作日内向国家网信办申请复评，复评结果为最终结论。

评估内容

数据处理者在申报数据出境安全评估前，开展数据出境风险自评估，重点评估以下事项：数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；出境数据的规模、范围、种类、敏感程度，数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等；与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；其他可能影响数据出境安全的事项。

数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：数据出境的目的、范围、方式等的合法性、正当性、必要性；境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；出境数据的规模、范围、种类、敏感程度，出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；数据安全和个人信息权益是否能够得到充分有效保障；数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；遵守中国法律、行政法规、部门规章情况；国家网信部门认为需要评估的其他事项。

由此可以看出，数据出境风险自评估与安全评估的不同点主要体现在评估主体和评估内容的侧重点上。自评估是由数据处理者在申报数据出境安全评估前主动开展的内部审查，主要评估数据出境活动的合法性、正当性和必要性，关注数据规模、敏感程度以及境外接收方的安全保障措施等。同时，自评估也特别强调数据处理者与境外接收方的责任分配以及数据出境可能带来的风险，以确保数据的安全性和合规性。安全评估则由国家网信部门主导，侧重于从国家安全和公共利益的角度来评估数据出境活动的潜在风险。相对而言，不仅涵盖了自评估中的部分内容，还特别关注境外接收方所在国家或地区的法律法规和网络安全环境对出境数据的影响，评估境外接收方是否具备与中国法律和标准相符的安全保护水平。安全评估更具有权威性，且其结论直接影响数据出境活动的合规性审批。因此，自评估是可以看成是数据处理者的自我审查，而安全评估则是国家对数据出境活动的全面审查和监管。

评估报告

根据数据出境风险自评估报告模板，出境风险自评估需要描述以下方面。

1、自评估工作情况。简要概述自评估工作开展情况，包括起止时间、组织情况、实施过程、实施方式等内容。

2、出境活动整体情况。简要说明数据处理者基本情况、数据处理者安全保障能力情况、境外接收方情况、法律文件约定情况等，详细说明拟出境数据情况。

一是数据处理者基本情况，主要包括股权结构、实际控制人、境内外投资情况等，组织架构和数据安全管理机构信息，以及整体业务与数据资产情况。

二是拟出境数据情况，主要包括数据出境涉及业务、数据资产等情况，数据出境及境外接收方处理数据的目的、范围、方式及其合法性、正当性、必要性。按照申报业务场景梳理对应的出境数据项情况并逐一说明，数据项名称 与内容描述、出境必要性 、数据项示例等。针对出境后的情况，需要提供拟出境数据在境内存储的系统平台、数据中心（包含云服务）等情况，数据出境链路相关情况，计划出境后存储的系统平台、数据中心等；数据出境后向境外其他接收方提供的情况。涉及个人信息的，按照自然人（去重）统计当年的出境数量，预估未来3年的出境数量。

三是数据处理者数据安全保障能力情况，包括数据安全管理能力、技术能力、安全保障措施有效性证明以及是否受到违规处罚情况等。数据安全管理能力，包括管理组织体系和制度建设情况，全流程管理、分类分级、应急处置、风险评估、个人信息权益保护等制度及落实情况。数据安全技术能力，包括数据收集、存储、使用、加工、传输、提供、公开、删除等全流程所采取的安全技术措施等。数据安全保障措施有效性证明，例如开展的数据安全风险评估、数据安全认证、数据安全检查测评、数据安全合规审计、网络安全等级保护测评等情况。

四是境外接收方情况，主要包括境外接收方基本情况，境外接收方处理数据的用途、方式等，境外接收方履行责任义务的管理和技术措施、能力等。

五是法律文件约定数据安全保护责任义务的情况，主要包括：数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等；数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；对于境外接收方将出境数据再转移给其他组织、个人的约束性要求；境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、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，导致难以保障数据安全时，应当采取的安全措施；违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式；出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式。

3、出境活动的风险自评估情况及结论。对照《数据出境安全评估办法》，说明数据出境风险自评估情况，重点说明自评估发现的问题和整改情况。综合风险自评估情况和相应整改情况，对拟申报的数据出境活动作出客观的风险自评估结论，充分说明得出自评估结论的理由。

企业在申报数据出境安全自评估过程中重点关注以下几个要点：

1、动态关注企业可能触发安全评估的条件。如对跨国企业而言，首先，跨国企业在统计个人信息数量时需先考量在公众号、小程序、App或电商渠道收集个人信息的数量，往往公众号或者电商店铺的关注用户很容易触及100万个人信息的红线，便满足了申报条件。其次，由于跨国集团境外总部集中管理的需要，可能会采用境外系统集中管理人力资源数据，如涉及员工或应聘者的（敏感）个人信息出境，数量也很容易触发安全评估的申报条件。除此之外，由于企业处理

个人信息的数量处于不断变化的状态，建议企业持续关注年度累计处理的个人信息数量，如有可能达到安全评估所要求的量级，可以提前为申报安全评估做好准备。

2、开展数据出境相关培训。企业在开展数据出境风险自评估之前，宜提前在公司内部进行宣贯培训，或是以邮件的方式通知相关部门，向其科普当前法律背景下数据出境安全评估的紧迫性和重要性。这有利于安全自评估小组更清晰地梳理数据出境场景、撰写自评估报告，同时，也有利于管理层更便利地协调不同业务部门，使得相关人员在访谈中更全面、具体地披露其所了解的情况。

3、与境外关联机构进行沟通。企业在开展数据出境风险自评估时，建议尽快梳理好企业内部的岗位分工架构、数据安全制度、数据安全技术能力、数据安全保障措施有效性证明及与境外的法律文件（数据处理协议）。对于跨国企业而言，这些材料大部分需要与境外总部沟通，实践中境外总部往往很难理解提供上述材料的必要性，建议企业提前预留时间向境外获取材料，避免在报告即将完成时因材料不足影响后续工作。

个人信息保护认证

认证程序

2022年11月4日，国家互联网信息办公室、市场监管总局联合印发《个人信息保护认证实施规则》，对个人信息保护认证实施程序做出了详细规定，包括认证申请、技术验证、现场审核、获证后监督等一系列环节，如下图所示：

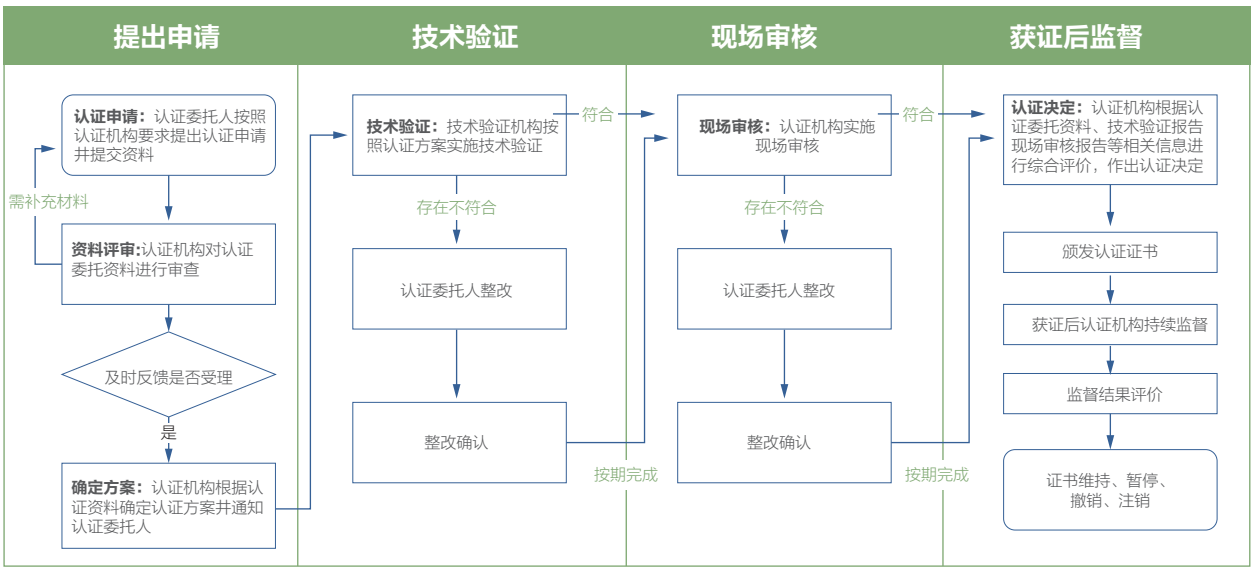


图3-1 个人信息保护认证流程

个人信息保护认证的认证模式为“技术验证 + 现场审核 + 获证后监督”。

认证委托

认证机构应当明确认证委托资料要求，包括但不限于认证委托人基本材料、认证委托书、相关证明文档等。认证委托人应当按认证机构要求提交认证委托资料，认证机构在对认证委托资料审查后及时反馈是否受理。认证机构应当根据认证委托资料确定认证方案，包括个人信息类型和数量、涉及的个人信息处理活动范围、技术验证机构信息等，并通知认证委托人。

技术验证

技术验证机构应当按照认证方案实施技术验证，并向认证机构和认证委托人出具技术验证报告。

现场审核

认证机构实施现场审核，并向认证委托人出具现场审核报告。

认证结果评价和批准

认证机构根据认证委托资料、技术验证报告、现场审核报告和其他相关资料信息进行综合评价，作出认证决定。对符合认证要求的，颁发认证证书；对暂不符合认证要求的，可要求认证委托人限期整改，整改后仍不符合的，以书面形式通知认证委托人终止认证。

如发现认证委托人、个人信息处理者存在欺骗、隐瞒信息、故意违反认证要求等严重影响认证实施的行为时，认证不予通过。

获证后监督

认证机构应当在认证有效期内，对获得认证的个人信息处理者进行持续监督，并合理确定监督频次。

认证机构应当采取适当的方式实施获证后监督，确保获得认证的个人信息处理者持续符合认证要求。

认证机构对获证后监督结论和其他相关资料信息进行综合评价，评价通过的，可继续保持认证证书；不通过的，认证机构应当根据相应情形作出暂停直至撤销认证证书的处理。

认证依据

1、认证依据：个人信息处理者不仅应当符合GB/T 35273《信息安全技术 个人信息安全规范》的要求，还需符合TC260-PG-2-222A《个人信息跨境处理活动安全认证规范》的要求。

2、组织管理：开展个人信息跨境处理活动的个人信息处理者与境外接受方均需既要指定个人信息保护负责人，又要设立个人信息保护机构。

3、处理规则：处理规则包括跨境处理个人信息的基本情况、目的、方式和范围、存储时间、中转国家、保障个人信息主体权益所需资源和措施及个人信息安全事件的赔偿、处置规则，且个人信息跨境处理者和境外接收方应约定并共同遵守同一个人信息跨境处理规则。

4、个人信息保护影响评估：个人信息处理者应对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估，并形成个人信息保护影响评估报告，评估报告至少保存3年。

5、获证后监督：个人信息处理者在通过个人信息保护认证后，还应进行必要的管理与技术投入，以确保“持续符合”各项监督评价要求。

6、有效期内变更：若获得认证的个人信息处理者名称、注册地址，或认证要求、认证范围等发生变化时，认证委托人应当向认证机构提出变更委托。

7、认证时限：认证机构应当对认证各环节的时限作出明确规定，并确保相关工作按时限要求完成。认证委托人应当对认证活动予以积极配合。

个人信息出境标准合同

备案流程

根据《个人信息出境标准合同办法》、《促进和规范数据跨境流动规定》，个人信息处理者通过订立标准合同的方式向境外提供个人信息，同时符合下列情形的应当向所在地省级网信部门备案：关键信息基础设施运营者以外的数据处理者；自当年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）的；自当年1月1日起，累计向境外提供不满1万人敏感个人信息的。其中，特别强调，个人信息处理者不得采取数量拆分等手段，将依法应当通过出境安全评估的个人信息通过订立标准合同的方式向境外提供。

个人信息出境标准合同只有按流程通过备案，才能符合数据跨境合规要求。个人信息处理者应当在标准合同生效之日起10个工作日内，通过数据出境申报系统备案，系统网址为https://sjcj.cac.gov.cn。标准合同备案流程包括材料提交、材料查验及反馈备案结果、补充或者重新备案等环节。

1、材料提交。个人信息处理者备案标准合同，应提交承诺书、标准合同、以及《个人信息保护影响评估报告》。

2、材料查验及反馈备案结果。省级网信办应当自个人信息处理者提交备案材料之日起15个工作日内完成材料查验，并向符合备案要求的个人信息处理者发放备案编号。需要补充完善材料的，个人信息处理者应当在10个工作日内提交补充完善材料；逾期未补充完善材料的，可以终止本次备案程序。

3、补充或者重新备案。在标准合同有效期内出现下列情形之一的，个人信息处理者应当重新开展个人信息保护影响评

估，补充或者重新订立标准合同，并履行相应备案手续：一是向境外提供个人信息的目的、范围、种类、敏感程度、方式、保存地点或者境外接收方处理个人信息的用途、方式发生变化，或者延长个人信息境外保存期限的；二是境外接收方所在国家或者地区的个人信息保护政策和法规发生变化等可能影响个人信息权益的；三是可能影响个人信息权益的其他情形。个人信息处理者在标准合同有效期内补充订立标准合同的，应当向所在地省级网信办提交补充材料；重新订立标准合同的，应当重新备案。补充或者重新备案的材料查验时间为15个工作日。

评估报告

个人信息安全影响评估旨在发现、处置和持续监控个人信息处理过程中对个人信息主体合法权益造成不利影响的风险。针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。

个人信息处理者备案个人信息出境标准合同时需提供个人信息保护影响评估报告，并对所提交的评估报告真实性负责；报告所述评估工作为本次申报前3个月内完成；如有第三方机构参与评估，须在评估报告中说明第三方机构的基本情况及参与评估的情况。

根据评估结果，展个人信息处理的组织可实施适当的安全控制措施，从而降低收集和处理个人信息的过程中对个人信息主体权益造成的不利影响；并根据组织的业务现状和可预期的变化、对个人信息安全可能产生威胁的内外部因素、有关法律法规标准要求等内外部因素的定期评估，持续修正个人信息安全控制措施，使个人信息收集、处理过程对个人合法权益不利影响的风险处于总体可控的状态。

个人信息安全影响评估一般作为事前预防机制，识别对个人信息主体权益的风险，实施有针对性的保护措施。个人信息安全影响评估有助于在工作开展的初期识别个人信息安全问题，通过尽早考虑、分析和处理个人信息安全问题，降低组织的时间管理成本、法律风险以及潜在的声誉或公众问题。

个人信息安全影响评估的基本实施流程，包括评估准备阶段、分析阶段、评估报告阶段、风险处置和持续改进阶段、评估报告发布阶段。其中，分析阶段应至少包括必要性分析、数据映射分析、个人权益影响分析、安全事件可能性分析和风险分析等环节。

《个人信息保护影响评估报告（模板）（出境版）》分为出境活动整体情况和拟出境活动的影响评估情况及结论。

出境活动整体情况

（1）个人信息处理者基本情况，包括：股权结构、实际控制人、境内外投资情况、组织架构和个人信息保护机构信息等；整体业务与处理个人信息情况；以及拟出境个人信息情况等。

其中，拟出境个人信息情况，具体包括：个人信息出境涉及业务、个人信息收集使用、信息系统等情况；个人信息处理者和境外接收方处理个人信息的目的、范围、方式，及其合法性、正当性、必要性；出境个人信息的规模、范围、种类、敏感程度，处理敏感个人信息情况；拟出境个人信息在境内存储的系统平台、数据中心等情况，个人信息出境链路相关情况，计划出境后存储的系统平台、数据中心等；个人信息出境后向境外其他接收方提供的情况。

（2）境外接收方情况，包括：境外接收方基本情况；境外接收方处理个人信息的用途、方式等；境外接收方履行责任义务的管理和技术措施、能力等。

（3）个人信息处理者认为需要说明的其他情况。

拟出境活动的影响评估情况及结论

对照《个人信息出境标准合同办法》第五条规定事项，说明个人信息保护影响评估情况，重点说明评估发现的问题和整改情况。

数据出境场景个人信息保护影响评估，重点评估以下内容：个人信息处理者和境外接收方处理个人信息的目的、范围、方式等的合法性、正当性、必要性；出境个人信息的规模、范围、种类、敏感程度，个人信息出境可能对个人信息权益带来的风险；境外接收方承诺承担的义务，以及履行义务的管理和技术措施、能力等能否保障出境个人信息的安全；个人信息出境后遭到篡改、破坏、泄露、丢失、非法利用等的风险，个人信息权益维护的渠道是否通畅等；数据接收国个人信息保护政策和法规对合同履行的影响；其他可能影响个人信息出境安全的事项。

综合影响评估情况和相应整改情况，对个人信息出境活动作出客观的影响评估结论，充分说明得出评估结论的理由和论据。

合同内容

根据《个人信息出境标准合同（模板）》，标准合同主要约定个人信息处理者的义务、境外接收方的义务、境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响、个人信息主体的权利等事项。

个人信息处理者义务

一是遵循告知同意和最小必要原则。按照相关法律法规规定处理个人信息，向境外提供的个人信息仅限于实现处理目的所需的最小范围。向个人信息主体告知境外接收方的名称或者姓名、联系方式、处理目的、处理方式、个人信息的种类、保存期限，以及行使个人信息主体权利的方式和程序等事项。向境外提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。向个人信息主体告知其与境外接收方通过本合同约定个人信息主体为第三方受益人，如个人信息主体未在30日内明确拒绝，则可以依据本合同享有第三方受益人的权利。

二是安全保障义务。综合考虑个人信息处理目的、个人信息的种类、规模、范围及敏感程度、传输的数量和频率、个人信息传输及境外接收方的保存期限等可能带来的个人信息安全风险），合理确保境外接收方采取加密、匿名化、去标识化、访问控制等技术和管理措施。

三是开展个人按照相关法律法规对拟向境外接收方提供个人信息的活动开展个人信息保护影响评估。保存个人信息保护影响评估报告至少3年。

境外接收方的义务

境外接收方应当履行下列义务：

（1）按约定处理个人信息。如超出约定的处理目的、处理方式和处理的个人信息种类，基于个人同意处理个人信息的，应当事先取得个人信息主体的单独同意；涉及不满十四周岁未成年人个人信息的，应当取得未成年人的父母或者其他监护人的单独同意。

（2）受个人信息处理者委托处理个人信息的，应当按照与个人信息处理者的约定处理个人信息，不得超出与个人信息处理者约定的处理目的、处理方式等处理个人信息。

（3）根据个人信息主体的要求向个人信息主体提供本合同的副本。如涉及商业秘密或者保密商务信息，在不影响个人信息主体理解的前提下，可对本合同副本相关内容进行适当处理。

（4）采取对个人权益影响最小的方式处理个人信息。

（5）个人信息的保存期限为实现处理目的所必要的最短时间，保存期限届满的，应当删除个人信息（包括所有备份）。受个人信息处理者委托处理个人信息，委托合同未生效、无效、被撤销或者终止的，应当将个人信息返还个人信息处理者或者予以删除，并向个人信息处理者提供书面说明。删除个人信息从技术上难以实现的，应当停止除存储和采取必要的安全保护措施之外的处理。

（6）按下列方式保障个人信息处理安全：采取技术和管理措施，并定期进行检查，确保个人信息安全；确保授权处理个人信息的人员履行保密义务，并建立最小授权的访问控制权限。

（7）如处理的个人信息发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问，应当开展下列工作：及时采取适当补救措施，减轻对个人信息主体造成的不利影响；立即通知个人信息处理者，并根据相关法律法规要求报告监管机构；记录并留存所有与发生或者可能发生篡改、破坏、泄露、丢失、非法利用、未经授权提供或者访问有关的情况，包括采取的所有补救措施。

（8）同时符合下列条件的，方可向中华人民共和国境外的第三方提供个人信息：确有业务需要；已告知个人信息主体该第三方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向第三方提供敏感个人信息的，还应当向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外；基于个人同意处理个人信息的，应当取得个人信息主体的单独同意；与第三方达成书面协议，确保第三方的个人信息处理活动达到中华人民共和国相关法律法规规定的个人信息保护标准，并承担因向中华人民共和国境外的第三方提供个人信息而侵害个人信息主体享有权利的法律责任；根据个人信息主体的要求向个人信息主体提供该书面协议的副本。

（9）受个人信息处理者委托处理个人信息，转委托第三方处理的，应当事先征得个人信息处理者同意，要求该第三方不得超出本合同附录一“个人信息出境说明”中约定的处理目的、处理方式等处理个人信息，并对该第三方的个人信息处理活动进行监督。

（10）利用个人信息进行自动化决策的，应当保证决策的透明度和结果公平、公正，不得对个人信息主体在交易价格等交易条件上实行不合理的差别待遇。通过自动化决策方式向个人信息主体进行信息推送、商业营销的，应当同时提供不针对其个人特征的选项，或者向个人信息主体提供便捷的拒绝方式。

（11）承诺向个人信息处理者提供已遵守本合同义务所需的必要信息，允许个人信息处理者对必要数据文件和文档进行查阅，或者对本合同涵盖的处理活动进行合规审计，并为个人信息处理者开展合规审计提供便利。

（12）对开展的个人信息处理活动进行客观记录，保存记录至少3年，并按照相关法律法规要求直接或者通过个人信息处理者向监管机构提供相关记录文件。

（13）同意在监督本合同实施的相关程序中接受监管机构的监督管理，包括但不限于答复监管机构询问、配合监管机构检查、服从监管机构采取的措施或者作出的决定、提供已采取必要行动的书面证明等。

境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响

（1）双方应当保证在本合同订立时已尽到合理注意义务，未发现境外接收方所在国家或者地区的个人信息保护政策和法规（包括任何提供个人信息的要求或者授权公共机关访问个人信息的规定）影响境外接收方履行本合同约定的义务。

（2）结合下列情形进行评估：

一是出境的具体情况，包括个人信息处理目的、传输个人信息的种类、规模、范围及敏感程度、传输的规模和频率、个人信息传输及境外接收方的保存期限、境外接收方此前类似的个人信息跨境传输和处理相关经验、境外接收方是否曾发生个人信息安全相关事件及是否进行了及时有效地处置、境外接收方是否曾收到其所在国家或者地区公共机关要求其提供个人信息的请求及境外接收方应对的情况。

二是境外接收方所在国家或者地区的个人信息保护政策和法规，包括下列要素：该国家或者地区现行的个人信息保护法律法规及普遍适用的标准；该国家或者地区加入的区域性或者全球性的个人信息保护方面的组织，以及所作出的具有约束力的国际承诺；该国家或者地区落实个人信息保护的机制，如是否具备个人信息保护的监督执法机构和相关司法机构等。

三是境外接收方安全管理制度和技术手段保障能力。

（3）境外接收方保证，在根据本条第二项进行评估时，已尽最大努力为个人信息处理者提供了必要的相关信息。

（4）双方应当记录根据本条第二项进行评估的过程和结果。

因境外接收方所在国家或者地区的个人信息保护政策和法规发生变化（包括境外接收方所在国家或者地区更改法律，或者采取强制性措施）导致境外接收方无法履行本合同的，境外接收方应当在知道该变化后立即通知个人信息处理者。

境外接收方接到所在国家或者地区的政府部门、司法机构关于提供本合同项下的个人信息要求的，应当立即通知个人信息处理者。

个人信息主体的权利

双方约定个人信息主体作为本合同第三方受益人享有以下权利：

（1）个人信息主体依据相关法律法规，对其个人信息的处理享有知情权、决定权，有权限制或者拒绝他人对其个人信息进行处理，有权要求查阅、复制、更正、补充、删除其个人信息，有权要求对其个人信息处理规则进行解释说明。

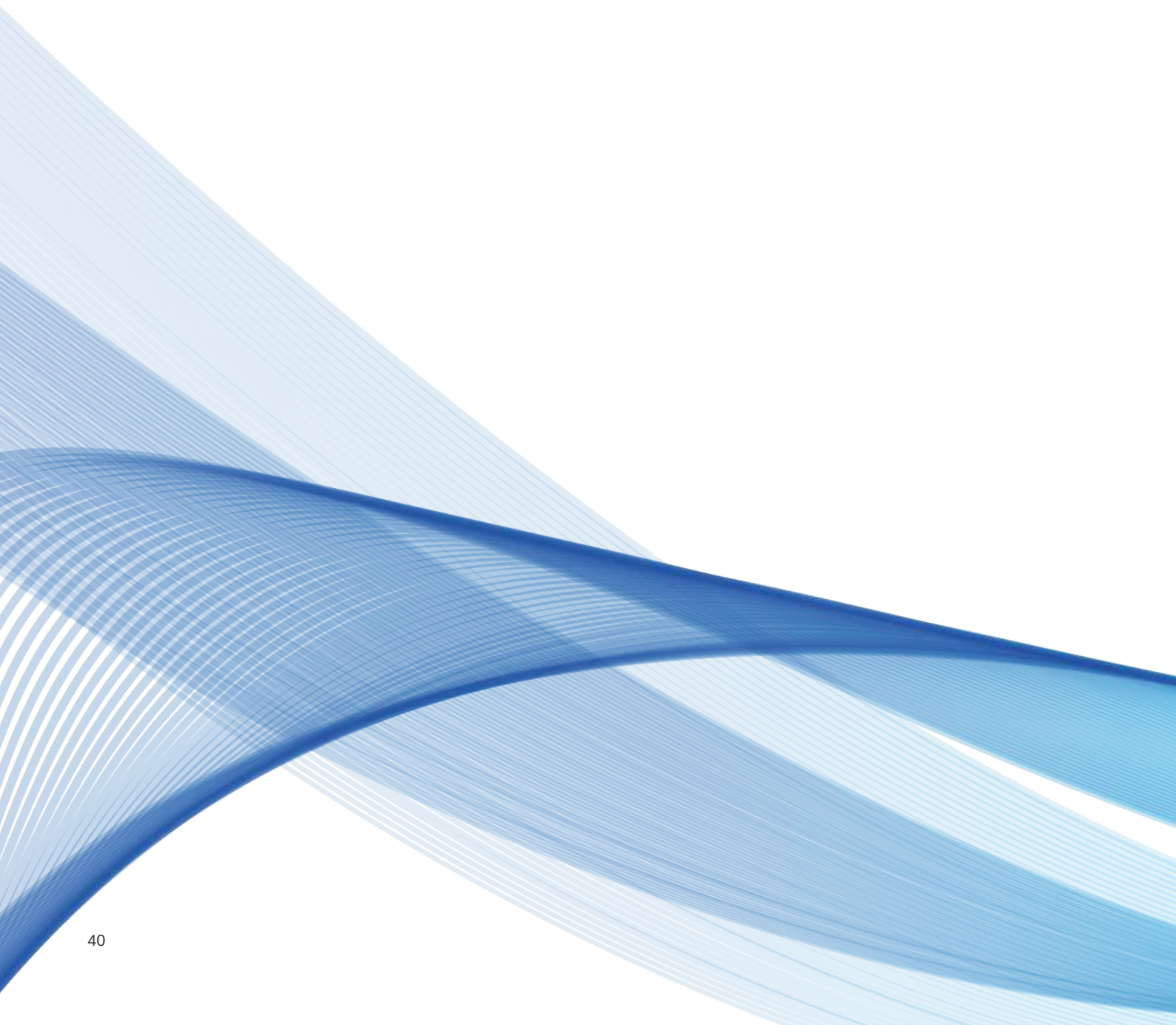
（2）当个人信息主体要求对已经出境的个人信息行使上述权利时，个人信息主体可以请求个人信息处理者采取适当措施实现，或者直接向境外接收方提出请求。个人信息处理者无法实现的，应当通知并要求境外接收方协助实现。

（3）境外接收方应当按照个人信息处理者的通知，或者根据个人信息主体的请求，在合理期限内实现个人信息主体依照相关法律法规所享有的权利。

境外接收方应当以显著的方式、清晰易懂的语言真实、准确、完整地告知个人信息主体相关信息。

境外接收方拒绝个人信息主体的请求的，应当告知个人信息主体其拒绝的原因，以及个人信息主体向相关监管机构提出投诉和寻求司法救济的途径。

企业数据跨境安全合规指引 2024



第四章
自贸区数据跨境试点

自贸区数据跨境试点概况

在数字化浪潮的推动下，推进数据跨境流动是推动更高水平对外开放的必然要求，也是优化营商环境的现实需要。早在2020年8月，商务部发布《关于印发全面深化服务贸易创新发展试点总体方案的通知》，提出全面探索提升便利水平，推动数字营商环境便利化。对标国际高标准高水平，探索构建与我国数字经济创新发展相适应、与我国数字经济国际地位相匹配的数字营商环境。在条件相对较好的试点地区开展数据跨境传输安全管理试点。在试点任务、具体举措及责任分工当中，支持北京、上海、海南、雄安新区等试点开展数据跨境流动安全评估，建立数据保护能力认证、数据流通备份审查、跨境数据流动和交易风险评估等数据安全管理机制。鼓励有关试点地区参与数字规则国际合作，加大对数据的保护力度。2023年7月，国务院发布了《关于进一步优化外商投资环境　加大吸引外商投资力度的意见》进一步强调支持北京、天津、上海、粤港澳大湾区等地“探索便利化的数据跨境流动安全管理机制”。

我国数据跨境政策中，明确鼓励自贸区开展数据跨境先试先行。国家互联网信息办公室发布的《数据出境安全评估办法》和《促进和规范数据跨境流动规定》为数据跨境流动提供了清晰的指导和框架，指出自由贸易试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单等。数据跨境政策实施以来，北京、上海、天津、海南等自由贸易试验区在这一领域展开了积极的探索和实践，这些试验区不仅是连接国内外数据流动的桥梁，更是推动数据要素市场化和国际化的重要引擎。

北京自由贸易区

中国（北京）自由贸易试验区，实施范围119.68平方公里，涵盖科技创新、国际商务服务、高端产业三个片，包括国际商务服务片区48.34平方公里（含北京天竺综合保税区5.466平方公里），高端产业片区39.49平方公里，科技创新片区31.85平方公里。2022年3月，《中国（北京）自由贸易试验区条例》出台，提到自贸试验区将在风险可控的前提下，开展数字领域的国际合作，促进数据跨境传输、数字产品安全检测与认证、数据服务市场安全有序开放等领域互惠互利、合作共赢，推动数字贸易港建设。

2023年11月，北京数据基础制度先行区启动运行，将按照适应数据要素和数字经济特征的新型监管方式建立先行先试机制。《北京数据基础制度先行区政策清单》提出多项举措，包括：支持数据跨境流动服务机构，为数据先行区范围内的市场主体开展的数据跨境流动业务，提供一站式绿色通道服务；支持开展数据跨境流动国际合作，开展国际数据流动规则和标准研究，鼓励参与或成立国际数据组织和开源技术；鼓励行业龙头企业联合相关专业研究机构开展国际数据空间创建，开展数据空间测试等服务。

在政策制定上，北京自由贸易区深化服务业扩大开放中加强数据安全管理，支持设立跨国机构数据流通服务窗口，以合规服务方式优先实现集团内数据安全合规跨境传输。制定自动驾驶、生物基因等行业数据分类分级指南和重要数据目录，以重点领域企业数据出境需求为牵引，明确重要数据识别认定标准。

在平台建设上，积极建设数据跨境技术创新平台。大兴机场临空区于去年7月发布“国际数据合作合规编码与登记平台”，首创国际数据合作合规登记服务体系。同月，北京国际数据实验室、国际数据空间协会中国能力中心也揭牌成立。北京国际数据实验室由下一代互联网国家工程中心牵头建设，开展数据安全和数据跨境服务平台研究与建设，推动基于IPv6的数据专网和数据空间平台研究与建设。国际数据空间协会中国能力中心开展数据空间的技术研发和标准建立，促进数据领域的国际交流与合作。

在实施案例上，北京自贸区数据跨境试点在不同领域已有多项案例。2023年1月，首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目被审批通过，标志着全国首个数据合规出境案例在北京完成，也标志着国家数据出境安全评估制度在北京市率先落地。

2023年6月，北京德亿信数据有限公司与香港诺华诚信有限公司签订的个人信息出境标准合同通过市网信办组织的备案审核，成为首家通过订立标准合同实现个人信息合规出境的企业，标志着个人信息出境标准合同备案制度在北京率先落地。

2024年2月，国家网信办正式批复拜耳公司申报的药物警戒、临床试验等业务场景通过安全评估，标志着全国首个外资医药企业核心业务完整获批案例在北京落地。据悉，在总结拜耳模式的基础上，北京市网信办与大兴组团加强协作，提出外商投资企业数据出境“绿色通道”服务机制，会同有关行业部门开展联合会诊，帮助企业精准理解监管要求，针对性解决外资企业反映的数据出境合规共性问题，提升工作效率。目前，“绿色通道”已覆盖汽车、医药、民航、零售、人工智能5个行业117家企业，全面助力企业合规提质增效。企业经“绿色通道”通过数据出境安全评估时长平均缩短约50%。

上海自由贸易区

中国（上海）自由贸易试验区，是中国政府设立在上海的区域性自由贸易园区，位于浦东境内，属中国自由贸易区范畴。自贸区面积120.72平方公里。扩展区域包括陆家嘴金融片区、金桥开发片区和张江高科技片区。上海自贸区加快数字贸易和数据跨境产业集聚发展，打造国际数据经济产业园。

2023年1月，临港新片区《国际数据产业专项规划（2023-2025年）》提到，2025年临港国际数据产业规模超200亿元，特别是发展“两头在外”“来料加工”的国际数据加工、交换中心等业务。

2023年7月，上海发布《推动数据要素产业创新发展行动方案(2023-2025年)》，提出“新建直达东亚和东南亚的海光缆，布局面向国际数据合作的高等级数据中心”。探索数据跨境制度创新，研究编制场景清单和操作指引，优化临港数据跨境服务产业布局，大力发展数据跨境服务业。

2023年10月，上海市发布《中国（上海）国际贸易单一窗口智慧化创新行动方案》，提出了“区块链+大数据+大模型”相融合的航贸目标。

2023年10月27日，在临港新片区召开国际数据经济产业合作大会，临港管委会发布《国际数据经济产业园实施方案》提出，国际数据经济产业园将建设成为高水平国际数据合作桥头堡、高标准数据跨境制度创新先行区、高质量国际数据

产业集聚地和高能级数据流通基础设施新枢纽。到2025年，产业园将重点打造形成10个高能级国际数据合作平台，50个以上数据便捷流动和国际合作创新场景，集聚100家头部企业，达到1000亿元的数据产业规模。

金融数据出境向高水平开放迈出新步。2023年11月，国务院发布《全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案》。方案指出，在国家数据跨境传输安全管理制度框架下，允许金融机构向境外传输日常经营所需的数据。涉及金融数据出境的，监管部门可基于国家安全和审慎原则采取监管措施，同时保证重要数据和个人信息安全。

2023年12月7日，国务院印发《全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案》（国发〔2023〕23号），赋予上海“打造国家制度型开放示范区”的新使命。《总体方案》要求上海自贸区率先实施高标准数字贸易规则，支持上海自贸试验区率先制定重要数据目录，并探索建立合法安全便利的数据跨境流动机制。

2024年1月，在临港新片区举行了国际数据经济产业创新大会，会上发布了《临港新片区数据跨境流动分类分级管理办法（试行）》，将跨境数据分为核心数据、重要数据、一般数据3个级别进行分级管理。同时，临港新片区将加强与DEPA（《数字经济伙伴协定》）国家数字贸易领域合作，积极创建DEPA合作示范区，推动“无纸化贸易”等规则在临港新片区落地；在航运贸易领域，率先探索电子提单、电子信用证等在贸易支付结算、单证融资、供应链金融等场景中的应用；搭建数字身份跨境互操作服务平台，打造数字身份跨境认证枢纽；探索开展数据出境标准合同与个人信息保护认证与国际互认试点，推动相关领域应用场景落地。

2024年2月3日，上海市政府印发了《上海市落实<全面对接国际高标准经贸规则推进中国（上海）自由贸易试验区高水平制度型开放总体方案>的实施方案》，其中在规范和促进数据跨境流动方面，提出率先制定重要数据目录、探索建立合法安全便利的数据跨境流动机制、在临港新片区建立数据跨境服务中心等措施。在促进数据开放共享方面，提出要建设国际开源促进机构、加大公共数据开放范围和力度、促进中小企业加强与境外机构在数字经济领域交流、加强数字包容性国际合作等措施。同时，临港新片区出台了“数据流动操作指引”，率先建立“事前评估备案、事中备份存证、事后抽查核验”的全流程数据跨境流动管理机制，探索了近50个数据跨境便捷流通场景。

2024年5月17日，中国（上海）自由贸易试验区临港新片区发布数据跨境场景化一般数据清单及清单配套操作指南。首批一般数据清单包含智能网联汽车、公募基金、生物医药3个领域，涉及智能网联汽车跨国生产制造、医药临床试验和研发、基金市场研究信息共享等11个场景，划分成64个数据类别600余个字段。

天津自由贸易区

中国（天津）自由贸易试验区是经国务院批准设立的中国北方第一个自贸试验区，区域面积119.9平方公里，全部位于滨海新区辖区范围之内，2015年4月21日正式运行。2015年4月，《中国（天津）自由贸易试验区总体方案》出台，对加快政府职能转表、扩大投资领域开放、推动贸易转型升级、深化金融领域开放创新、推动实施京津冀协同发展战略等方面做出了重要部署。2018年5月，国务院发布《进一步深化中国（天津）自由贸易试验区改革开放方案》，并表示支持海关、外汇等部门开展数据交换合作，鼓励自贸试验区内符合资质要求的保理企业开展离岸、跨境、跨省市国际保理业务。

2024年2月，天津市商务局、中国（天津）自由贸易试验区管委会联合发布了数据分类分级标准规范《中国（天津）自由贸易试验区企业数据分类分级标准规范》。该规范适用于天津自贸试验区内企业在生产经营过程中产生、收集、存储、传输和处理的数据的分类分级，将企业数据分成13大类40子类，从高到低分为核心、重要、一般3个级别，明确了重要数据的识别标准。

2024年5月，中国（天津）自由贸易试验区管理委员会、天津市商务局会同有关部门制定了首份自贸试验区数据出境负面清单。《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024版）》列明了天津自贸试验区企业向境外提供数据需要申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形。围绕生物医药、服务外包、金融、互联网平台、汽车、集成电路、气象、国际贸易等自贸试验区8大重点领域产业发展和监管需要，将企业出境数据分为战略物资和大宗商品类、自然资源和环境类、工业类、金融类等13个大类46个子类，并对每一类数据基本特征做出了详细描述。

粤港澳大湾区

粤港澳大湾区的设立旨在进一步推动粤港澳三地的经济合作，充分发挥区域内科技创新、高端制造、金融服务等优势，打造具有国际竞争力的世界级城市群，涵盖广东省的九个城市（广州、深圳、珠海、佛山、东莞、中山、惠州、江门、肇庆）以及香港特别行政区和澳门特别行政区，总人口超过7000万，是中国经济最发达、开放程度最高的区域之一。

由于香港、澳门与内地有不同的法律制度和政策，设立大湾区的目标之一是通过制度创新和政策协调，增强区域内的联通性与资源的高效配置。如何在大湾区内部及跨境管理数据流动是一个重要的议题，尤其在全球数据安全和隐私保护要求日益严格的背景下。

2021年7月，广东省发布《广东省数据要素市场化配置改革行动方案》提出，推动粤港澳大湾区数据有序流通，支持广州南沙（粤港澳）数据要素合作试验区、珠海横琴粤澳深度合作区建设，开展跨境数据流通的审查、评估、监管等工作。

2023年11月，广东省发布《“数字湾区”建设三年行动方案》，提出“探索推行数据跨境流通‘白名单’制度，通过纳入数据授权跨境目录、数据主体授权等模式，实现数据安全有序跨境。建设全国一体化算力网络粤港澳大湾区国家枢纽韶关数据中心集群，探索在特定区域建设离岸数据中心，为粤港澳三地提供数据跨境服务”。

2023年12月，国家互联网信息办公室、香港创新科技及工业局发布《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》，为促进粤港澳大湾区个人信息跨境安全有序流动，推动粤港澳大湾区高质量发展奠定基础。粤港澳大湾区数据保护和数据跨境服务平台正式上线，平台提供“数据跨境合规”“APP合规”“数据交易流通”“企业数据合规治理”以及“合规能力提升”五大核心解决方案，并提供关于粤港澳大湾区数据跨境流动便利化政策的专项服务等。粤港澳数据合作会议专家委员会同期成立，专家们为粤港澳数据跨境流通相关的产业及技术发展建言献策。

2024年1月，广东省发布《中国（广东）自由贸易试验区提升战略行动方案》，强调促进数据跨境安全有序流动。支持南沙（粤港澳）数据服务试验区、国际海缆登陆站、区域性国际互联网出入口局建设。推进前海全业务关口局、互联网骨干直联点、中新国际互联网数据专用通道、海缆登陆站服务区建设。支持横琴打造国际数据合作产业发展集聚区，启动澳门科技大学—大湾区科研数据跨境专网试点。

2024年3月，国务院办公厅印发《扎实推进高水平对外开放更大力度吸引和利用外资行动方案》，提到支持外商投资企业与总部数据流动，规范数据跨境安全管理，组织开展数据出境安全评估、规范个人信息出境标准合同备案等相关工作，促进外商投资企业研发、生产、销售等数据跨境安全有序流动。制定粤港澳大湾区跨境数据转移标准，依托横琴粤澳深度合作区、前海深港现代服务业合作区等重大合作平台，建立港澳企业数据跨境流动机制，探索建立跨境数据流动“白名单”制度，稳步推动实现粤港澳大湾区内数据便捷流动。

2024年5月，深圳前海上线了全国首个内地香港跨境数据验证平台-深港跨境数据验证平台。该平台致力于打造深港两

地新型数字化跨境服务基础设施，基于国产开源区块链底层技术（FISCO BCOS）和分布式数据传输协议（DDTP）进行开发，运用区块链不可篡改且可追溯的技术优势，以哈希值跨境验证实现用户自主携带资料的可信验证。

深港跨境数据验证平台的优势在于较好地解决了数据泄露、数据滥用和数据可信三大问题，避免了过度授权、数据过度采集、第三方机构泄露数据等情况发生。横琴则表示将依托横琴超算中心、粤澳跨境数据验证平台等数字基础设施，探索建立跨境数据流动的标准和机制。

海南自由贸易港

海南自由贸易港是国家在海南岛全岛设立的自由贸易港。2020年6月，国务院发布《海南自由贸易港建设总体方案》，提出“在国家数据跨境传输安全管理制度框架下，开展数据跨境传输安全管理试点，探索形成既能便利数据流动又能保障安全的机制”。

2024年1月，海南省发布《海南省培育数据要素市场三年行动计划（2024—2026）》，在数据跨境应用方面，提出利用自贸港数据安全有序流动的政策优势，主动对接高标准国际经贸规则，支持海南在《数字经济伙伴关系协定》（DEPA）等规则方面先行先试。在贸易、航天、深海、医疗等领域形成一批跨境典型应用案例，打造国际数据要素市场体系。利用国际海缆、国际数据中心、海底数据中心、智算中心等基础设施，探索培育游戏出海、跨境直播、跨境贸易等典型应用。在数据产业方面，提出将海南打造为国际数据特区，在海南谋划中国国际数据要素产业服务大会，在海南发展中国国际数据服务外包基地、中国数据知识转化研究培训胜地、数据智慧(人工智能)产业应用创新高地，培育以数据要素为核心的自贸港特色产业。

2024年5月，海南省工业和信息化厅发布《海南自由贸易港数字经济促进条例》，明确表示将引进跨国公司和大型互联网企业在海南自由贸易港建设数据中心，探索发展国际数据中心，支持开展跨境数据处理、算力租售等服务；支持设立海南自由贸易港国际数据交易场所，培育数据要素市场，依法建立数据资源流通交易监管制度及机制，鼓励和引导数据供需双方在数据交易场所进行交易。

北京自贸区数据跨境实践

为积极用好自贸试验区可自行制定数据出境负面清单的政策红利，经国家数据安全工作协调机制和北京市委网信委批准，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局会同有关部门与2024年8月30日制定发布了《中国（北京）自由贸易试验区数据出境负面清单管理办法（试行）》（本节简称《管理办法》）、《中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版）》（本节简称《负面清单》），并通过国家网信办、国家数据局备案。上述数据出境政策适用于在北京自贸试验区内登记注册、开展数据跨境流动等相关活动的企业、事业单位、机构、团体或其他组织。这标志着北京市数据跨境便利化服务改革取得重大突破，形成了高效便利安全的数据跨境流动“北京实践”。

《管理办法》重点围绕负面清单的制定流程、职责分工、使用管理、安全监管等方面进行深化设计，是制定负面清单和开展日常监管的基本规范，并同步完善了重要数据识别规则，提出13类41子类数据分类分级参考规则，助力企业提升识别能力。《负面清单》首批选取汽车、医药、零售、民航、人工智能5个领域，详细列举23个业务场景和198个具体字段。主管部门将采取动态管理机制，未来将分行业、分领域、分批次推进清单编制工作，持续优化迭代负面清单政策体系。

在管理流程上，数据处理者根据负面清单出境数据时，需向相应的自贸组团提交申请，自贸组团会对数据处理者提交的申请材料进行审核并在5个工作日内反馈审核结果，并协助通过审核的数据处理者开展负面清单使用备案、指导数据处理者申报安全评估、标准合同备案、开展个人信息保护认证。

重要数据识别规则

《管理办法》规定了自贸区数据分类分级参考规则，提出重要数据统一识别参考规则以及13类41子类数据分类分级参考规则。

重要数据识别规则包括个人信息、高价值敏感数据、关键信息基础设施相关数据等类型。首先，企业掌握的 1000 万人以上个人信息（不含敏感个人信息），100 万人以上敏感个人信息，10 万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息。其次，关键信息基础设施运营者掌握的 10 万人以上个人信息。第三，北京自贸试验区企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据，涉及国家安全的企业供应链相关数据。第四，北京自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。

《数据分类分级参考规则》所提出的重要数据识别规则符合重要数据的定义，考察该数据一旦泄露或非法利用是否可能“危害国家安全、经济运行、社会稳定、公共健康和安全”。在此基础上，《负面清单》针对不同行业的重要数据类型提供了更具体的字段描述。后续《负面清单》将结合相关行业主管部门制定的重要数据目录以及行业需求动态更新。

典型场景负面清单

北京自由贸易试验区在负面清单的分行业推进策略上，充分体现了以企业需求为导向的政策制定原则，并通过灵活的动态调整机制和试点示范作用，提升了政策的适应性和执行效果。通过针对不同领域的具体需求进行政策设计，可以更好地满足企业的实际运营需求，提高政策的适应性和有效性。综合考虑数据出境需求迫切的重大场景、全市重点产业布局等因素，按照“急用先行、小步快跑”原则，首批选择汽车、医药、零售、民航、人工智能等5个领域率先制定，详细列明23个业务场景和198个具体字段，便于企业准确识别判断。后续，按照动态管理机制，分行业、分领域、分批次推进编制工作，成熟一批发布一批，持续优化迭代负面清单政策体系。

随着技术的进步和市场环境的变化，企业的数据需求和风险状况也在不断变化。北京自贸区的负面清单采取动态调整机制，能够根据市场和技术的发展不断更新和优化。这种灵活性使政策能够更好地适应快速变化的市场环境，为企业提供了更大的操作空间和灵活性。不仅能够帮助企业更好地应对国际市场的变化，也有利于促进国内产业的创新发展和技术进步。

汽车行业

根据《负面清单》，汽车行业的7类重要数据及2类个人信息需要通过安全评估开展数据出境；2类个人信息需要通过标准合同备案、个人信息保护认证出境。《负面清单》适用于汽车制造商、零部件和软件供应商、经销商、维修机构以及出行服务企业等，“自动驾驶领域相关企业不适用本清单”。

（1）涉及重要数据出境的情形

《汽车数据安全管理若干规定（试行）》规定了汽车行业的重要数据类别，《负面清单》在此基础上明确了部分类别重要数据的应用场景，并对其定义与范围提供了字段级的说明。

1）涉及军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据。在向政府机关、军工企业及其他敏感重要机构提供车联网信息服务过程中产生的不宜公开信息。其中，重要敏感区域的地理信息包括涉及的车辆精准坐标、行踪轨迹，也包括该等区域的地址。针对确需处理客户网联数据的情况，企业通常采取严格的权限管控措施、制定客户数据管理制度，规范访问、分析、使用敏感重要机构客户数据的行为，包括限制相关数据出境活动。

2）涉及车辆流量、物流等反映经济运行情况的数据。根据《负面清单》，车流数据包括路面交通流量数据，物流数据包括物品流转精确路径信息。开展货运、物流业务的企业通常需要实施监控并记录物流车辆的精准定位与行踪轨迹，并在地图上可视化展示相关路径，这种情况下可能涉及处理物品流转精确路径信息。若相关物流监控平台部署在境外、或由境外技术团队负责运维，则可能涉及物流数据出境。

3）能够反映一定区域内汽车充电网运行情况的数据。在《负面清单》提供的字段级描述中，充电桩/站位置信息、使用状态属于典型的电网运行情况相关字段，除此之外，计费和支付信息也属于重要数据的范围。除原始数据外，充换电车

辆统计信息、站点统计、分布信息等统计类型数据也会被纳入重要数据的范围。实践中，充电行业企业处理的数据类型相较《负面清单》提供的字段示例可能颗粒度更细，例如充电订单号、充电设备接口编码、开始/结束充电时间、电费金额、服务费金额，根据《负面清单》目前的规定，该等数据可能均会落入“计费和支付信息”的范畴，构成重要数据。此外，在重要数据统一识别参考规则的基础上，《负面清单》进一步将这一类别的重要数据限定为“能够反映一定区域”充电网运行情况的数据，如何划定该等“区域”的范围，有待主管部门进一步明确。

4）涉及人脸信息、车牌信息、路牌信息等的车外视频、图像数据。《负面清单》将包含路牌的车外视频、图像数据也纳入重要数据的监管范围，这意味着企业数据匿名化的范围将从人脸、车牌信息延伸至路牌信息。

5）涉及车辆远程操控、车辆工况等的关键车联网信息服务数据。根据《负面清单》，这类重要数据包括身份鉴权信息、车辆远程操控类信息、车辆工况类数据、涉车服务类数据、车联网服务平台基础属性数据、车辆外部环境感知数据。

6）涉及车辆控制等在线升级数据（OTA）。《负面清单》列举了OTA在线升级场景的各类重要数据字段，包括电控单元信息、固件配置信息、重编程相关数据、诊断仪数据、车辆钥匙相关数据等。同时，《负面清单》针对在线升级数据的认定作出了豁免，规定已在工信部备案并通过相关安全技术措施处理可确保升级包数据不被篡改的情形除外。

7）其他类型重要数据。可能被利用实施对车联网关键设备、系统组件供应链的破坏，以发起高持续威胁等网络攻击相关的数据，可一定程度反映交通、运输等行业性关键信息基础设施网络安全保护情况，可被利用从而对车联网关键信息基础设施实施网络攻击的数据；涉及车联网信息服务的关键信息基础设施相关数据这类重要数据关注对汽车行业关键设备、供应链、以及关键信息基础设施的保护，其识别标准与GB/T 43697-2024《数据安全技术 数据分类分级规则》附录G“重要数据识别指南”列举的考虑因素基本一致。

（2）涉及个人信息出境的情形

针对自贸区内汽车行业的个人信息出境，《负面清单》规定的需通过安全评估、标准合同备案、个人信息保护认证的数量门槛均与《促进和规范数据跨境流动规定》一致，规定属于《促进和规范数据跨境流动规定》第三条、第四条、第五条第一款第一项至第三项、第六条规定的情形的，不计入累计数量。

在敏感个人信息认定方面，《负面清单》基本采纳了《汽车数据安全管理若干规定（试行）》对汽车行业敏感个人信息的定义，并补充了身份证号、行驶证号、驾驶证档案编号属于敏感个人信息。值得注意的是，《若干规定》规定“涉及个人信息主体超过10万人的个人信息”属于重要数据，但《负面清单》并未直接将这一类数据认定为重要数据。也就是说，如果拟出境个人信息不涉及关键车联网信息服务数据或其他类型的重要数据，汽车数据处理者不会仅因为拟出境个人信息数量超过10万人而需申报安全评估。

零售与现代服务业

（1）涉及重要数据出境

《负面清单》中未针对零售与现代服务业额外认定重要数据类别，因此目前该行业领域中的重要数据识别规则应适用通用规则（例如《数据分类分级参考规则》所明确的重要数据统一识别参考规则），并且当与其他行业存在交叉时需考虑其他行业的重要数据目录。

（2）涉及个人信息出境

1）不涉及敏感个人信息出境的情形。《负面清单》规定在会员管理场景下，若自当年1月1日起累计向境外提供500万人以上的个人消费者会员个人信息（不含敏感个人信息），则需要开展安全评估；若提供50万人以上且不满500万人

的个人消费者会员个人信息（不含敏感个人信息），则需要开展标准合同备案或个人信息保护认证。相比国家层面的数据跨境规定，《负面清单》将需要开展安全评估的门槛由100万提升至500万，并将需要开展标准合同备案或个人信息保护认证的门槛由10万提升至50万，放宽了会员场景下的个人信息出境限制。此外，并非会员场景下的所有个人信息出境均可以适用上述500万/50万的门槛。《负面清单》并未对会员场景下的个人信息进行穷尽列举，因此其列举之外的个人信息类型也可能落入《负面清单》的适用范畴，但对于部分《负面清单》中明确限缩适用个人信息范围的情形，例如“地址（含邮编，仅限消费者选择跨境物流或上门售后服务的情形）”、“会员爱好偏好（仅限产品类型、编号数字、偏好语言、积分兑换方式）”，若出境的个人信息在该等“仅限”范围之外（例如出境会员偏好的生日祝福形式），仍应当适用《数据出境新规》的100万/10万门槛。

2）涉及敏感个人信息出境的情形。《负面清单》规定在会员管理场景下，若自当年1月1日起累计向境外提供100万人以上的个人消费者会员敏感个人信息则需要开展安全评估，若提供10万人以上且不满100万人的个人消费者会员敏感个人信息，则需要开展标准合同备案或个人信息保护认证。根据此前的《数据出境新规》，为订立、履行个人消费者作为一方当事人的合同而提供商品或服务（如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等）而确需向境外提供个人信息的情形已豁免安全评估、标准合同备案和个人信息保护认证，但对于基于上述跨境交易和服务而衍生的会员服务而言，虽然其可以为消费者提供更多福利，其通常较难被上述豁免情形包含（例如会员等级、会员积分、会员偏好等服务均较难属于为提供商品或服务所必需），因此企业仍需就会员场景履行相关出境义务。在此背景下，《负面清单》为会员场景提供了更宽松的出境限制。受《负面清单》影响的企业主要是面向个人消费者建立会员制度并提供商品交易或服务的零售、住宿、餐饮、软件和信息技术服务、互联网信息服务等企业。对于其他企业或除会员外的其他场景，仍应按照此前《促进和规范数据跨境流动规定》等规定履行数据出境合规义务。

3、人工智能训练数据

（1）涉及重要数据出境的情形

根据《负面清单》，如人工智能模型训练、算法开发、产品测试等场景涉及的人工智能训练数据符合如下特征，将被认定为重要数据：

1）在研发设计过程中，收集和产生的与行业竞争力相关的高价值敏感数据。因此，如北京自贸试验区内数据处理者在AI产品出海等业务中，涉及向境外传输可能影响行业竞争力的人工智能算法源代码、关键组件数据、控制程序、基础模型数据、数据挖掘分析数据、测试数据等数据，则需要事先申报数据出境安全评估。

2）内容中涉及一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全的音频、图像及文本数据。因此，如北京自贸试验区内数据处理者拟向境外提供人工智能训练数据（包括音频、图像及文本），需要结合所涉领域、群体、区域、精度及规模等考虑因素，评估泄露或不当利用可能对国家安全、经济运行、社会稳定、公共健康和安全产生的危害后果。

3）纳入出口管制或技术出口管理事项的数据。根据国家出口管制清单以及《中国禁止出口限制出口技术目录》，可能涉及人工智能的物项包括但不限于具备特定性能（机器翻译系统得分>4.5分，满分为5分）的中译外翻译技术、专门用于汉语及少数民族语言的语音合成技术/人工智能交互界面技术/智能阅卷技术、水下自治或半自治机器人制造技术及控制技术、专门设计用于航空/航天/船舶/火车的有源噪声控制的系统设计技术和算法软件等。如人工智能训练数据落入前述事项范围，须根据有关规定进行数据出境安全评估以及履行出口许可申请义务。

（2）涉及个人信息出境的情形

在个人信息出境方面，《负面清单》针对拟出境训练数据模态、出境场景设置了差异化的数量门槛：对于在模型训练、算法开发、产品测试场景中的人工智能训练数据（仅限音频、图像、文本模态）出境，需通过安全评估、标准合同备案、个人信息保护认证的数量门槛相较于《促进和规范数据跨境流动规定》有所放松。其中，音频数据、图片数据、文本数据均包括相应模态的内容数据、标签数据等。

同时，除履行跨境合规机制外，大模型训练相关音频数据、图片数据、文本数据出境还需按照《生成式人工智能服务安全基本要求》中的有关要求进行处理，包括但不限于：1）确保语料来源可追溯，按要求保存不同类型语料的有关授权文件或记录；2）对于包含个人信息/敏感个人信息的语料，应依法取得个人同意/单独同意，或者符合法律、行政法规规定的其他情形（例如已经合法公开的个人信息）。对于其余出境场景或其他模态训练数据出境，需通过安全评估、标准合同备案、个人信息保护认证的数量门槛均与《促进和规范数据跨境流动规定》一致。

《负面清单》进一步明确了北京自贸试验区内人工智能领域“重要数据”的认定规则，同时适当放宽了模型训练、算法开发、产品测试三大场景中特定模态训练数据出境的个人信息跨境合规机制数量门槛。

整体而言，我们理解《负面清单》针对重要数据出境的规定较为严格，与我国对于重要数据一贯的审慎监管口径相一致，为数据有序自由流动守牢安全底线。同时，《负面清单》在北京自贸试验区内适当放宽了特定场景下的个人信息跨境合规机制数量门槛，减轻了试验区内数据处理者在相应场景下的数据跨境合规负担。值得注意的是，《负面清单》在特定行业的重要数据、敏感个人信息认定等方面有所创新，例如其中AI训练数据中重要数据识别的细化规定可能导致诸多AI出海企业需要履行数据出境安全评估义务。考虑到各行业、地区的重要数据目录制定工作仍在推进过程中，各自贸区的《负面清单》也可能作为重要参考。对此，建议试验区内外的企业持续关注有关规定的落实情况以及其他后续规定，及时调整数据处理和跨境传输策略，以确保有关数据跨境活动符合最新的法律合规要求。

负面清单落地举措

为做好负面清单组织实施，北京市自贸区实施四项“重点落地举措”，包括统筹布局北京数据跨境服务中心，在大兴机场临空区、商务中心区、北京经济技术开发区、中关村科学城前置设立并启动运行4个服务站，优化政务服务功能，拓展社会化服务领域，面向企业形成“一站式”服务能力。全面拓宽“绿色通道”服务范围，分行业、分领域拓展服务对象，畅通企业申报“直通车”。开发上线全市数据跨境便利化信息服务平台，形成全市统一的便利化服务能力。编发《北京市数据跨境流动便利化服务指南》，细化百余项具体服务，并分行业领域尽快组织开展政策宣讲和企业辅导，提高政策措施的覆盖面和到达率。

首先，严谨的准入机制保障数据出境的安全性。负面清单的使用需经过严格的准入程序，各自贸组团根据企业的申请材料进行审核。这种严谨的准入机制确保了只有符合条件的企业才能使用负面清单进行数据出境，极大地提高了数据出境的安全性和合规性。例如，在企业申请数据出境时，需提交详细的申请材料，包括数据出境的业务场景、出境数据目录、境外接收方等信息，通过严格的审核程序，确保每一次出境数据的合法性和安全性。

其次，规范的备案管理机制提升了数据管理的透明度。通过备案管理机制，各自贸组团能够动态掌握企业数据出境的实际情况。这种规范性的备案管理不仅有助于对数据出境活动进行有效的监督和管理，也能够为政策的进一步优化提供数据支持和决策依据。例如，企业在完成数据出境后，需及时向各自贸组团更新备案，确保数据出境活动的透明性和可追溯性。

再次，科学的风险评估机制确保数据出境的安全。北京自贸区在负面清单的使用过程中，通过科学的风险评估机制，及时识别和应对潜在的安全风险。这种科学性的风险评估机制不仅能够保障数据出境的安全性，也能够提高政策的应急响应能力。例如，通过对数据出境活动的风险监测和评估，能够及时发现和应对可能出现的安全隐患，确保数据出境的安全性和合规性。

此外，多层次的监管机制增强了政策的执行力。北京自贸区通过建立多层次的监管机制，确保负面清单的使用和管理的有效性。这种多层次的监管机制包括自贸区管理机构、市级管理部门以及各自贸组团的联动合作，确保政策的执行力和效果。例如，各自贸组团在数据出境活动中，需与市级管理部门进行密切合作，共同开展监督和核验工作，确保负面清单有效使用。

最后，完善的反馈机制提升了政策的优化能力。在负面清单的实施过程中，北京自贸区通过完善的反馈机制，积极收集企业和社会的意见和建议。这种反馈机制不仅能够帮助政策制定者及时了解政策实施的效果和问题，也能够为政策的进一步优化和调整提供参考和依据。例如，通过定期的政策评估和反馈收集，能够不断优化和改进负面清单的管理措施，提高政策的执行效果和企业的满意度。

综上所述，北京自由贸易试验区在负面清单的使用与管理中，通过严谨的准入机制、规范的备案管理、科学的风险评估、多层次的监管以及完善的反馈机制，提升了数据出境的安全性和管理的有效性。这些创新措施不仅保障了数据出境的便利度、合规性和安全性，也为自贸区的国际化发展提供了坚实的政策支持，为其他地区的数据管理提供了重要的参考和借鉴。这些创新措施在促进产业发展的同时，也为自贸区的国际化和现代化进程注入了新的活力。

上海自贸区数据跨境实践

数据分类分级制度

2024年2月8日，中国（上海）自由贸易试验区临港新片区（下称“临港新片区”）管理委员会正式发布了《临港新片区数据跨境流动分类分级管理办法（试行）》（下称“《管理办法》”）。临港新片区作为我国体制机制创新的“试验田”，在数据跨境方面加快更大力度先行先试、更高水平对外开放，在我国数据跨境较强监管的背景下，对于数据跨境流动、跨境离岸金融等领域率先开展更大程度的压力测试。

《管理办法》采用行业+场景的形式，结合上海“五个中心”建设，即国际经济中心、金融中心、贸易中心、航运中心、科技创新中心，围绕汽车、金融、航运、生物医药等重点领域以及临港新片区相关行业的发展要求，以跨境需求最迫切的典型场景为切入口，对跨境数据进行分类管理。

五大分类：重点领域场景

临港新片区围绕智能网联汽车、金融理财、高端航运、国际贸易、生物医药、文化出海等重点领域的具体场景，组织行业龙头企业和专家组成工作组，陆续发布一批一般数据清单和重要数据目录。

在智能网联汽车领域，特斯拉（上海）有限公司、上海汽车集团股份有限公司、保时捷（中国）汽车销售有限公司等14家汽车行业代表企业已成立工作组，共同推进清单和目录的编制工作。

新片区将充分依托前期开展数据跨境流动试点积累的经验，遵循“从企业到行业，从案例到清单，从正面到负面”的原则，以行业为维度，以企业数据跨境需求场景为切入口，有序推进一般数据清单和重要数据目录的编制工作。

三大分级：数据分级管理

跨境数据分级从高到低依次分为核心数据、重要数据、一般数据3个级别，核心数据禁止跨境；重要数据形成重要数据目录，安全评估后出境；一般数据形成一般数据清单，备案后出境。

数据分类	出境规定	出境流程
核心数据	禁止跨境	/
重要数据	安全评估后出境	通过临港新片区数据跨境服务中心申报数据出境安全评估
一般数据	备案后出境	向临港新片区管委会申请登记备案，并在满足相关管理要求下自由流动

表4-1 跨境数据分类及对应出境要求

（1）核心数据

核心数据是对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。核心数据禁止跨境。

（2）重要数据

重要数据是特定领域、特定群体、特定区域或达到一定精度和规模的数据，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全。仅影响组织自身或公民个体的数据，一般不作为重要数据。

重要数据的目录由临港新片区管委会负责制定、进行更新，并报相关部门备案。同时按照要求制定纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单，报经市委网络安全和信息化委员会批准后，报相关部门备案。

数据处理者对重要数据目录内的数据，可通过临港新片区数据跨境服务中心申报数据出境安全评估。

（3）一般数据

一般数据是核心数据、重要数据外的其他数据。一般数据清单由临港新片区管委会负责制定、进行更新。若相关领域出台场景化重要数据目录，则该领域的一般数据清单自动失效。

数据处理者对在一般数据清单内的数据，可向临港新片区管委会申请登记备案，并在满足相关管理要求下自由流动。

数据跨境服务中心

2024年4月7日，临港新片区数据跨境服务中心启用，致力于为数据处理者提供全方位、全流程数据跨境服务，包括材料受理、业务咨询等环节，在自贸区一线打造数据跨境流动的“绿色通道”。

服务中心主要承担上海市委网信办与临港新片区管委会赋予的统筹发展与安全，保障国家数据安全，保护个人合法权益，进一步促进和规范新片区数据依法有序自由流动；为新片区企业提供就近服务，为全市企业提供便利服务。推动新片区开展数据分类分级工作，探索制定“负面清单”；推动新片区高标准对接国际数据规则，助力数据数字经济领域高水平开放。

服务中心的主要职能包括：保障国家数据安全和个人权益，规范数据流动；为新片区及全市企业提供数据服务；推动新片区开展数据分类分级工作；推动新片区探索对接国际数据规则，助力数字经济领域高水平开放。服务内容包括：个人信息出境标准合同备案、重要数据安全评估受理、数据跨境试点场景评估受理、一般数据清单内的数据跨境备案。促进国际数据业务合作。探索对接CPTPP、DEPA等国际高标准经贸规则，支撑临港新片区与新加坡、新西兰、智利、一带一路、金砖国家等国家和地区开展跨境数据流动、电子票据、数字身份互认、区块链对接等合作，研究对接跨境数据流动认证机制。

数据跨境一般清单

2024年5月17日，在前期出台《中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行）》的基础上，进一步发布了《数据跨境场景化一般数据清单》（以下简称“一般数据清单”）及清单配套操作指南。首批一般数据清单包含智能网联汽车、公募基金、生物医药3个领域，涉及智能网联汽车跨国生产制造、医药临床试验和研发、基金市场研究信息共享等11个场景，划分成64个数据类别600余个字段。三大领域“一般数据清单”的发布，意味着一种有别于“负面清单”的数据跨境传输机制正在从理论走向实践。

“一般数据清单”有助于降低企业合规成本。“一般数据清单”直接且明确地列出了可以自由出境的数据字段，这些字段直接贴合了组织内部的业务人员、法务人员的认知体系和话语体系，减少在企业内部不同部门之间沟通并达成共识的合规成本。具体而言，临港新片区的“一般数据清单”通过“三要素”结合作为清单的基本框架——即传输目的、传输字段（配合描述）、传输后的要求。其中，传输目的限定了数据在境外的处理目的，也就同时建立了评价数据出境后是否合法处理的基线；传输字段实际上确立了某项传输目的之下，为完成特定业务而确需出境的数据字段，也就完成了数据出境安全管理中的必要性判断；传输后的要求，针对的是境外数据接收方的数据安全管理和技术措施，也就是对应的数据出境安全管理中对数据传输和使用的完整性、保密性、可用性的要求。

综上，“一般数据清单”是在“传输目的、传输字段（配合描述）、传输后的要求”框架下的数据清单，将在实践中已经被主管部门批准或已经被证明出境安全风险确实较低的场景或业务，形式固定下来和对外展示出来，对其他具有类似需求的企业给于明确的信号和指引。临港新片区关于“一般数据清单”的尝试，在国家“自上而下”编制重要数据目录的前提下，更好发挥自贸区“自下而上”先行先试作用，通过收集梳理目前企业对数据跨境的实际需求，根据场景来编制一般数据清单且可操作可落地的做法，为编制数据跨境的负面清单和重要数据目录提供新的实践样本。

国际数据经济产业园

临港新片区依托“五自由一便利”（投资自由、贸易自由、资金自由、运输自由、人员从业自由、信息快捷联通）的制度优势，以国际数据经济产业园为核心载体，致力于建设高水平国际数据合作桥头堡、高标准数据跨境制度创新先行区、高质量国际数据产业集聚地和高能级数据流通基础设施新枢纽。据报道，国际数据经济产业园聚焦“实施国际互联网数据跨境安全有序流动”的核心功能，面向数据服务、国际金融、跨境电商、国际航运、跨境供应链、人工智能等核心产业领域，力争打造高水平国际数据合作桥头堡，高标准数据跨境制度先行区，高质量国际数据产业集聚地，高能级数据流通基础设施新枢纽。

2023年10月27日，国际数据经济产业合作大会上正式揭牌后，已推动数据跨境服务中心、国际数据港研究院、国际合作交流工作站等一批服务机构挂牌入驻，签约中法合作数字IP产业园、中汽研等一批重点项目，引进普联斯通、光环云等一批国际龙头企业入驻。

国际数据经济产业园实施五大“特殊功能”，包括：

（1）国际规则压力测试与国际合作：为中国加入《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）等高水平国际贸易规则进行先行试点和压力测试，并积极建设国际数据经济合作平台。

（2）数据跨境流动：建立数据安全、有序、快捷的跨境流动新模式；

（3）国际数据合作：建设国际功能性数据中心，发展两头在外的数据服务；

（4）电信市场开放：推动外商投资国内电信业务，试点增值电信业务股权比例限制开放；

（5）国际数据交易：开展国际数据交易探索。

为加快打造实现上述“特殊功能”，园区在支撑数据跨境的基础设施、功能平台、创新制度、载体配套等方面进行了系统规划并积极推动相关项目落地，以数字基础设施方面为例，重点推动海光缆登陆站、国际光缆、数据中心、国际互联网专用通道等基础设施建设，建设完备的通信基础设施体系，进一步为国际数据服务赋能。

天津自贸区数据跨境实践

中国（天津）自由贸易试验区2014年12月由国务院批准设立。2018年5月4日，国务院印发《进一步深化中国（天津）自由贸易试验区改革开放方案》，再次为天津自贸试验区建设发展赋能。天津自贸区内的三大区域各有其产业发展基本定位与功能：东疆保税港区主要着眼于航运、物流、仓储等功能；空港保税区则是先进制造业的集聚区；滨海新区中心商务区则侧重金融、贸易与商务服务业的发展。

作为天津市营商环境质量提升行动方案的重点举措，天津自贸试验区于2024年2月发布数据分类分级标准规范、2024年5月发布《中国(天津)自由贸易试验区数据出境管理清单(负面清单)(2024年版)》，以规范和促进数据有序跨境流动，为企业数据出境提供精准指导。负面清单既是对接DEPA、CPTPP等国际高标准规则，践行“为国家试制度”的积极探索，也是积极回应企业诉求，为“地方谋发展”的实际行动。

数据跨境流动挑战

以自贸区工业场景为例，数据跨境流通面临数据权属难理清、流通技术不成熟、流通标准不统一等问题，显著降低了数据的流通效率与应用效果。

1、工业数据要素流通归属权复杂。工业数据涉及主体众多，如工业应用运行过程中产生诸如运行、分析、预测等数据，不同类型的数据价值评估、定价及利益分配均无清晰的数据流通权属规则。许多工业数据是由多个企业或组织共同产生的，数据归属权难以确定。一些数据通过合作或共享生成，数据所有者不明确。

2、工业数据分类分级标准实操性不强。参考工信部《工业数据分类分级指南（试行）》，分类维度包括但不限于研发数据域（研发设计数据、开发测试数据等）、生产数据域（控制信息、工艺参数、系统日志等）、运维数据域（物流数据、产品售后服务数据等）、管理数据域（系统设备资产信息、产品供应链数据等）、外部数据域（与其他主体共享的数据等）5大类，仅按照平台运营、企业管理两个大类对平台企业数据进行了分类，更多场景和行业数据的具体分类分级规则尚不具备可落地性。

3、数据流通技术应用不成熟。工业数据要素流通技术应用不成熟是“有数流不动”的根源所在，在工业数据要素应用保障、技术路线、系统工具等方面仍有很多不足。

数据跨境负面清单

《中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024年版）》是国家互联网信息办公室《促进和规

范数据跨境流动规定》实施以来，首个经省级网络安全和信息化委员会批准并报国家网信部门、国家数据管理部门备案的自贸试验区数据出境管理负面清单。

此次发布的《负面清单》列明了天津自贸试验区企业向境外提供数据需要申报的数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形。围绕生物医药、服务外包、金融、互联网平台、汽车、集成电路、气象、国际贸易等自贸试验区8大重点领域产业发展和监管需要，将企业出境数据分为战略物资和大宗商品类、自然资源和环境类、工业类、金融类等13个大类46个子类，并对每一类数据基本特征作出详细描述，使企业易于理解、便于操作。《负面清单》列明之外的数据可以自由跨境流动。此前，国家网信办公布《促进和规范数据跨境流动规定》，提出自贸试验区在国家数据分类分级保护制度框架下，可以自行制定区内需要纳入数据出境安全评估、个人信息出境标准合同、个人信息保护认证管理范围的数据清单。

数据跨境安全管理

天津自贸区企业向境外提供《负面清单》外的数据免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。《负面清单》主要考虑落实数据分类分级管理要求、加强个人信息保护、服务企业高质量发展、规范数据出境行为。涉及国家秘密的数据、核心数据、政务数据不纳入《负面清单》管理，相关数据出境按照有关法律、法规和规定执行。

根据《负面清单》的适用范围，天津自贸试验区内有数据出境需求的企业，应当对照《负面清单》识别其拟出境数据是否在清单范围内，在清单范围内的数据按照国家规定、根据实际情况申报数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证，清单外数据可以自由跨境流动。比如，化学工业领域某企业计划向境外某公司传输某危化品的运输路线规划信息，根据《负面清单》中工业类的化学工业子类数据基本特征与描述，该信息应当纳入需要申报数据出境安全评估的数据清单管理，该信息出境应当申报数据出境安全评估。根据国家网信办发布的《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》，数据出境行为包括：一是数据处理者将在境内运营中收集和产生的数据传输至境外。二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以查询、调取、下载、导出。三是符合《个人信息保护法》第三条第二款情形，在境外处理境内自然人个人信息等其他数据处理活动。

对天津自贸试验区的企业来说，以下七种数据出境活动免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：一是国际贸易、跨境运输、学术合作、跨国生产制造和市场营销等活动中收集和产生的数据向境外提供，不包含个人信息或者重要数据的。二是在境外收集和产生的个人信息传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的。三是为订立、履行个人作为一方当事人的合同，如跨境购物、跨境寄递、跨境汇款、跨境支付、跨境开户、机票酒店预订、签证办理、考试服务等，确需向境外提供个人信息的。四是按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的。五是紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的。六是关键信息基础设施运营者以外的数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的。七是向境外提供《负面清单》外的数据。其中，第三种至第七种条件所称向境外提供的个人信息，不包括被相关部门、地区告知或者公开发布为重要数据的个人信息。

天津自贸试验区的企业，与天津行政区域内其他数据处理者一样，申报数据出境安全评估、备案个人信息出境标准合同可以登录数据出境申报系统。具体方式可以查看国家网信办公布的《数据出境安全评估申报指南（第二版）》和《个人信息出境标准合同备案指南（第二版）》。已经通过线下方式提交安全评估申报、标准合同备案材料的，不需要通过数据出境申报系统进行重新提交。申请个人信息保护认证可以登录个人信息保护认证管理系统。关键信息基础设施运营者或者其他不适合通过数据出境申报系统申报数据出境安全评估的，采用线下方式申报数据出境安全评估。

粤港澳大湾区数据跨境实践

区域经济特征与数据跨境需求

1、大湾区数据跨境试点优势

“一国两制三法域”制度结构为大湾区探索数据跨境流动创新提供了多元化的法律环境和政策实践空间。渐进式改革路径下，粤港澳独立的法律体系构筑了大湾区改革创新的防火墙基础，不仅为探索数据跨境流动改革提供了一个低成本试错环境，也易于所形成的有效数据跨境流动方案对全国层面形成示范效应。

一是大湾区提供了国际接轨优势与多样化的实验空间。大湾区融合了内地法律体系的稳定性与香港、澳门作为特别行政区保持的独立司法体系和国际接轨的法律规则，法律多样性为数据跨境流动提供了不同的法律环境和治理模式，能够探索和融合不同法律体系下的数据治理平衡点，形成适应性强、普适性广的数据跨境流动规则和机制，为我国数据跨境流动规则的制定提供宝贵经验。

二是大湾区具备丰富应用场景与市场需求奠定了数据跨境流动产业基础。大湾区经济总量庞大，拥有多元化的产业结构和高度国际化的市场环境，为数据跨境流动提供了丰富应用场景和厚实市场需求。大湾区在金融、医疗、教育、物流等多个领域都有大量的数据跨境流动需求，多元化的需求有利于推动数据跨境流动规则的创新和完善。近年来大湾区在粤澳健康码跨境互认、电子病历跨境互通等数据跨境流动方面进行了有益尝试，不仅提高了公共服务效率，也为数据跨境流动的规则制定提供了实践基础。

三是先进的基础设施与技术为大湾区数据跨境流动提供了坚实的技术支撑。一是大湾区在5G、人工智能、云计算等新一代信息技术领域具有领先优势，为数据跨境流动提供了坚实的技术支撑。二是基础设施建设如国际互联网数据专用通道、数据中心等，为数据的高效传输和安全存储提供了硬件保障。三是在隐私计算、区块链等数据安全技术研发和应用方面走在前列，为数据跨境流动的安全性和可信度提供了技术安全保障。

2、大湾区数据跨境流动需求难点

一是协调难度大，法律不确定性风险高。当前大湾区内地9市与香港、澳门在法律体系、数据保护法规、隐私政策等方面存在显著差异，香港遵循英美法系，而内地为大陆法系，导致大湾区在数据跨境流动的法律适用、个人信息保护标准、数据安全要求等方面的不一致。此外，三地在数据出境安全评估、数据分类分级管理等方面也缺乏统一的标准和流程，不仅增加了企业合规成本，也限制了数据流动的效率。

二是规则标准不统一、平台建设滞后，数据交易成本高。尽管大湾区在数字基础设施建设方面取得了显著进展，但在数据跨境技术标准统一、数据跨境交易平台建设等方面仍面临挑战，不同地区在数据格式、接口协议、加密技术等方面的标准不统一，使得数据在跨境传输过程中难以实现无缝对接。此外，缺乏统一的数据跨境交易平台，导致数据跨境交易、流通和监管成本过高。

三是数据安全与隐私保护问题仍然是数据跨境流动最大障碍。在数字跨境流动的过程中，数据安全和隐私保护是关键的考量因素。大湾区在数据安全法律体系、监管能力、技术防护措施等方面存在不足，尤其是在面对跨境数据流动可能带来的安全风险时，如何确保数据不被非法访问、泄露或滥用，是一个亟待解决的问题。此外，随着国际社会对数据保护意识的增强，如何在保障个人隐私权益的同时，促进数据的合理利用和流动，也是大湾区需要面对的挑战。

数据跨境标准合同实施指引

2023年12月10日，国家互联网信息办公室与香港特区政府创新科技及工业局发布了《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同实施指引》（以下简称“《粤港澳指引》”）以及相应的个人信息出境标准合同文本《粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》（以下简称“《粤港澳标准合同》”），并于发布当日起实施。相比起2023年6月正式实施的《个人信息出境标准合同办法》以及相应的个人信息出境标准合同文本，两者总体框架相似，但在文件目的、适用范围、备案流程，以及各自标准文本的条款设置方面有所不同。

《粤港澳指引》的出台主要旨在为粤港澳大湾区间企业的个人信息跨境流动“减负”，促进粤港澳大湾区个人信息安全有序流动，协同联动打造“粤港澳大湾区数据特区”。大湾区内的企业则能够依照更为精简、便捷的《粤港澳指引》及《粤港澳标准合同》进行相关备案手续，优化了数据流通机制。

从适用范围上看，根据《粤港澳指引》第二条规定，该文件的适用范围为注册（适用于组织）或位于（适用于个人）“广东省广州市、深圳市、珠海市、佛山市、惠州市、东莞市、中山市、江门市、肇庆市，或者香港特别行政区”的个人信息处理者及接收方，也即本次主要为粤港间的数据流通创设了便利条件。但是，需要格外注意的是《粤港澳指引》要求个人信息处理者及接收方双方需同时满足注册或位于粤港澳大湾区的条件，即一方不在粤港澳大湾区即不在本指引适用范围之内。另一方面，《粤港澳指引》对于适用的个人信息处理者的范围相较《办法》更为宽松。《办法》参照了《数据出境安全评估办法》第四条规定，在下列四种情形下需要进行数据出境安全评估，而不能适用内地《标准合同》：一是非关键信息基础设施运营者；二是处理个人信息不满100万人的；三是自上年1月1日起累计向境外提供个人信息不满10万人的；四是自上年1月1日起累计向境外提供敏感个人信息不满1万人的。相较之下，《粤港澳指引》第二条明确规定，被相关部门、地区告知或者公开发布为重要数据的个人信息不适用《粤港澳标准合同》。对比而言，《粤港澳指引》并未提及个人信息的数量、时间的要求，这意味着拥有大体量数据的个人信息处理者也能够依据《粤港澳指引》，无需申报数据出境安全评估。

相较于《个人信息出境标准合同办法》，《粤港澳标准合同》在总体框架上除了将“境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响”整条删除之外，并无太大的变动。以下对有较大变化部分进行解读。

首先，《粤港澳标准合同》从术语定义、合同义务履行方面尊重属地法、基于境外接收方更大合同适用与解释空间。在术语定义方面，《粤港澳标准合同》在内地《标准合同》的基础上考虑了香港当地的定义，例如第一条中对于“个人信息处理者”与“个人信息主体”的定义中额外考虑了香港对于“资料使用者”与“资料当事人”的说法；将监管机构、相关法律法规的定义相应扩大，同香港当地监管部门与相应规定同步，这将极大便利粤港间对《粤港澳标准合同》的适用与数据的流通。此外，在合同义务履行方面，《粤港澳标准合同》明确关于个人信息处理者与接收方的义务和责任符合属地相关法律规定即可。例如，在第三条第一项中“个人信息处理者属地相关法律法规要求不需要告知的，从其规定”，简化内地《标准合同》中的内容，给予了香港属地《个人资料（私隐）条例》适用的空间。

其次，《粤港澳标准合同》简化了个人信息保护安全评估的内容，有效减轻了备案负担。《粤港澳标准合同》相较于内地《标准合同》，最显著的变化是将“境外接收方所在国家或者地区个人信息保护政策和法规对合同履行的影响”内容整条删除，无需再对香港的个人信息保护水平进行评估，此举从侧面体现了内地对香港作为境外接收方，适用《个人资料（私隐）条例》等相关法律具有 “适当保护水平”之肯定。此外，在个人信息保护影响评估时的内容也如上文“三、重点比较”中所述有所简化。

最后，《粤港澳标准合同》对接收方向第三方提供个人信息的限制更宽松，便利了粤港澳大湾区辖区内数据的再流转。内地的《标准合同》中对境外接收方向中国境外第三方提供个人信息提出了高标准，需要满足“业务需要+告知+依照法律法规要求取得同意+第三方保证+书面协议副本”，此外合同中对于敏感个人信息、儿童个人信息等有更严格的要求。然而，《粤港澳标准合同》第三条第八项中，接收方满足“业务需要+告知+依照法律法规要求取得同意”即可向粤港澳大湾区辖区内第三方再流转数据，有助于促进辖区内的数据流通。

数字基建与数据跨境基础设施

当前，粤港澳大湾区建设已进入数据要素市场化配置综合改革全面深化期，应多措并举加快探索数据跨境有序便利流通，深入推进粤港澳大湾区建设，打造新发展格局战略支点。

超前规划三大数据枢纽节点，系统推进四大合作平台建设

借鉴粤港澳大湾区经济圈和都市圈的发展思路，以建设粤港澳大湾区数据枢纽为核心，规划建设广佛、深港、珠澳三大数据枢纽节点，构建多源汇聚、安全有序、高效流通的粤港澳大湾区数据资源体系。深化粤港澳合作，充分发挥深圳前海、广州南沙、珠海横琴、河套深港四大合作平台新型空间载体功能和示范引领作用，探索数据跨境有序便利流通新机制、新模式。

加快推进粤港澳大湾区规则衔接、机制对接，促进数据跨境流动创新监管和协同治理

推动粤港澳数据跨境立法和政策协同，在安全可信、风险可控前提下探索支持粤港澳数据要素高效流通的便捷安排。完善数据跨境制度规则体系，建立数据安全保护能力评估认证、数据流通备份审查、跨境数据流通和交易风险评估等数据安全管理机制。构建跨境数据分级分类管理制度，建立白名单和负面清单机制，探索建立行业性低风险跨境流动数据目录。建立粤港澳数据跨境联合监管机构，创新监管沙盒等数据跨境监管互信机制。

加快数据跨境基础设施建设，推动数据跨境流动技术应用创新

整合粤港澳大湾区大数据中心、鹏城“云脑”、横琴先进智能计算中心等算力资源，强化数据跨境基础设施优势。推进新型互联网交换中心、国际互联网数据专用通道等数字基础设施建设。建设数据跨境流动安全威胁感知和监测预警基础设施，统筹数据安全威胁信息的获取、分析、研判和预警工作。围绕金融、交通、医疗、物流、科研、跨境电商等行业，探索数据跨境流通技术行业性解决方案，合理利用隐私计算、区块链存证、数据空间等新型数字技术，为跨境数据全流程防篡改、可追溯、可信任提供关键技术支撑。

构建数据跨境可信流通体系，培育跨境数据产业生态

建立跨境数据交易负面清单制度，明确不能交易或严格限制交易的数据产品，推动形成合规有序、安全可控的跨境数据交易流通机制。探索建立跨境数据保荐人，跨境数据经纪人、跨境数据托管人等创新制度，开展合规保荐、数据经纪、受托行权等多样化服务。鼓励大湾区金融机构开展跨境数据资产质押、跨境数据知识产权证券化等创新服务。参考“一线放开、二线管住”的管理模式，以离岸数据交易平台为核心，探索建设涵盖基础设施支撑、专业服务提供、数据产业发展、应用场景丰富的离岸数据产业生态试验区。

海南自贸港数据跨境实践

推动数据安全有序流动

根据《海南自由贸易港建设总体方案》，海南自贸港是中央授权最早探索“在确保数据流动安全可控的前提下，扩大数据领域开放”的地区。海南自贸港同时作为海南自贸试验区，享有自行制定负面清单的权力。海南自由贸易港提出“6+1+4”的制度设计，推动五个自由便利与一个安全有序流动，即贸易自由便利、投资自由便利、跨境资金流动自由便利、人员进出自由便利、运输来往自由便利和数据安全有序流动，构建一大现代产业体系，加强税收、社会治理、法治、风险防控等四方面制度建设。

《海南自由贸易港建设总体方案》围绕数据安全有序流动明确专项制度安排，聚焦电信业务对外开放，将为海南自由贸易港构建现代产业体系、抢抓全球新一轮科技革命和产业变革提供重要支撑。开放增值电信业务，逐步取消外资股比等限制。根据《海南自由贸易港外商投资准入特别管理措施(负面清单)(2020年版)》，海南自贸港允许实体注册、服务设施在海南自由贸易港内的企业，面向自由贸易港全域及国际开展在线数据处理与交易处理等业务，并在安全可控的前提

下逐步面向全国开展业务。安全有序开放基础电信业务。开展国际互联网数据交互试点，建设国际海底光缆及登陆点，设立国际通信出入口局。

由此看出，海南自由贸易港数据安全有序流动将主要通过开放电信业务实现，三大具体举措包括：开放基础电信业务、开放增值电信业务、开展国际互联网数据交互试点。根据《海南自由贸易港建设总体方案》，为保障顺畅的跨境互联网数据互通，海南自由贸易港将建立国际互联网数据专用通道，覆盖洋浦经济开发区、海口国家高新技术产业开发区、博鳌乐城国际医疗旅游先行区、三亚崖州湾科技城、海南生态软件园、海口复兴城互联网信息产业园、海口江东新区、海口综合保税区等9个园区。通道建成后，将明显提升覆盖园区企业的国际互联网访问质量，改善国际网站访问、跨国视频会议、大文件传输等应用场景下的用户体验，为园区营造优质的国际通信营商环境。

推动国际数据中心业务

为促进海南自由贸易港国际数字产业发展和数据跨境安全有序流动，推进高水平对外开放合作，支持数字经济高质量发展，海南省网信办起草了《海南自由贸易港国际数据中心发展条例（公开征求意见稿）》并于2024年6月26日至7月25日公开征求意见。该促进条例如果生效，将是我国首个专门针对国际（离岸）数据中心的地方性法规文件。随着增值电信业务的扩大开放和数据跨境规则的进一步完善，离岸数据中心将迎来发展新机遇。

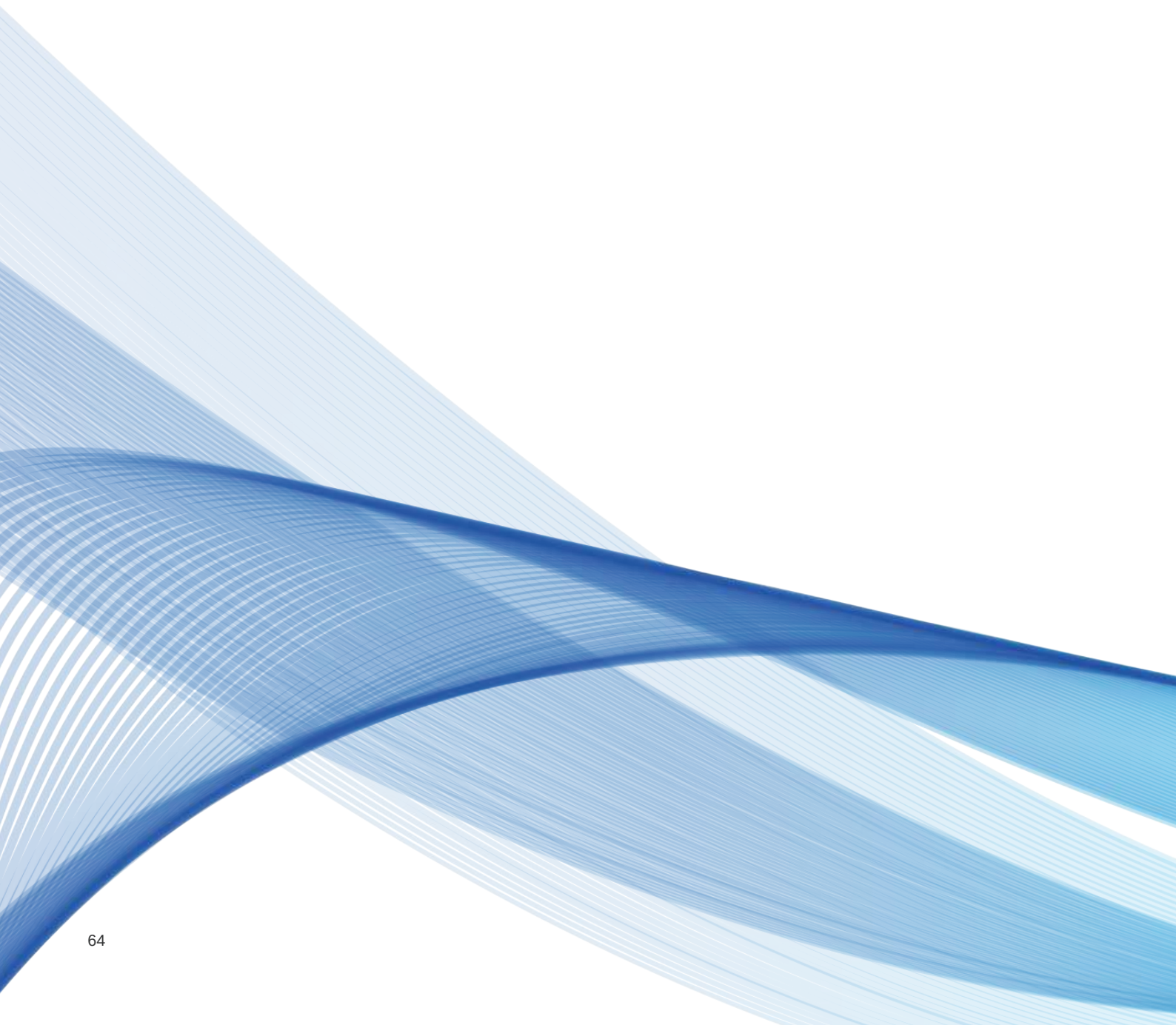
国际数据中心业务，是指企业在海南自由贸易港内利用高速便捷的跨境数据专用通道，仅面向境外提供数据存储、加工、交易等国际数据服务业务。国际数据中心业务运营者可以面向境外提供游戏服务、影视加工、商业航天、北斗应用、跨境电商、跨境直播、跨境旅游、远程医疗、远程教育、国际学术交流合作和跨国生产制造等国际数据服务。

在出境豁免方面，海南自由贸易港开展国际数据中心业务，符合下列条件之一的，免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证：一是仅对在境外收集和产生的数据进行存储、加工、交易等数据服务，服务过程中没有引入境内个人信息或者重要数据；二是向境外提供海南自由贸易港数据出境负面清单以外的数据。尽管尚未发布数据出境负面清单，该条例第八条指出，在国家数据分类分级保护制度框架下，海南自由贸易港按照《促进和规范数据跨境流动规定》制定海南自由贸易港数据出境负面清单，建立健全负面清单管理制度。

在推动对外合作方面，海南自由贸易港加强与“一带一路”沿线国家和地区及其他国际平台的交流合作，构建与《数字经济伙伴关系协定》（DEPA）相衔接的制度体系，支持国际数据中心业务运营者在数字身份、电子支付、数据跨境流动等领域开展国际互认互信。国际数据中心业务运营者可以自主选择使用可信、安全的国内外云服务、AI算力芯片、AI大模型等开展国际数据中心业务。

在安全保障方面，省网信部门负责统筹协调国际数据中心网络安全和数据安全相关监管工作，指导有关部门和企业建设国际数据中心数据安全保障体系和监管体系，建立健全数据安全风险评估、信息共享、监测预警、应急处置等机制，保障国际数据中心网络安全和数据安全。国际数据中心业务运营者应当依照法律、法规的规定，落实安全管理制度和技术措施，建立健全全流程网络安全和数据安全管理制度及应急处置预案，保障网络安全和数据安全。省级基础电信运营商应当依照法律、法规的规定，制定安全管理制度，履行网络安全和数据安全保护义务。有关部门在履行监管职责中，发现数据出境活动存在较大风险或者发生数据安全事件的，可以要求国际数据中心业务运营者进行整改。

企业数据跨境安全合规指引 2024



第五章
数据跨境安全典型场景

数据出境合规场景

企业在出海过程中面临的数据跨境传输需遵守严格的国际和目标国家的数据保护法规，这一过程中的合规性、安全风险及解决方案构成了企业国际化战略中的重要组成部分。

场景与风险分析

合规风险是企业出海过程中不可忽视的问题。不同国家和地区有着不同的数据保护法规，这些法规在数据收集、存储、处理和使用等方面都有着严格的规定。企业在出海过程中，必须深入研究并遵守这些不同国家的法律要求，如果未能全面遵守这些法规，就可能面临法律处罚、业务受限等风险。此外，合规风险还可能影响企业的合作伙伴关系和市场准入，对企业的国际业务运营造成障碍。

不同国家之间的法律差异也可能导致企业在数据跨境传输中面临不确定性。因此，企业在出海过程中，应密切关注国际政治和法律环境的变化，及时调整数据处理策略，确保企业的运营符合相关法规和政策要求。同时，企业还应加强内部员工培训，提高员工对数据保护法规的认识和遵守意识。

合规风险主要关注以下方面：一是数据本地化要求。有些国家要求金融数据、医疗数据或政府数据等敏感信息必须在本国境内存储和处理。企业出海过程中必须了解并遵守这些国家的数据本地化要求，以免因违规而面临法律制裁或业务中断的风险。二是数据审计和合规报告要求。为了确保企业在数据处理活动中持续遵守相关法律法规，一些国家要求企业定期进行数据保护合规性审计，并向相关监管机构提交报告。这些审计和报告可以帮助企业发现潜在的安全风险和合规问题，并及时进行改进。同时，这也是企业向监管机构展示其合规诚意和实际行动的重要途径。因此，电子商务企业在出海过程中，应建立完善的审计和报告机制，确保数据处理活动的合规性。三是出口管制要求。国际政治形势的变化可能对数据跨境传输政策产生重大影响。例如，某些国家可能因国家安全考虑而限制或禁止特定类型的数据跨境传输。

解决方案

1、深入了解和遵守法规。满足合规要求是企业出海数据安全的基石，企业需要详细了解目标市场的数据保护法规。通过深入研究这些法规，企业可以确保自己的业务操作符合当地法律要求，避免因违规而面临法律风险和罚款。同时，企业还应及时关注出海所在国家法规的更新和变化，及时调整自身的数据处理策略，确保始终保持在合规的轨道上。

2、建立跨国数据保护框架。随着企业全球化步伐的加快，企业需要制定制定跨境数据保护政策时，参考欧盟GDPR等较为严格的数据保护法规，从而可以确保企业在处理跨国数据时，能够达到最高的合规要求。

3、数据加密与数据保护。加密和数据保护技术是保障数据安全的重要手段。在数据传输过程中，企业应采用强加密技术，确保数据在传输过程中不被窃取或篡改。同时，企业还应采取适当的数据保护措施，如使用VPN、TLS等安全协议进行数据传输，确保数据的完整性和保密性。此外，企业还可以考虑使用数据脱敏技术，对敏感数据进行脱敏处理，降低数据泄露的风险。

4、数据本地化策略。根据目标市场的法规要求，企业可能需要在当地建立或租用数据中心来存储和处理数据。通过实施数据本地化策略，企业可以确保数据在目标市场内得到安全存储和处理，避免跨境数据传输带来的风险。同时，企业还应与当地的数据中心运营商建立良好的合作关系，确保数据中心的安全性和稳定性。

5、数据安全合规审计。企业定期对数据保护措施和合规性进行审计和评估，确保数据安全措施的有效性。同时，企业还应关注新技术和新法规的发展，及时调整自身的数据安全策略和技术手段，确保随着法规和技术的变化持续保持合规。

敏感数据流通场景

在企业出海的过程中，不仅要在不同国家和地区之间高效、稳定地传输数据以支持其国际业务运营，同时还必须确保这些数据的安全性，严格遵守当地的数据保护法规，以避免可能的法律风险和经济损失。这种场景下具体的情境多样且复杂，可能包括跨境数据传输、跨地区的云服务存储、国际间的数据共享和处理等。

场景与风险分析

1、敏感数据泄露风险。在跨境数据传输过程中，企业可能面临数据泄露的风险。由于网络环境的复杂性和不确定性，数据在传输过程中可能会被截取、窃取或滥用。这种泄露不仅可能导致企业核心信息的泄露，还可能损害客户的隐私权益，对企业的声誉和业务造成严重影响。

2、敏感数据丢失风险。除了数据泄露和合规风险外，企业还可能面临数据丢失和访问控制风险。由于技术故障、人为错误或恶意攻击等原因，数据在传输或存储过程中可能会丢失，导致业务中断或数据无法恢复。

3、数据访问控制风险。未经授权的访问也可能导致数据被非法访问或修改，进而引发一系列安全问题。

解决方案

1、跨境数据加密传输。为了确保敏感数据在跨境传输过程中的安全，对于跨境传输的敏感数据，采用强加密标准，如AES（高级加密标准）或RSA（非对称加密算法）等。这些加密标准能够有效地保护数据在传输过程中的机密性和完整性，防止数据被未经授权的第三方窃取或篡改。通过加密处理，即使数据在传输过程中被截获，攻击者也无法轻易解密和获取其中的敏感信息。同时企业需要采用专业的密钥管理服务来确保加密密钥的安全。

2、跨境数据实时监测与响应。通过专业的数据安全风险工具实时监测数据传输过程中的各种参数，包括传输数量、传输内容、目标地址等，以及网络流量的行为特征，及时发现异常安全风险。当出现安全威胁或违规行为时可以发出警报，帮助企业应对发生的数据安全事件。

3、跨境数据异常行为分析。通过对异常的跨境行为的分析，识别如大规模数据下载、频繁登录尝试以及数据泄露等行为，帮助企业发现风险及时处置。

4、多因素认证与访问控制。在保障敏感数据安全的过程中，多因素认证和访问控制是两个至关重要的环节。通过实施基于角色的访问控制（RBAC）和最小权限原则，企业可以确保只有经过授权的用户才能访问敏感数据，从而有效防止数据泄露和非法访问。基于角色的访问控制（RBAC）是一种灵活且高效的安全策略。企业可以精确地控制用户对敏感数据的访问权限，避免权限过大或过小的问题。这种策略不仅简化了权限管理过程，还提高了数据的安全性。除了RBAC和最小权限原则外，多因素认证也是增强访问安全性的重要手段。这种认证方式比传统的单一密码认证更为安全，因为它结合了多种验证方式，提高了账户的安全性。企业可以确保只有授权用户才能访问敏感数据，并降低数据泄露和非法访问的风险，有助于提升企业的数据安全防护能力。

5、建立应急响应机制。建立应急响应机制也是企业出海数据安全不可或缺的一环。企业应针对可能的数据泄露和安全事件制定详细的应急响应计划，包括应急响应团队的组织、事件报告流程、数据恢复措施等。通过应急响应机制的建立，企业可以在发生安全事件时迅速采取行动，减轻事件对企业运营和客户信任的影响。

6、员工培训与意识教育。随着企业在全球范围内开展业务，跨境数据传输和数据处理成为常态，敏感数据的安全问题也愈发凸显。提升员工对数据保护和安全性的认识，培养员工安全意识和行为习惯，成为企业保障数据安全不可或缺的一部分。

供应链安全场景

在企业出海的过程中，向海外第三方服务商采购数据存储、云计算、支付处理等服务，可以提高效率、扩大市场覆盖和提升服务质量。这种合作模式也引入了供应链数据安全风险，需要通过有效的策略进行管理。

场景与风险分析

1、数据泄露风险。第三方服务商可能负责存储和处理企业的敏感数据，如用户个人信息、财务记录等。同时数据在企业与第三方服务商之间传输时可能面临截取和非授权访问的风险。第三方服务商的安全漏洞和数据传输风险可能导致敏感数据泄露，危害企业和用户的利益。

2、第三方服务商合规风险。第三方服务商合规风险是企业在数据安全管理中必须面对的重要挑战之一。当企业选择将部分业务或数据处理任务委托给第三方服务商时，必须确保这些服务商能够严格遵守相关的数据保护法律。然而，如果第三方服务商未能履行其合规义务，企业可能会因此面临严重的法律诉讼和罚款。首先，数据保护法律对于企业和第三方服务商都有明确的规定和要求。这些法律旨在保护个人隐私和数据安全，防止数据被滥用或泄露。在选择第三方服务商时，企业应进行严格的尽职调查，评估其合规能力和信誉度。其次，企业应与第三方服务商签订明确的合同，明确双方的权利和义务，特别是关于数据保护和合规方面的要求。此外，企业还应定期对第三方服务商进行合规审计和监督，确保其持续遵守相关法律和规定。

3、供应链攻击风险。企业往往依赖于众多的第三方服务商来支持其业务的顺利开展，这些服务商可能涉及云服务、数据分析、数据处理等多个环节。然而，这也为攻击者提供了可乘之机。攻击者可能将目标转向这些第三方服务商，通过渗透攻击、恶意软件植入等手段，获得对服务商系统的控制权。

4、供应商内部威胁风险。第三方服务商内部人员的恶意行为或疏忽可能导致数据安全事件。企业出海场景下第三方服务商为企业提供了各种关键服务，如数据存储、处理、传输等。然而，这也使得第三方服务商内部人员成为了潜在的安全风险点。这些人员可能因个人动机、经济利益或其他原因，对企业的数据进行窃取、篡改或破坏。

解决方案

1、建立供应商筛选机制。在选择第三方服务商前，开展必要的安全和合规性审查，包括：了解服务商的安全政策，评估其是否具备完善的安全管理制度和措施；查阅服务商的合规记录，确保其业务操作符合相关法律法规的要求；关注服务商的数据保护实践，确保其能够妥善处理和保护企业的敏感数据。通过这样的筛选过程，企业能够筛选出真正可信赖的合作伙伴，确保企业数据的安全与合规。

2、建立详尽的合同条款。在签订合同时，双方应明确数据保护责任，确保服务商能够严格遵守相关法律法规，保护企业数据的安全与隐私。同时，合同中也应详细规定合规要求，包括数据处理的规范流程、安全措施的具体实施等。此外，还应明确审计权和违约责任，以便在发生问题时能够及时追溯和解决。通过详尽的合同条款，企业能够有效地降低与第三方服务商合作中的风险，确保合作的顺利进行。

3、实施数据加密传输。实施端到端加密是企业在与第三方服务商合作中保护数据安全的重要手段，也是保障数据在传输过程中安全的关键措施。对于任何传输给第三方服务商的数据，企业都应采用强加密标准进行加密，以确保数据在传输过程中不被非法截获或篡改。这种传输方式可以确保数据从发送端到接收端始终保持加密状态，即使在网络传输过程中被截获，攻击者也无法解密和获取其中的敏感信息。

4、定期安全和合规性审核。定期安全和合规性审核是确保第三方服务商持续遵守合同安全标准和法规要求的关键环节。企业应设立完善的审核机制，定期对服务商的安全管理制度、数据处理流程、安全防护措施等进行全面检查。通过这样的审核，企业可以及时发现并纠正潜在的安全隐患，确保服务商能够始终维持高标准的安全防护水平。

5、开展访问控制与安全监测。督促第三方服务商建立细致的权限管理制度，对敏感数据的访问进行严格限制，确保只有经过授权的人员才能访问相关数据。同时应保证第三方服务商实时监控数据访问活动，记录每一次访问的详细信息，以便在发生异常情况时能够迅速追溯和定位问题。

6、实施数据处理和存储的地理限制。根据企业的实际需求和法规要求，应对服务商的数据处理和存储地理位置进行明确限制。这既有助于保障数据的合规性，避免违反相关法规，又能确保数据的安全性和隐私性。通过设置地理限制，企业可以防止数据被传输到被限制地区，从而有效减少数据泄露和滥用的风险。因此，在与第三方服务商合作时，企业应充分考虑数据处理和存储的地理限制，并将其纳入合同条款中，以确保数据的合法、安全和有效使用。

7、建立应急响应和安全事件通报机制。在与第三方服务商合作时，企业应确保合同中明确包含这两项条款。应急响应条款规定了当发生数据安全事件时，服务商应迅速启动应急响应计划，采取必要的措施来减轻损失和恢复数据安全。而数据泄露通知条款则要求服务商在发现数据泄露事件后，及时通知企业，并提供详细的泄露情况和处理进展，以便企业能够迅速做出反应，防止事态进一步恶化。

网络攻击防护场景

面对日益复杂的网络威胁，企业必须采取一系列措施来防范和应对潜在的网络攻击，以保护企业资产和客户数据。

场景与风险分析

1、恶意软件攻击。恶意软件攻击攻击形式多种多样，包括病毒、蠕虫、特洛伊木马等，它们不仅会对企业的信息系统造成破坏，导致业务中断，还可能窃取企业的敏感数据，甚至进行勒索，给企业带来巨大的经济损失。在全球化背景下，企业面临的网络环境日趋复杂，恶意软件攻击的频率和复杂性也在不断增加。

2、社会工程攻击。社会工程攻击如钓鱼邮件等方式，通过假冒合法实体的电子邮件或网站，精心构造逼真的信息，诱使用户点击链接或下载附件，进而获取用户的敏感信息，如账号密码、企业核心数据等。一旦攻击者得手，这些信息可能会被用于非法活动，给企业带来巨大的经济损失。

3、分布式拒绝服务攻击（DDoS）。DDoS攻击者通过操控大量计算机或网络设备，向目标企业的网络服务发送海量请求，导致合法用户请求无法得到及时处理，进而使网络服务陷入瘫痪状态。这种攻击不仅严重影响了企业的正常运营，还可能导致客户流失、业务中断等严重后果。

4、零日漏洞攻击。零日漏洞指的是那些尚未被公开或修复的软件漏洞，而攻击者往往能够利用这些漏洞进行精准打击。一旦攻击者发现了某个软件的零日漏洞，他们可以迅速利用这个漏洞入侵企业系统，窃取敏感数据，甚至篡改系统数据，给企业带来无法估量的损失。

5、内部威胁。企业内部人员，无论是出于疏忽还是恶意行为，都有可能成为安全事件的导火索。一些员工可能由于安全意识薄弱，随意泄露企业敏感信息或误操作导致数据泄露；而另一些员工则可能出于个人利益或其他目的，故意破坏企业系统或窃取数据。这些内部威胁不仅可能导致企业经济损失，还可能损害企业声誉和客户关系。

6、供应链攻击。攻击者利用企业的供应商或合作伙伴作为切入点，通过渗透这些合作伙伴的网络，进而侵入企业的核心系统。这种攻击方式不仅隐蔽性强，而且难以防范，一旦攻击成功，攻击者便能够轻易获取企业的敏感数据，甚至对企业的运营造成严重影响。

解决方案

1、建立全面的安全管理制度：企业应建立全面的安全管理制度，不仅应涵盖网络设备的配置、数据传输的加密等技术细节，还应包括定期的安全审计和风险评估，以便及时发现潜在的安全隐患。此外，加强员工的网络安全培训也是不可或缺的一环。通过培训，员工能够提升对网络威胁的识别能力，掌握应对网络攻击的基本方法，从而为企业数据安全筑起一道坚实的防线。

2、强化技术防护措施：首先，安装并定期更新防病毒软件、防火墙和入侵检测系统，以有效抵御恶意软件和其他网络攻击的威胁。这些工具能够实时监控网络流量，及时发现并阻断潜在的安全风险。其次，采用先进的加密技术，保护数据的传输和存储过程，防止敏感信息被窃取或篡改。此外，实施多因素认证机制，要求用户在登录时提供多个验证信息，进一步提高账户的安全性，降低被攻击的风险。

3、备份和恢复计划：为确保企业业务的连续性与数据的完整性，企业应当建立一套定期备份关键数据和系统的机制，以防止数据因各种潜在风险而丢失或损坏。同时，制定并严格测试数据恢复预案也至关重要，这一预案应明确阐述在遭遇网络攻击或其他安全事件时，如何迅速且有效地恢复业务运营。通过模拟真实的攻击场景进行演练，企业能够确保恢复预案的可行性和有效性，从而最大限度地减少因数据安全问题而带来的潜在损失。

4.DDoS攻击防御：企业应建设业务系统的抗DDoS能力，以实时监测和应对各种DDoS攻击。同时，企业还应配置网络流量监控和过滤机制，通过精准识别和及时阻止异常流量，确保网络服务的稳定性和可用性。

5、零日漏洞防护：为了确保企业数据和系统的安全，保持软件和系统的及时更新是首要任务。通过及时修补已知的安全漏洞，企业能够降低被攻击者利用这些漏洞进行攻击的风险。此外，采用先进的终端保护解决方案也是关键措施之一。这些解决方案，如行为分析和沙箱技术，能够实时监控和识别可疑行为，从而有效隔离和防御潜在的零日漏洞攻击。

6、内部安全控制：为了防范内部威胁，企业需实施严格的访问控制和权限管理，确保员工只能访问其工作所需的敏感数据，防止数据泄露或被滥用。同时，监控内部网络活动也是必不可少的措施，通过实时监控和分析网络流量、用户行为等数据，企业能够及时发现异常行为，并迅速响应，防止内部安全事件的发生。

7、供应链安全管理：为确保供应链的安全稳定，企业应首先对供应商和合作伙伴进行全面的安全评估，确保他们严格遵守相关的安全标准和规范。同时，与供应链各方建立明确的安全协议也必不可少，这有助于明确各方的安全责任和要求，形成共同的安全防护体系。

企业数据跨境安全合规指引 2024

第六章
数据跨境安全保障方案

数据跨境合规要求

在企业数据跨境流动场景下，构建数据安全防护体系是保护企业敏感数据和确保合规性的关键。在全球化进程中，企业出海已成为重要的商业策略，出海过程中同时需要遵守不同市场的法律法规，避免数据泄露和违规操作。因此，建立一套完整的数据安全技术体系，有助于企业全面加强数据安全保护，降低因数据泄露和违规操作而带来的法律风险和业务损失。

数据跨境流动合规监管

在数据跨境过程中，数据流向难以清晰可见，难以确定是否存在敏感或重要数据流出的问题，行业内存在业务系统交互复杂、多样化的数据交互方式，导致数据交换缺乏监管。建设数据跨境流动合规监管平台，旨在为数据跨境提供全面的数据出境流动安全合规监管。该平台的目标是实现对出海数据全生命周期的风险管控，包括但不限于出海数据流动的实时监控、风险态势的监测、使用区块链技术进行审计的跨境行为、即时告警通报、出海数据舆情监测以及有效应对跨境威胁的响应与处置。

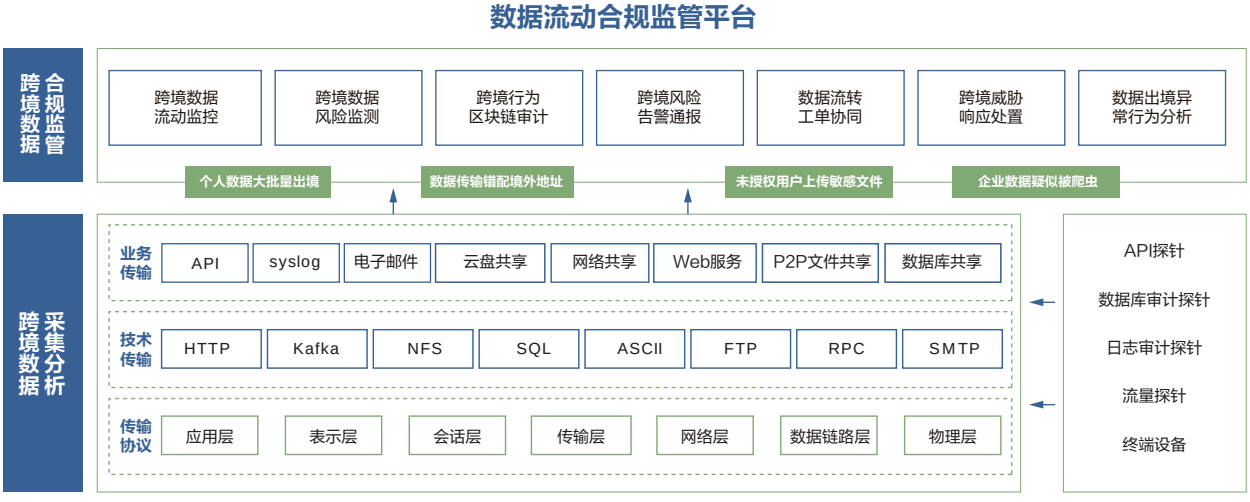


图6-1 数据流动合规监管平台

数据采集分析

利用各种采集工具（探针）实现出海数据全流程日志数据的采集和汇聚，具体采集内容包括安全设备日志、数据库审计

日志、数据流动环境的流量等，建立安全数据仓库，为出海数据安全监控和风险分析提供原始数据支撑。安全设备告警日志：利用日志采集工具针对业务系统及安全设备告警日志进行采集，实现安全设备数据的统一收集。数据生命周期关键流量：利用节点流量采集工具针对数据流转各环节的安全问题，平台采集各业务系统的数据产生、传输、存储、处理、交换、销毁等数据全生命周期过程中的关键流量。通过云原生支持的内部流量镜像的方式或在业务系统ECS主机上部署代理的方式采集数据全生命周期关键流量，并深度分析以HTTP、FTP、SMB、SQL等方式实现的数据增删改查操作行为的安全风险。

流量采集：数据出海检查与分析系统产品支持对镜像到设备上的网络流量进行在线数据采集。可基于源地址/地区、目的地址/地区、传输方式、传输应用等多种采集策略进行流量采集。

流量还原：数据出海检查与分析系统产品通过对采集的流量进行还原，生成各种网络原数据，比如TCP、UDP会话日志、Web访问、SSL访问、邮件传输、DNS请求、文件传输等类别的网络行为日志，对原始日志进行合并、去重、关联，形成独立告警信息和事件关联分析。

内容识别：数据出海检查与分析系统产品通过内容深度分析技术，实现文件类型检测、文件内容提取及分析、压缩文件内容提取及分析、图片文件内容提取及分析等，还支持对数据库、API、应用等载体进行深度识别，结合用户业务数据特点进行深度内容分析，判断内容中是否包含个人/敏感、重要等信息。

敏感数据传输检测：数据出海检查与分析系统产品内置常见个人/敏感信息，重点行业的重要数据等敏感标签，通过协议解析、解码、应用识别与私有协议还原能力，提取各类应用传输数据要素，将涉及个人/敏感信息、重要数据等带有敏感标签的内容进行深度检测分析。

出海数据检测：数据跨境检查与分析系统产品具备对出境数据的检测能力，通过监测网络数据的源地址以及目的地址，关联区域地址信息，可精准检测从境内到境外的数据传输行为，对出境数据进行精准检测。另外针对敏感信息出境场景，实现跨境地区分布展示、跨境敏感信息趋势展示及跨境敏感信息的多维筛选、统计分析，通过对敏感数据告警与流量协议还原、行为还原元数据进行去重、归并、关联分析，发现跨境敏感信息传输。

数据合规监管

围绕着数据跨境全生命周期及数据使用业务场景等数据安全监控预警，实现对数据跨境的全生命周期风险管控，包括出海数据流动监控、出海数据风险监测、跨境行为区块链审计、跨境风险告警通报、出海数据舆情监测、跨境威胁响应处置。并对发现的数据安全风险进行提前预警和处置，实现数据跨境安全监管对象安全建设的可知、可管、可控。

跨境数据流动监控：建立实时监控系统，追踪和记录跨境数据的流动情况。通过监控系统，可以迅速发现任何未经授权的数据流出，以及监测数据传输的合规性和安全性。可针对出海数据进行流动分析，自动关联流出IP、流出国家、流入IP、流入国家，形成出海数据流动的可视化清单列表。

跨境数据风险监测：利用先进的数据分析和机器学习技术，对跨境数据进行风险评估。识别潜在的数据泄露、攻击或其他安全风险，及时采取措施进行防范。对于违规告警产生的原始数据需要进行数据留存，留存的信息包括原始传输的数据包信息，经过数据还原加工的文件信息、数据库信息、邮件信息等格式化之后的原始数据信息。

跨境行为区块链审计能力：引入区块链技术，建立跨境行为审计系统。记录网络数据审计日志，比如TCP、UDP会话

日志、Web访问、邮件传输、API接口传输数据、数据库传输数据、文件传输等信息进行汇总，关联分析的维度包括但不限于传输源信息，传输目的信息，传输数据类型信息等，最终统计出境数据的数量、范围、种类、敏感程度等各维度信息。

跨境风险告警通报：可对出海数据进行合规性检查，分析系统通过对关联分析出的出境数据的数量、范围、种类、敏感程度等各维度信息结合规则进行比对判定是否合法合规，规则包括系统内置的根据法律法规生成的数据传输规则以及数据出境风险自评估审批后生成的规则等。

跨境数据舆情监测：建立出海数据舆情监测能力，开展多渠道监控。通过整合多渠道的信息源，包括社交媒体、新闻、论坛等，实时监测舆情动态。利用自然语言处理技术进行情感分析，了解舆情事件的正面、负面和中性情感，帮助客户更全面地理解舆情背后的情感趋势。识别和提取关键词，帮助用户更快速准确地了解舆情事件的核心内容和关注点。对舆情事件进行趋势分析，帮助用户预测和应对可能的影响。

跨境威胁响应处置：结合跨境威胁响应和处置流程。一旦发现威胁，能够迅速采取措施进行应急响应和风险处置，减轻潜在损失。通过统一安全策略和联动管理中心，在高频数据安全风险场景下，针对由组件监测识别出在数据流转链路中出现的风险隐患，可以实现点对点的快速联动验证、风险处置，提高整体数据跨境安全运营效能。

数据跨境安全服务平台

跨境数据安全服务平台是为企业提供的一套完整的出海数据安全解决方案，旨在帮助企业在全球市场运营过程中，确保数据安全合规。该平台设计为三个组成部分，包括数据跨境安全基础能力、安全可信融合计算中台以及安全能力服务总线。

首先，数据跨境安全基础能力为企业提供了一系列保障数据安全的核心功能。这些功能涵盖了从设备层到数据层的全面保护，如设备漏洞检测、数据的分类分级、数据运维审计与控制、数据接口的安全管理等。通过这些功能，企业可以有效识别并修复数据处理设备中的安全漏洞，确保跨境数据传输中的合规性。此外，平台还具备账号统一身份认证、数据脱敏技术及数据防泄漏等能力，保障数据在跨境过程中不会被恶意窃取或不当使用。通过用户行为分析模块，平台还可以监测数据使用情况，进一步防范潜在的内外部威胁。

其次，安全可信融合计算中台提供了更为高级的数据安全处理机制，包括安全可信执行环境、多方安全计算、密文存储和区块链合规审计等模块。安全可信执行环境确保数据在处理和计算时不会被篡改或泄露，多方安全计算允许多个参与方在不暴露各自数据的情况下进行联合分析，而密文存储和密钥管理则保证了数据在存储过程中即使遭受攻击也能保持保密性。通过区块链技术的应用，平台能够提供透明、不可篡改的数据审计记录，确保跨境数据传输的合规性和透明度。

最后，安全能力服务总线通过调用基础安全能力和中台的融合计算能力，为企业提供了数据出境场景下的全面安全保障。总线为企业提供了诸如数据出境场景识别服务、数据出境安全评估、数据加密和脱敏等服务，确保数据在跨境流动过程中保持完整性、保密性和可用性。这一模块的重点是帮助企业在全球不同的监管环境下实现合规性，并根据不同地区的数据保护法律（如GDPR等）进行相应的数据安全措施，以减少数据出境的风险。

综上，数据跨境流通安全服务平台不仅为企业提供了坚实的数据安全基础，还通过先进的计算技术和安全服务总线，实现了多层次、多场景的数据安全保障，帮助企业在全球化过程中有效应对数据跨境流动的复杂性与挑战。

数据跨境数据安全服务平台架构

图6-2 数据跨境数据安全服务平台架构

设备漏洞检测

加强终端安全管理，能够发现数据跨境主机、设备、数据库等存在的网络安全漏洞。可对不同操作系统下计算机进行漏洞检测，分析指出网络安全漏洞及被测系统薄弱环节并给出详细检测报告及修补措施和安全建议。包括设备资产探测，对目标基础信息识别，支持任务操作及状态结果上报；弱口令和系统漏洞扫描，对存活目标主机漏洞识别及深入信息扫描，弱口令扫描结合字典尝试登录，支持任务操作及状态结果上报；Web 应用安全漏洞扫描，对网站爬取和漏洞识别，支持任务操作及状态结果上报；数据库漏洞扫描，通过指定账号信息登录目标数据库进行漏洞识别、安全信息展示和深度漏洞检测，支持任务操作及状态结果上报；安全配置基线核查，基于模板对目标进行配置检查，使用登录协议判断配置是否符合标准并输出符合情况。

数据分类分级

建立数据分类分级保护机制，可对跨境数据进行自动数据发现、敏感数据识别，能使用系统内置或导入法规标准进行分类分级操作并生成数据资产目录。内置多种智能识别模型，包括基于深度学习 + 条件随机场的命名实体识别模型可准确高效识别中英文姓名等，基于 NLP 技术的文本识别模型可判断敏感文本数据，还支持正则表达式、字典等识别规则。能从多个维度感知数据资产分布和使用状况，对多次扫描结果提供变化标注，数据资产目录支持多维度展示，可与数据防护系统 API 对接以实现进一步分级保护。分类分级模板管理内置丰富模板，可根据行业和法律法规细分选择，支持对规则进行过滤和编辑，包括对算法规则启用/禁用、修改和删除，设定敏感数据定义策略，更改分级标签名称，配置数据表级分类分级策略。

数据运维审计

以数据安全事件为中心，以全面审计和精确审计为基础，实时记录网络上的数据库活动，包括记录一切对数据库的访问行为，记录维度涵盖客户端信息、服务端信息、操作信息、操作状态、返回结果集、SQL 模板等，并存储记录行为时产生的包括审计日志、会话日志、告警日志及系统相关配置的日志。支持在已有的日志中通过时间、类型、数据库实例名、操作结果、客户端、服务端等查询维度查询关键信息完成事件溯源。将数据库访问的行为与安全规则库进行匹配进行风险和威胁告警，包含页面告警、外送告警（钉钉、邮件、企业微信、SNMP 等）。其次，支持海量协议，包括国内外主流数据库，涵盖传统数据库系统、大数据系统和 Web 系统等，保持最快更新速度适配相关协议最新版本。还可进行加密协议解析，通过导入证书采用加密协议通讯对加密流量进行审计；进行中间件规则解析与审计，通过接口调用获取中间件转换规则提升协议解析准确率；实现无连接信息还原，根据通信信息特征倒推协商信息提升解析精准度进行精准审计；以及具备审计补偿机制，在 SQL Server 审计场景下补全缺失用户信息将数据库访问行为关联到实际操作人。

数据运维控制

数据安全网关系统包含基本数据库防火墙功能及融合了精细化访问控制、具体行为策略、数据库动态脱敏等功能。数据访问控制可通过多个维度对用户身份进行识别，结合分级分类结果对进出核心数据服务访问流量进行高效精准解析和精细控制，实现强制访问控制保障数据不被越权访问，识别可疑违规行为。内置多种常见数据攻击规则可针对多种攻击场景提供防护，减少数据风险，也支持自定义安全规则适应复杂业务场景防止数据库攻击和避免误操作隐患。动态脱敏具备对多种数据库敏感数据脱敏功能，内置多种脱敏方法和标识符变形方法，实现用户数据可用不可见，丰富算法库满足各种场景脱敏需求，降低使用难度和工作负担，有效避免或降低数据泄露风险，开启动态脱敏规则可在无法实施数据加密时保障数据机密性。

接口安全管理

系统可自动识别梳理跨境 API 接口，检测 API 脆弱性防止敏感数据泄漏，对违规数据行为监控告警。当数据泄漏事件发生时，可快速溯源分析定位泄漏源并评估影响面。具备敏感操作还原功能，可记录网络上流动的敏感数据，解析还原操作事件，识别多种文档类型，关联账号身份及组织架构信息。提供数据资产梳理和可视化能力，包括数据资产全景图及监控告警能力，基于网络流量解析还原技术形成数据资产目录，区分 API 和应用 URL。账号行为监测可分析用户行为，对比是否存在异常行为。安全风险分析包括 API 脆弱性风险和用户行为风险，提供业务系统安全状况监控展示能力，实时监测接口脆弱性问题和异常访问行为，用户行为画像构建标准基线发现潜在威胁。风险策略定制提供自定义脆弱性和风险规则指标，可根据多种方式进行配置，协助用户加强数据安全管理机制，内置数据安全策略。

账号统一身份认证

统一身份认证核心组件由零信任身份服务中心、零信任安全客户端、零信任应用代理系统三大部分组成，用于控制用户内部使用账号执行跨境数据操作的统一身份认证。

零信任身份服务中心负责认证、授权、策略管理与下发，是整体的调度与管理中心，可控制主体与客体间的通信连接，生成身份验证令牌或凭证，支持自适应身份认证、动态权限控制，对身份、终端、环境、行为进行信任评估以决定会话的允许或拒绝，受 SPA 单包授权技术保护实现设备服务隐身，只有授权客户端能打开认证页面及接入服务，提供身份管理服务可对设备、用户、角色等身份统一配置管理，支持与第三方数据源对接及加密存储身份信息，还提供用户认证服务，本地默认提供账号密码、OTP 认证方式，支持调用多种第三方认证源认证，非标接口标准认证源可定制对接。

零信任安全客户端覆盖 PC 和移动端，支持 SSL 隧道访问，PC 客户端提供终端安全检测能力并上报给零信任身份服务中心进行信任评估，开启 SPA 服务隐身后，只有授权客户端才能连接零信任身份服务中心和零信任代理系统进行认证、授权和代理访问。

零信任应用代理系统负责建立、监视及切断主体与客体间连接，与零信任身份服务中心通信接收策略和指令，支持 HTTPS 和 SSL 隧道代理访问，受 SPA 单包授权技术保护，记录访问请求可进行日志审计并支持对接第三方日志平台。零信任身份服务中心通过 SPA 技术实现网络隐身，降低业务暴露面。

数据脱敏功能

数据静态脱敏能对敏感数据进行去标识化、匿名化处理，有多种算法，如置空（直接将待脱敏信息以填充空字符或者删除的形式抹除）、乱序（在结构化数据中常用，随机打乱数据顺序）、遮蔽（保留部分信息，用指定字符替换敏感位置信息）、分割（保留部分信息，删除敏感位置信息）、替换（用固定值或字典映射表对敏感数据进行替换）、取整（对数值和日期时间类型数据取整）、哈希（将哈希编码后的数据作为脱敏结果输出）、仿真（保留业务含义，生成符合核验规则的数据）、密码学（用指定加密算法对数据进行加密，支持 RSA/AES/SM2/SM4 等算法）。静态数据脱敏主要是将数据库根据过敏规则隐藏或模糊化真实敏感数据，提高生产数据在新的应用开发、测试等场景下的数据安全性和有效性。数据溯源算法多样，有伪行伪列等常见算法，还有脱敏水印、内容修改水印等隐蔽性强不易绕开的算法予以支持。

数据网络防泄漏

数据防泄漏系统以流量解析还原和敏感数据识别为基础，自动识别流量中传输的敏感数据，防止数据跨境敏感数据泄漏，对违规使用数据行为进行监控告警。当数据泄漏事件发生时，可快速溯源分析，定位泄漏源并评估影响面。在应用协议解析方面，平台支持 HTTP/HTTPS 协议，可对数据外发进行实时审计和阻断；支持邮件协议，对 SMTP 发送邮件内容及加密邮件进行实时审计和阻断，对 POP3 和 IMAP 接收邮件进行内容审计；支持 FTP 协议，对上传和下载数据进行实时内容审计；支持文件共享协议，对 SMB 和 NFS 协议文件传输进行实时审计，监控敏感文件上传下载。在文件内容解析方面，提供文件类型及内容识别、嵌套及多层压缩文件识别、图片 OCR 解析以及多种语言和汉字编码格式识别功能。策略匹配系统支持多种维度的策略制定、查询和修改等操作，包括关键字策略、正则表达式策略、结构化与非结构化指纹策略、数据标识符策略以及反向关键词和例外规则检测。

数据终端防泄漏

终端防泄漏以数据智能识别和发现为基础，通过多种手段保护业务系统和终端上的业务数据。信息识别方面，支持对文档、源代码、图片等文件进行源格式识别，基于多种方法对内容感知，实现文档类别、级别判定及数据血缘关系等分析。监控保护方面，可无感知扫描硬盘数据生成敏感数据分布地图，识别潜在风险，记录各种行为，支持可视化展示和灵活策略设置，对违规行为进行阻断、提示和告警及动态策略应对。还支持添加水印，对文档进行全方位记录和溯源，一旦泄密可追溯源头并进行全面分析定位。

数据用户行为分析

用户行为分析实现对用户整体数据跨境环境的威胁感知，通过标准化和规范化零散数据，利用深度安全分析模型及算法和 AI 分析模型发现安全风险和异常行为，实现多种形式场景建模，为用户提供实体安全和应用安全分析能力。

首先，用户信息管理建立用户与账号关联台账并全生命周期管理，为用户异常行为分析提供依据。其次，用户行为特征创建建立标准化安全特征管理，可根据业务场景调整权重、创建模型、自定义特征，满足实时和离线建模需求。第三，用户总体风险监测提供宏观全局风险视角，包括风险排行、分布、高危类型概览和风险阈值调整，方便安全人员定位高风险用户和排查风险。第四，用户行为画像采用大数据技术描绘用户信息全貌，可对比异常行为、威胁溯源和检测未知威胁，提供风险趋势和全局画像模式以及自适应威胁场景，通过用户总体风险和用户实体画像辅助安全人员定位高危用户，提升安全运维效率。

数据隐私计算平台架构

安全可信融合计算中台

除了一般数据外，数据跨境流动还存在高敏感、高价值、高保护需求的数据流动情形。例如，汽车自动驾驶场景需要车外视频数据等重要数据，如何平衡数据应用与跨境流动安全是企业亟需解决的问题。

安全可信融合计算提供多方数据融合计算解决方案，实现数据的“可用不可见”，对数据的所有权和使用权做有效分离。可用于敏感数据的挖掘，在原始数据不泄露的情况下有效挖掘价值数据。安全可信计算中台是数据跨境数据安全服务平

台的核心，其能够保证数据隐私安全的基础上，实现数据的计算价值，同时也能灵活扩展、兼容其他多种技术，对打破数据孤岛、促进数据共享流通有重要意义。安全可信计算中台包括可信执行环境、多方安全计算、数据审核授权、密文存储、密钥管理、区块链安全审计等核心能力。

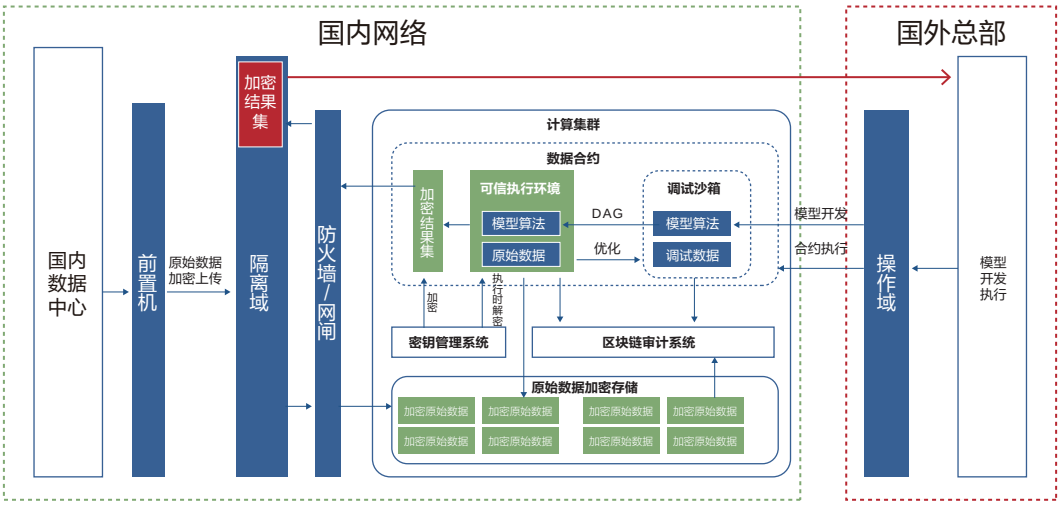


图6-3 安全可信融合计算平台架构

可信执行环境：可信执行环境包含两部分，安全调试沙箱、安全计算沙箱。安全调试沙箱通过调试测试进行数据模型开发和数据模型验证。安全计算沙箱通过验证成功的数据模型运算数据集得到满足数据获益方需求的数据结果集。安全调试沙箱：数据进入安全计算沙箱进行运算前，给开发人员提供安全测试沙箱环境，开放部分样本数据进行算法的调试。技能保障最终算法的准确性，又能确保开发人员不过多的接触到敏感数据，保障数据安全；安全计算沙箱：基于安全计算沙箱技术，沙箱环境与数据合约绑定，为每个计算任务创建独立的容器环境，不同合约之间的数据完全隔离；为关键数据计算任务创建可信执行环境BDTee执行空间和资源分离，所有需要高度保密的操作在操作系统内核隔离态执行，其余操作在正常环境执行；安全计算沙箱内的计算任务和操作都会详细审计和记录，可实现操作监控和历史回放，方便后续事件溯源。

多方安全计算：多方安全计算包括：Hive、Spark、Python研发开发、密文计算、密文查询、密文求交等技术。可信执行环境构建在大数据底层架构之上。支持分布式任务调度，并可根据业务发展情况动态扩容。平台提供Hive、Spark、Python、shell等开发页面。

数据审核授权：数据审核授权具备“所有权”和“使用权”的界定。数据的所有权应当归属数据提供方/生产方，得到授权的用户方可拥有数据的使用权。通过细粒度数据授权控制、数据合约审批、结果审批等，实现数据所有权和使用权分离。当数据被第三方使用时，保障数据拥有者具备知情和拒绝的权利，让参与各方都可以安全、便捷、灵活的进行数据共享和交换，保证数据安全和保护隐私。

密文存储：提据加密可以防止明文存储引起的数据泄密，应对突破边界防护的外部黑客攻击、来内部高权限用户的数据窃取、及绕开合法应用系统直接访问数据库等行为等。数据存储加密包括文件加密和数据库加密两部分内容。文件加解密：支持按指定格式自动发现和统一加密文档；支持用户手动选择文档进行加密，并可在加密后设置该文档的具体使用权限。数据库加解密：支持细粒度加解密，可配置整库加密、表加密、字段加密等不同粒度的加密方式；支持透明加解

密，实现SQL语句透明、存储程序透明、开发接口透明和管理工具透明；支持动态加解密，实现密文存储明文显示的效果。支持我国密码管理机构认定的加密算法，用户可灵活选择3DES、AES、SM4等算法。数据防泄漏主要通过监听全流量数据，实现数据传输应用和传输协议的分析，实现对数据泄露的监测，联动动态数据安全网关，实现对数据泄露操作的阻断。数据泄露行为识别：使用自然语言处理、数据挖掘、和机器学习技术自动学习数据的使用行为，生成可信行为区间，以提高对数据泄露行为识别的准确率和可靠性；泄露数据定位能力：包含数据定位的策略手段，支持对结构化数据和非结构化数据中的已泄露数据信息进行定位。

密钥管理：提供独立统一密钥管理，支持独立密钥管理体系，包含加密密钥生成，分配，备份，恢复，密钥不出设备。加密密钥统一由主密钥进行保护，主密钥由KMS通过硬件密码设备产生并管理，确保主密钥安全。为数据合约的参与方提供私钥，私钥的获取方式包括平台方分发和参与方自行生成后，注册至平台。私钥由参与方自行保管，从而保障私钥的安全性。

区块链安全审计：为了防止用户违规操作导致平台发生安全事件，需要对用户在平台上的操作行为进行详细记录和审计。使用区块链技术存储合规审计日志，杜绝审计日志丢失或被篡改。同时结合日志和流量分析技术，对用户的操作行为进行准确记录和验证。并对其行为进行智能分析，及时发现异常现象，防止不合规的操作发生。

数据安全计算调度平台

数据安全计算调度平台主要包括：账户管理、数据管理、合约管理、接口管理等功能。

根据数据融合交换的业务需求，平登用户角色和权限如下：

1、系统管理员。平台建设方掌握系统管理员账户。作为平台的权限、用户和组织架构的管理员，主要负责对整个系统的正常运行及维护，其他数据合约账户的申请、授权和分配等。

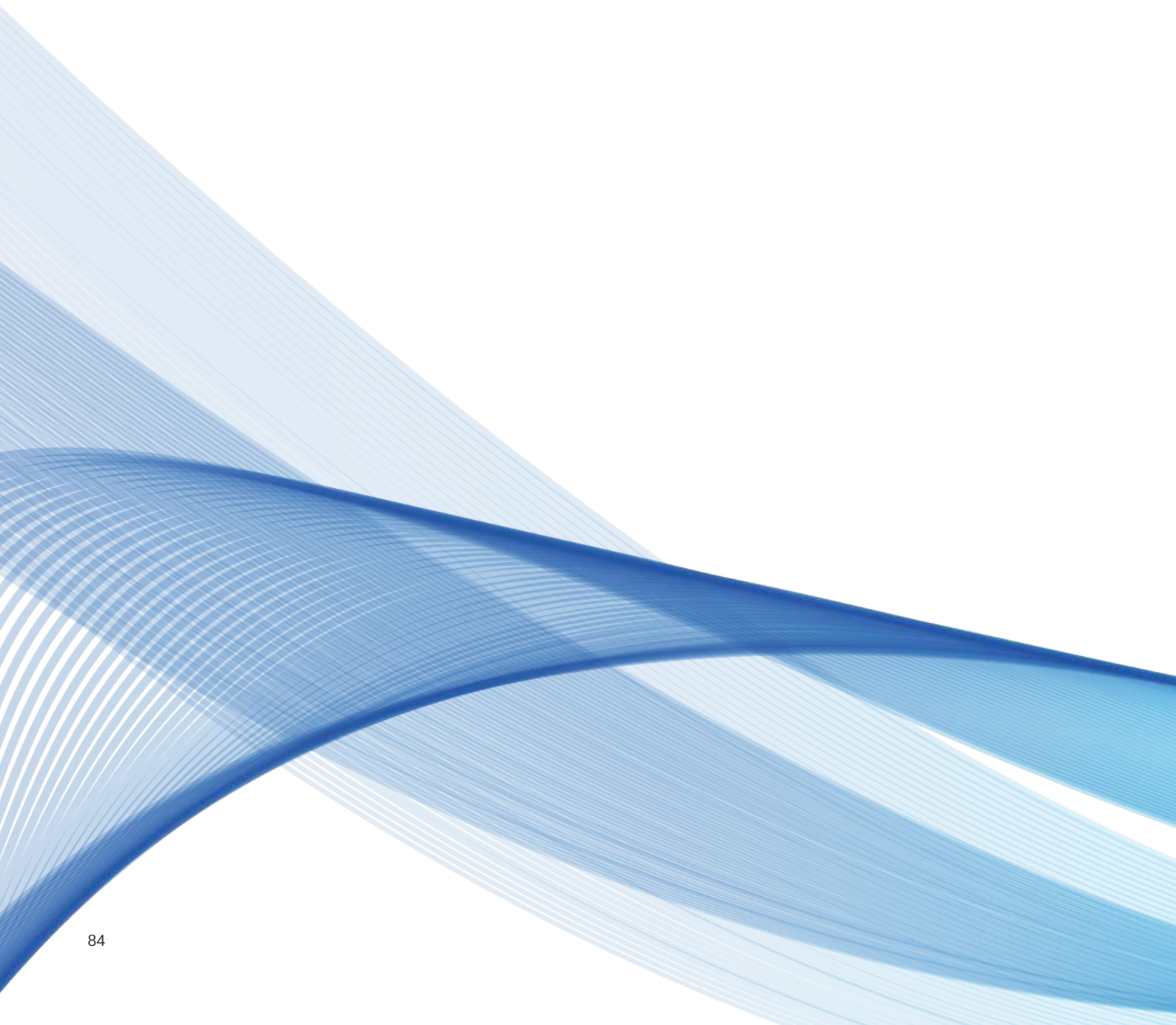
2、数据合约账户。数据合约账户主要分为数据需求方账户和数据提供方账户，具体的账户权限和类型由系统管理员进行分配与预授权。在某些场景下，数据需求方账户也可以具备数据提供方的权限。主要具备数据上传、数据融合计算授权、结果集审核、下载等。

3、数据建模账户。数据建模账户由平台建设方掌握，由平台建设方建立运营团队负责，具体的账户权限和类型由系统管理员进行分配与预授权。主要的职责为根据数据合约账户提供的原始数据、数据需求进行模型开发和运行，得到数据融合计算结果。

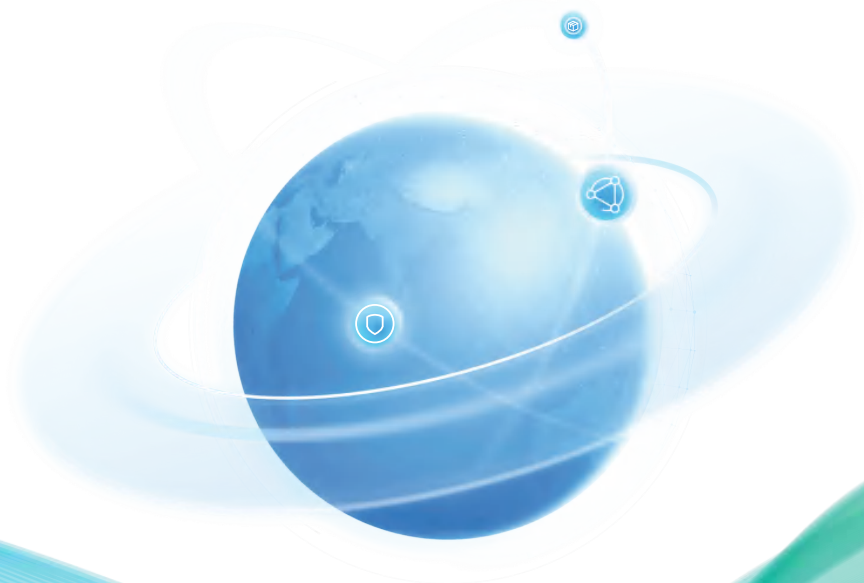
4、数据管理。数据管理主要针对由数据提供方上传至平台的用户融合计算的数据、融合计算的结果数据的管理。

数据的管理功能主要包括数据集的上传方式管理，其中包括上传通道建立、数据加密秘钥分配、上传方式审核等；数据集使用的授权和管理，数据集的使用主要采用数据提供方和平台方双方授权的方式进行，授权的数据主要包括上传的原始数据和结果集数据。支持查看平台内已开放的数据集、查看数据集的详情和关联的调试数据。

企业数据跨境安全合规指引 2024



第七章
总结与建议



企业数据跨境安全合规至关重要

在全球化背景下，中国企业出海呈现多行业、多区域的特点。各行业如信息技术、金融科技、电商零售、医药生命科学、智能制造、汽车等企业积极拓展海外市场，面临发达国家与新兴国家不同的机遇与挑战。出海企业面临市场准入和政策法规、供应链及全球化运营等风险与挑战。

在企业出海过程中，数字化建设是关键手段，包括数字化平台建设、互联互通、供应链管理及全球运营等方面，能提升企业全球竞争力。数据跨境安全与合规至关重要，防止重要数据、健康数据泄露及软件供应链攻击等安全问题，数据安全问题关系企业声誉、经济利益及海外拓展。

除了遵循我国数据跨境合规要求，企业必须了解并遵守目标市场的数据保护法规。因各国数字经济发展水平和理念不同，跨境数据流动管理模式各异。美国虽无联邦统一数据与隐私安全保护立法，但有多个领域的法律及国际贸易协定来推动跨境数据流动；欧盟通过《通用数据保护条例》等建立个人数据跨境传输机制，与美国、英国的跨境数据流动规则不断演进；新加坡通过《个人数据保护法》等规范跨境数据流动，设立主管部门并与专业领域部门合作监管；日韩中目前亚洲仅有日本、韩国通过欧盟“充分性认定”程序，日本通过“补充规则”解决与欧盟差异，韩国修订法律对标 GDPR 要求。此外，还有国家采取强监管“本地化”模式，国际贸易协议中也有跨境数据流动要求。

根据《网络安全法》《数据安全法》《个人信息保护法》等法律法规，明确了数据出境的三条路径，依据网信办发布的《数据出境安全评估办法》《个人信息出境标准合同办法》以及全国信息安全标准化技术委员会发布的《个人信息跨境处理活动安全认证规范》。数据出境合规路径涉及不同程序和要求，安全评估具有法定强制性，未触发时可选择 “保护认证” 或 “标准合同” 。《促进和规范数据跨境流动规定》在促进数据自由流动与强化数据安全保护间建立平衡，规范了6类豁免情形。

作为数据跨境流动的前沿阵地，我国的自由贸易试验区在这一领域展开了积极的探索和实践，这些试验区不仅是连接国内外数据流动的桥梁，更是推动数据要素市场化、国际化的重要引擎。北京、上海、天津、粤港澳大湾区、海南、平潭等地自贸区发布相关地方性政策文件鼓励该区域的相关数据跨境流动工作开展。

建立“政市企”多层跨境服务机制

随着全球数字经济的快速发展，数据跨境流动变得日益普遍，但同时也带来了复杂的安全、合规、隐私保护等问题。单一监管主体很难全面应对这些多维度的问题，为了有效解决这一复杂局面，建立“政府、市场、企业”多层数据跨境安全服务机制是确保数据跨境流通的安全性、合规性与高效性的重要途径。将政府、市场和企业的角色有效结合，使数据在跨境过程中既能促进数字经济发展，又能够应对潜在的安全威胁和风险。

提升数据跨境服务效率

在数据跨境流通的背景下，建立多层监管机制有助于应对复杂的监管环境。政府监管机构在人力和技术资源上有限，尤其是在面对复杂的跨国数据流动时，完全依赖政府主管部门的监管会导致效率低下和资源过度消耗。通过政府、市场、企业的分工合作，能够在遵守国内法规的基础上更好地应对国际监管环境的复杂性，实现全球数据流通中的安全与合规。

多层监管机制将监管责任合理分配到市场和企业层面，减少政府的直接监管负担。例如，政府监管可以专注于关键信息基础设施、重要数据和敏感行业的数据跨境监管，而市场和企业可以承担一般数据的合规和技术保障工作。这不仅提高了监管效率，也有助于政府更好地集中精力处理高风险领域。

通过政府、市场、企业的相互协调，既能确保数据跨境流动的安全性，又能在一定程度上降低合规成本和市场混乱，推动数据跨境流通的健康发展。市场机制的介入为企业提供更多的选择和服务，减少企业应对复杂法规的成本，进而促进数字贸易的增长和创新。

同时，多层监管机制使得市场和企业可以通过技术创新和自律机制应对新兴的网络威胁和技术变化，如数据加密、匿名化处理、零知识证明等。市场力量可以为企业提供合规和安全服务，并激励企业通过技术手段来提升数据安全水平，从而与政府的法律法规形成互补。

此外，多层监管机制可以通过不同主体的协作来增强数据跨境流通的透明度和问责性。政府提供明确的法规框架，市场通过认证、审核和标准化手段确保透明性，企业则通过内部合规管理和风险控制机制提升问责性。

建立多方有效协作机制

不同类型数据和不同应用场景在跨境流动时所面临的风险是不同的。关键信息基础设施和重要数据的跨境风险远高于一

般数据的流通。多层监管机制通过区分不同类型的数据和场景，能更有效地进行风险管理。政府重点监管高风险数据，市场机制通过竞争和技术创新来管理低风险数据，企业在自身操作中负责具体的合规实践。这种分层次的监管模式能够根据数据的重要性和风险等级采取相应的措施，从而优化整体资源的分配。

政府监管：聚焦数据跨境高风险场景，促进数据跨境国际合作。

明确不同行业的数据跨境要求和合规标准，以减少政策模糊性。例如，对医疗、金融、通信等关键信息基础设施的跨境数据流动进行分类定义，明确哪些数据是重要数据，哪些数据可以自由流动。参与国际数据安全合作，推动数据跨境流通的双边或多边协议，确保各国之间的数据保护标准得到互认和协同。通过监督执法手段，确保企业在跨境数据流动时符合国家和国际的数据保护规定。

市场监管：发挥市场多维监管机制，提供灵活的数据跨境服务。

市场机制在跨境数据流通中起到补充作用，主要由行业自律、第三方服务商以及市场竞争来实现。

针对数据跨境细分场景，行业协会和行业联盟制定统一的行业标准来规范企业的数据跨境行为，降低企业合规成本，增强企业的可操作性和预见性。

第三方数据跨境服务机构可以提供专业的数据跨境合规审计和认证服务，核查企业的数据处理流程，帮助企业识别和管理数据跨境中的合规风险。第三方的介入不仅提高了市场的透明度，还能为企业提供明确的指引。

数据安全技术服务商通过提供专业的安全技术解决方案来应对数据跨境中的风险。这包括加密技术、数据匿名化、隐私计算等新兴技术的应用，以确保数据在跨境传输、存储以及开发利用过程中的安全性。企业可以选择使用经过市场验证的安全技术服务，确保符合安全标准的同时提升效率。

同时，竞争激烈的市场环境会推动企业主动寻求更高效、更安全的跨境数据解决方案，进而整体提升数据跨境的市场成熟度。

企业合规：完善跨境数据合规流程，做好数据跨境流动风险管理。

一是建立企业内部跨境数据合规流程，建立数据分级分类体系，将数据根据重要性进行区分，以便于在不同场景下采取相应的安全保护措施。

二是应用跨境数据保护技术。采用先进的数据保护技术，确保数据跨境过程中不被非法访问、篡改或泄露。例如，使用端到端加密技术保护传输中的数据，或者在数据传输前进行脱敏处理。

三是跨境数据流动风险管理。企业还需建立全面的跨境数据风险管理机制，评估并监控跨境数据的风险，及时采取应对措施。通过定期进行风险评估和演练，企业可以提高其应对突发安全事件的能力。

四是开展员工意识培训。企业需加强内部培训，确保员工了解数据跨境合规的重要性以及操作流程。通过定期的培训，员工可以及时掌握最新的政策和技术要求，从而减少因操作不当导致的合规风险。

建立“政府、市场、企业”多层数据跨境安全服务机制，关键在于明确各方职责、加强协作与联动，形成一个有机的、多层次的安全保障体系。政府加强重点监管和顶层设计，市场发挥灵活性和效率，企业则通过合规和技术手段确保实际操作的安全性。这种多维度的协同机制不仅能提升数据跨境流动的安全性和合规性，还能够促进数字经济的繁荣与发展。

建立数据跨境分类分级规则

目前，不同自贸区在数据跨境政策方面存在差异、缺乏配套的安全措施，这给数据的跨境便捷流动带来了挑战。为了应对这些挑战，建立统一的数据跨境典型场景分类分级规则显得尤为重要，这也有助于加强自贸区之间的合作和协调，共同应对数据跨境流动带来的挑战。

这需要对数据跨境流动的典型场景进行详细分类，如国际贸易、跨境运输、生物医药、跨国生产制造和市场营销等。这些场景涉及的数据类型和敏感程度各不相同，需要制定相应的分级规则，以确保数据在跨境流动中的安全性和合规性。基于相对统一的数据跨境分类分级规，可以对数据传输过程中的安全技术要求，如加密技术和匿名化处理等。这些技术的应用可以有效降低数据在跨境传输过程中的安全风险。

一是解决不同自贸区跨境政策之间的差异。以汽车数据为例，不同自贸区有一定差异并缺乏相应的安全机制支撑。在《中国（北京）自由贸易试验区数据出境管理清单（负面清单）》列举了OTA在线升级场景的各类重要数据字段，包括电控单元信息、固件配置信息、重编程相关数据、诊断仪数据、车辆钥匙相关数据等。但是，在《中国（上海）自由贸易试验区临港新片区》发布的《智能网联汽车领域数据跨境场景化一般数据清单（试行）》将售后场景的车辆信息、故障状态数据、诊断数据、售后订单数据、售后配件数据、售后跟踪数据作为一般数据进行管理。不同区域的政策差异可能会给企业带来混淆。

二是进一步明确跨境政策与行业规定之间的差异。例如，自贸区内的汽车数据处理者在识别重要数据过程中可能首先面临判断准据法的难题，因为《中国（北京）自由贸易试验区数据出境管理清单（负面清单）》规定的重要数据识别标准与《汽车数据安全管理若干规定（试行）》并不完全一致。负面清单中规定的重要数据识别标准范围更广、颗粒度更细，在一定程度上可以为汽车数据处理者开展重要数据识别给予更明确的指导。如果自贸区内的汽车数据处理者希望通过负面清单开展数据出境活动，可能仍需要优先参考负面清单的规定进行重要数据识别。针对自贸区外的汽车数据处理者，现阶段仍然优先适用《汽车数据安全管理若干规定（试行）》开展重要数据识别工作，定期完成年度汽车数据安全管理情况报送与重要数据风险评估。未来不排除行业主管部门以各自贸区负面清单为基础，根据其试行效果发布全国汽车行业重要数据识别目录的可能性。

针对大模型训练场景，北京自贸试验区数据出境负面清单中明确“在研发设计过程中收集和产生的与行业竞争力相关的高价值敏感数据”构成重要数据，因此，北京自贸试验区内具有行业竞争力的AI企业在AI产品出海时，如将有关模型部署于境外，则也可能构成重要数据出境从而需要履行安全评估义务。此外，实践中数据处理者直接向境外主体提供训练数据集、在境外服务器上训练人工智能模型、引入境外合作方开展数据标注或预处理、与境外主体合作开发优化或测试模型、或调用境外闭源大模型接口训练模型，均可能构成人工智能训练数据出境。

加快数据跨境基础设施建设

跨境基础设施

数据跨境基础设施的增强，如建设全球化的数据中心、国际网络骨干链路、统一的数据交换平台，能够降低跨境数据传输的成本，为企业提供稳定、快速、可靠的数据流通环境，支持全球化业务的高效运作。

通过优化跨境数据传输链路和节点布局，可以减少数据传输的延迟和丢包率，提升跨境数据的传输效率。例如，通过建设更多的国际数据中心、边缘计算节点、数据交换中心等基础设施，能够降低跨境数据传输中的时延问题。

设立专用的数据跨境传输网络，如建设专门的数据传输通道和海底光缆，确保跨国数据传输的安全性和稳定性，防止数据传输过程中被非法截获。加强基础设施建设可以通过技术手段增强数据传输的安全性，如加密技术、区块链技术、分布式存储等，确保数据在跨境传输和存储过程中的完整性和保密性。此外，强化防火墙、防御机制、入侵检测系统等技术基础设施，有助于减少数据跨境中的安全风险。

建立合规性的数据跨境基础设施，如合规的数据存储中心、数据流动审计系统、数据跨境流动审查工具等，有助于企业满足各国对数据跨境流动的合规要求。通过加强基础设施建设，企业可以更轻松地适应各国的法律规定，降低合规风险。

离岸数据中心

离岸数据中心作为“数据跨境流动的绿色通道”，对发展跨境数字贸易、促进中国企业出海、推动双循环等有着重要推动作用。

一般认为，离岸数据中心业务具有以下特点：服务场所，在特定区域内（具备“境内关外”特点）利用相应的机房设施；服务对象，只对境外用户（包括企业用户和个人用户）提供服务；服务提供企业，经营数据中心的企业以及入驻数据中心的企业可为外资，但必须在我国境内注册，并符合相关规定；服务内容信息，在保障国家安全的前提下，离岸数据中心内信息来去自由；网络连接，离岸数据中心网络在境内应与国内网络采取严格的物理隔离措施。

随着我国高水平对外开放的推进及数据安全法律法规的不断完善，海南、上海、广东、江苏以及辽宁大连等省市均在“十四五”相关规划中提出了探索建立离岸数据中心的计划。例如，上海市提出利用上海关口局及国际通信海缆等资源优势，在临港新片区开展离岸数据中心试点研究，并探索国际互联网访问监管新模式，推动“两头在外”数据的自由流动和高效服务，带动发展跨境电商、国际金融科技、离岸数据服务外包等关联业态，促进国际信息流量在临港新片区集聚和落地。海南省提出建设我国首个国际（离岸）数据中心，进一步吸引海外IDC业务向海南迁移；前沿部署国际互联网数据专用通

道、海缆登陆站、国际通信出入口局。2020年，海南（文昌）—香港海底光缆（H2HE）工程启动建设；中国移动获批建设文昌国际通信信道出入口局、海口区域性国际通信业务出入口局；三家基础电信运营商获批建设海南自由贸易港国际互联网数据专用通道。

2024年6月，海南省发布《海南自由贸易港国际数据中心发展条例（公开征求意见稿）》。征求意见稿指出，国际数据中心业务运营者可以面向境外提供游戏服务、北斗应用、跨境电商、跨境直播、远程医疗、远程教育、跨国生产制造等国际数据服务。征求意见稿一旦通过，将成为国内首个专门针对离岸数据中心的地方性法规文件，标志着我国的离岸数据中心将进入实质性落地阶段。

强化企业数据跨境安全措施

数据跨境安全典型场景包括数据跨境安全风险、数据出海合规场景、敏感数据流通场景、供应链安全场景和网络攻击防护场景等。其中涉及诸多风险和应对难点，包括跨境数据流通实施标准和落地措施不足、境外主体数据安全保障能力评估受限、评估成本高耗时长、境外主体申报难、大模型训练数据监管难度大以及其他如隐私泄露等多方面威胁。针对这些风险，在数据出海合规场景中，可通过深入了解和遵守法规、建立跨国数据保护框架、数据加密与保护、数据本地化策略和数据安全合规审计来应对；敏感数据流通场景可采取跨境数据加密传输、实时监测与响应、异常行为分析、多因素认证与访问控制、建立应急响应机制和员工培训等措施；供应链安全场景可建立供应商筛选机制、详尽合同条款、实施数据加密传输、定期审核、开展访问控制与监测、实施地理限制以及建立应急响应和通报机制；网络攻击防护场景可建立全面安全管理制度、强化技术防护措施、备份和恢复计划、DDoS 攻击防御、零日漏洞防护、内部安全控制和供应链安全管理。

为了应对这些挑战，企业需建立完善的数据风险监测与处置机制，利用先进的技术手段构建数据安全监管体系，及时处置安全威胁。通过实时监控和分析数据流动过程中的安全风险，企业能够更好地保护其数据资产和维护合规性。同时，企业应强化技术建设，构建坚固的数据跨境安全屏障。随着云计算和大数据技术的广泛应用，数据集中程度不断提高，这对数据安全提出了新的挑战。因此，企业需要选择合适的安全服务，保障数据在整个生命周期中的安全性。

建立数据安全管理体系至关重要。制定并执行严格的安全策略和流程，强化人员培训以提高数据安全意识，并采用先进的安全防护措施，如数据加密和身份验证。

参考资料

[1] 中华人民共和国网络安全法，全国人民代表大会常务委员会，2017年6月1日起施行

[2] 中华人民共和国数据安全法，全国人民代表大会常务委员会，2021年9月1日起施行

[3] 中华人民共和国个人信息保护法，全国人民代表大会常务委员会，2021年11月1日起施行

[4] 促进和规范数据跨境流动规定，国家互联网信息办公室，2024年3月22日发布

[5] 数据出境安全评估办法，国家互联网信息办公室2022年5月19日发布，2022年9月1日起施行

[6] 数据出境安全评估申报指南（第一版），国家互联网信息办公室，2022年08月31日发布

[7] 数据出境安全评估申报指南（第二版），国家互联网信息办公室，2024年3月22日发布

[8] 个人信息保护认证实施规则，国家互联网信息办公室，2022年11月18日发布

[9] 个人信息跨境处理活动安全认证规范（网络安全标准实践指南），全国信息安全标准化技术委员会，2022年6月24日发布。

[10] 个人信息跨境处理活动安全认证规范（网络安全标准实践指南）V2.0，全国信息安全标准化技术委员会，2022年12月16日发布

[11] 个人信息出境标准合同办法，国家互联网信息办公室，2023年2月22日发布，2023年6月1日起施行

[12] 个人信息出境标准合同备案指南（第一版），国家互联网信息办公室，2023年5月30日发布

[13] 粤港澳大湾区（内地、香港）个人信息跨境流动标准合同》，2023年12月13日发布

[14] 个人信息出境标准合同备案指南（第二版），国家互联网信息办公室，2024年3月22日发布

[15] 《国务院关于进一步优化外商投资环境 加大吸引外商投资力度的意见》（国发〔2023〕11号,2023年7月

[16] 中国（天津）自由贸易试验区数据出境管理清单（负面清单）（2024版）， 中国（天津）自由贸易试验区管理委员、天津市商务局，2024年5月8日

[17] 中国（上海）自由贸易试验区临港新片区数据跨境流动分类分级管理办法（试行），中国（上海）自由贸易试验区临港新片区管理委员会，2024年2月8日

[18] 中国（上海）自由贸易试验区临港新片区智能网联汽车领域数据跨境场景化一般数据清单（试行）（沪自贸临管委〔2024〕52号），中国（上海）自由贸易试验区临港新片区管理委员会，2024年5月16日

[19] 中国（上海）自由贸易试验区临港新片区公募基金领域数据跨境场景化一般数据清单（试行）（沪自贸临管委〔2024〕52号），中国（上海）自由贸易试验区临港新片区管理委员会，2024年5月16日

[20] 中国（上海）自由贸易试验区临港新片区生物医药领域数据跨境场景化一般数据清单（试行）（沪自贸临管委〔2024〕52号），中国（上海）自由贸易试验区临港新片区管理委员会，2024年5月16日

[21] 中国（北京）自由贸易试验区数据出境管理清单（负面清单）（2024版），北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局，2024年8月26日

[22] 中国（北京）自由贸易试验区数据出境负面清单管理办法（试行），北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局，2024年8月26日

[23] 欧盟《通用数据保护条例》（GDPR），2016年4月

[24] 美国《2018年加州消费者隐私法》（CCPA），2018年6月28日

[25] 全球数据安全倡议，外交部，2020年9月

[26] 中国关于全球数字治理有关问题的立场（就制定“全球数字契约”向联合国提交的意见），外交部，2023年10月

[27] 胡啸，中国数据跨境流动安全管理制度设计，中国网信杂志，2024年6月

[28] 许可，自由与安全:数据跨境流动的中国方案，环球法律评论,2021年第1期第43卷

[29] 范渊、刘博等，数据安全与隐私计算，电子工业出版社，2023

[30] 中资出海企业数字化发展（亚太）蓝皮报告（2024年），中国信息通信研究院产业与规划研究所，2024年8月

[31] 数字贸易发展与合作报告2023，国务院发展研究中心，2023年9月

中国信息协会
信息安全专业委员会

中国网络安全产业联盟
数据安全工作委员会