跨境数据流通
合规与技术应用白皮书
（2022 年）

开放群岛开源社区跨境数据流通小组

2022 年 12 月

版权声明

编制说明

本白皮书由开放群岛开源社区跨境数据流通小组牵头撰写，限于撰写组时间、知识局限等因素，内容恐有疏漏，烦请各位读者不吝指正。

本报告在撰写过程中得到了开放群岛开源社区跨境数据流通小组各成员单位的大力支持，在此特别感谢参编单位的各位专家以及深圳市北鹏前沿科技法律研究院王青兰博士。

❖ **编写单位**（排名不分先后）：

联易融数字科技集团有限公司、广东广和律师事务所、星环信息科技（上海）股份有限公司、大成律师事务所、浙江九鑫智能科技有限公司、深圳数据交易所、贵阳大数据交易所、粤港澳大湾区大数据研究院、华东江苏大数据交易中心股份有限公司、南方财经合规科技研究院、深圳前海微众银行股份有限公司、中国电子系统技术有限公司、勤达睿（中国）信息科技有限公司、顺丰科技有限公司、深圳顺丰泰森控股（集团）有限公司、深圳市雁联计算系统有限公司、北京八分量信息科技有限公司、天翼电子商务有限公司、北京东卫（成都）律师事务所、北京市百瑞律师事务所、大数据协同安全技术国家工程研究中心、北京市中伦（上海）律师事务所、野村综合研究所、广东卓建律师事务所、北京市天元律师事务所、哈佛大学医学院-数据实证实验室、泰和泰（深圳）律师事务所、北京市京师律师事务所、微言科技有限公司、北京市两高律师事务所、北京恒都律师事务所、广东北源律师事务所、大众汽车(安徽)有限公司

❖ **编写组主要成员**（排名不分先后）：

陈　曦	李如先	王　冠	叶玉婷
朱　琳	丁振赣	张　巍	黄念念
吕寒冰	春　煜	李　贺	李文塔
张雅婷	林俊龙	刘　媛	刘舒予
王　健	梁　云	王玢玥	王　腾
黄　煜	韩坤洁	康孝余	王建冬
刘钊因	李嘉瑜	李昌旺	龚　楠
陈　璐	樊晓娟	李智慧	刘　骥
郭宏清	于上卿	张建民	李兰兰
朱宣烨	邓　浩	易怀炯	洪瑞成
王岩飞	贺　伟	史楠迪	张明明
胡晓治	官中奇	张　茜	陈光涛
陈喜波	刘戍微	黄廉天	李家菁
杨晓晋	王柯程	陈晓文	胡君杏
周　博	钱勇喜	刘汪根	汤寒林
杨淋雨	谭　坤	王铀之	康仙鹏
李紫薇	戴　靖	梁艳芬	候天赐
李林兴	钟松然	杨　强	肖禹琛
褚华斌	胡姣姣		

前 言

数字经济时代，数字贸易是外向型数字经济的核心内容和重要载体，正成为国际贸易增长新引擎。数字贸易的繁荣，离不开跨境数据的安全有序流通。一方面，加速数字贸易的发展，需要让跨境数据自由便利地流通；另一方面，数据的跨境流通往往涉及到数据安全、个人隐私保护等问题。

2022 年 12 月 19 日国务院关于构建数据基础制度更好发挥数据要素作用的意见指出“深化开放合作，实现互利共赢。积极参与数据跨境流动国际规则制定，探索加入区域性国际数据跨境流动制度安排。推动数据跨境流动双边多边协商，推进建立互利互惠的规则等制度安排。鼓励探索数据跨境流动与合作的新途径新模式”。加强数据跨境流动的探索，成为我国在全球数字经济发展格局中建立优势的关键。

开放群岛（Open Islands）开源社区是由深圳数据交易所联合众多发起单位共同发起成立的中国首个致力于构建可信数据要素流通体系的开源社区，围绕技术开源协同、行业标准制定、数据要素场景落地等目标，开展隐私计算、大数据、区块链、人工智能等前沿技术探索和落地。联易融受邀牵头创建开放群岛（Open Islands）跨境数据流通小组，以助力企业合法合规实现数据跨境流通，业务出海为目标，围绕国内数据出境、国外数据入境及第三国数据过境等领域，联合生态伙伴结合业务模式与技术能力推进合法合规可落地技术解决方案。

自 2022 年 8 月 2 日成立以来，跨境数据流通小组举办了多项活动，组织召开数据跨境合规之数据出境安全评估研讨会，并组织行业专家探讨跨境数据流通合规与技术解决方案，此次的《跨境数据流通合规与技术应用白皮书》（以下简称“白皮书”）就是行业专家合作的智慧结晶。

白皮书以跨境数据流通线下合规与线上技术解决方案相结合为特色，在研究分析数据出境接受国或地区的法律环境和调研行业数据跨境实践的基础上，探索用技术手段实现跨境数据的高效流转，也是跨境数据流通技术解决方案的首次集中展示。

白皮书按照行业对跨境数据流通技术解决方案进行分类，选择跨境数据流通需求大的行业，如物流、金融、汽车、医疗、跨境电商等，以区块链、数据网关、隐私计算等技术，为高效又合规的跨境数据流通提供科技思路。白皮书基于对欧盟、美国、香港、澳门、日本、新加坡等数据接收国或地区法律的分析，为国内从事合规的从业人员提供相关素材的参考。

本次白皮书编写和成功发布离不开跨境数据流通小组各成员单位的支持，他

们在跨境数据方面拥有极具竞争力的技术优势和丰富的实践经验，为小组的良性发展带来多维度的支持，也为成员单位的相关跨境业务提供经验上的借鉴与帮助。冀未来更多合作，守正创新，为提升跨境数据流通效率，助推数据跨境流通基础设施，创造数字贸易发展新机遇贡献出力量。

目 录

图列表

第一章 背景介绍

1.1. 跨境数据流通需求与意义

在信息时代的大背景下，数据作为新兴资源要素得到了各国重视，我国《数据安全法》中，将“数据”定义为任何以电子或者其他方式对信息的记录。全球数据的跨境流通也愈发频繁，国际上对数据跨境概念的界定尚未形成统一的标准。我国在《数据出境安全评估办法》中，将数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息视为数据出境活动。

作为国际贸易发展的最新趋势，数字贸易在提升贸易效率、拓展贸易对象、降低贸易成本、丰富贸易业态等方面发挥着重要作用。跨境数据流通是推动人才流、物流、资金流和信息流跨域自由流转的基础，在促进经济增长、加速技术创新、推动企业全球化等方面发挥了积极作用。

数字经济的全球扩张已经使得跨境数据流通成为常态。数据要素能够赋能土地、劳动、资本等传统生产要素，对提高生产效率的乘数效应愈发凸显。当前，数据跨境流动也成为全球数字经济发展中各国数据博弈的核心。依托数字技术和信息网络推动数据跨境流动，可带动各类资源要素快捷流动、各类市场主体加速融合，帮助企业重构组织模式实现跨界发展，促进数字经济做强做优做大。

1.2. 我国跨境数据流通发展现状

近年来，我国已经发展成为数字贸易大国，积极构建海量数据。根据 IDC 的预测，我国的数据量在 2021-2025 年间平均增长速度为 30%左右，将成为全球数据量最大的国家。随着国际贸易和数字服务进出口规模的持续扩大，跨境流通的数据量持续增加，我国跨境数据流通呈现规模化、区域化的特点。

（1）完善数据跨境流通法律法规体系

我国积极完善数据安全保护及数据跨境流通法律法规体系，立法覆盖面逐渐扩展，初步形成较为完整的数据安全保护、个人信息保护和跨境数据依法有序流通的法律体系。《网络安全法》《数据安全法》等就数据出境作出了相关规定，构建起安全条件下促进数据自由有序高效流动的基本管理制度。2022 年 7 月发布的《数据出境安全评估办法》，就我国个人信息和重要数据出境安全审查评估等提出全面系统的要求、提供具体的法律解决方案，是我国破题数据跨境流动管理规则的重要实践。

（2）探索数据跨境流通实施路径

我国高度重视跨境数据流通工作，坚持数据安全流通和数字经济发展并重，

积极探索跨境数据流通的实施路径。2020 年 8 月，商务部发布的《全面深化服务贸易创新发展试点总体方案》中提出“开展数据跨境传输安全管理试点”，并要求在北京、天津、上海、广州、深圳等 28 个省市区进行试点。2022 年 1 月，国家发改委、商务部发布《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》提出，放宽跨境数据业务等相关领域市场准入，开展数据跨境传输(出境)安全管理试点，加速数据要素跨境市场建设。地方层面，全国各省市陆续颁布数据条例或数据条例草案，促进数据流通利用，激发市场主体活力。从中央到地方的实践探索，为促进跨境数据自由高效有序流动奠定了良好基础。

（3）提升数据跨境流通规则制定话语权

我国积极提升全球数据跨境流通规则制定话语权。2021 年 11 月，我国申请加入了《数字经济伙伴关系协定》（DEPA)。同年，我国就加入《全面与进步跨太平洋关系协定》（CPTPP）提出申请。在我国已经陆续加入的中韩自贸协定、区域全面经济伙伴关系协定（RCEP）中，关于数据跨境流通议题被各方广泛关注。积极开展多边框架下的国际数字贸易合作，有利于提升我国在数据跨境流通等关键议题的国际话语权。

（4）挖掘数据跨境流通场景应用与技术

全球数据量以 59%以上的年增长率快速增长，其中 80%是非结构化和半结构化数据，非结构化数据的利用率和可见度尚具有很大的挖掘空间。在跨境数据流通中数据正从“汇聚可用”向“链接可用”的技术路线发展。

1.3. 我国跨境数据流通实践存在的问题

（1）数据跨境界定不清晰

目前，对于数据跨境的界定在法律层面仍不够清晰，仅国家互联网办公室负责人就《数据出境安全评估办法》相关问题答记者问时提到，数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外。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、组织或者个人可以访问或者调用。但仍然无法明确某些具体场景下，数据处理活动是否构成数据出境活动，例如数据中转（data transit）、境外主体访问公开信息，以及境外主体委托境内主体加工处理数据后再传输出境的情形。对于数据跨境场景界定的不清晰，将陷入数据处理者无法准确识别自身合规义务、监管部门无法明确监管事项的困境。

（2）市场对于国家核心数据、重要数据的判定存在差异

当前国家核心数据、重要数据的识别标准模糊，导致部分跨境数据流通或交

易对于国家核心数据、重要数据的判定存在差异而造成违规或合规压力。如国家核心数据仅在《数据安全法》中有所提及，缺乏可执行的判定标准；帮助界定重要数据范围的国家标准仍然处于制定阶段，同样缺乏权威认定标准。一方面，这让部分数据处理者因未识别到国家核心数据、重要数据，故未履行出境前置程序，存在合规义务未履行的风险。另一方面，部分数据处理者所处理的数据虽安全级别较低，不属于国家核心数据、重要数据，但同样由于国家核心数据、重要数据识别标准模糊，数据处理者将无需进行安全评估的跨境数据事项向网信部门进行申报，造成了不必要的行政监管资源浪费及企业合规负担加重。

（3）数据出境业务开展成本高

《数据出境安全评估办法》规定在申报数据出境安全评估前，应当开展数据出境风险自评估。特别是在监管趋严的情况下，为确保数据依法依规跨境流通，尽快达到前述办法明确的合规要求，数据处理者通常自我施压，主动“加码”，来应对可能出现的风险，最终致使有数据跨境传输需求的数据处理者合规义务陡增。同时，由于当前标准化自评估体系还未完善，数据处理者通常需要委托有能力的第三方机构开展评估工作，或将在效率及可操作性层面造成相应损耗，增大数据出境业务开展成本。

（4）数据接收方的合规义务核查难

根据现行有效的法律法规等规范文件，对于数据出境链路及数据接收方的数据安全保障能力均有相应的要求，但在实际业务开展中，域外法律识别、政策法规和安全环境评价、接收方数据安全保障能力、数据处理全流程等事项均涉及域外核查，开展实地调研及核查存在一定难度及较高成本，企业落实存在一定困难。

（5）数据跨境安全义务评价标准缺失

对于拟通过数据出境安全评估路径传输数据出境的企业，需对自身及境外数据接收方的数据处理安全保障能力进行描述，但是对于应当采取何种类型的安全措施以及应当在数据跨境传输过程中部署哪些安全保障策略等问题，《数据出境安全评估办法》《数据出境安全评估申报指南（第一版）》等规范文件中均未明确。数据跨境安全义务评价标准的不可知，将使企业无法判定究竟应当从何种维度补充或加强自身在数据出境过程中的安全保障措施。如因安全义务履行瑕疵而无法通过数据出境安全评估，企业也难以获知需要弥补之处。

（6）个人信息出境标准合同适用范围过小

根据国家互联网信息办公室 2022 年 6 月 30 日发布的《个人信息出境标准合同规定（征求意见稿）》，如个人信息处理者处理个人信息超过 100 万人次，将无法适用该标准合同传输数据出境，但实践中众多小微企业经营跨境电商等业务时，都会处理超过 100 万人次的个人信息。对于这类主体，如只能适用数据出境

安全评估或通过个人信息保护认证的方式传输数据出境，将导致其承担与其业务规模不匹配的巨大合规成本。

（7）跨境数据流通技术水平和数据治理能力有待提升

我国跨境数据流通的需求正从事件与合规驱动向业务驱动演进，跨境数据流通在技术上需要性能稳定、简单易用的全链条平台工具释放阻力。跨境数据还存在数据壁垒突出、碎片化问题严重等瓶颈。现有结构性数据为主治理方式，在数据质量、数据字段丰富度、数据分布和数据实时性等维度还难以满足跨境领域AI 应用对数据的高质量要求。

第二章 数据跨境流通域外法律环境分析

数据跨境流通不仅需要考虑数据提供方所在国家或地区的法律，数据接收方所在国家或地区的法律同样会产生极大的影响。重视主要国家或地区的法律环境与要求，将有利于中国境内的数据处理者同相关国家或地区的数据处理者进行数据跨境业务建立基本法律认识，促进合法合规高效的业务交流与合作。

2.1. 香港

2.1.1. 抓住时代机遇，推动香港成为亚太区数据中心基地

香港特别行政区政府致力推广香港成为优越的资讯及通讯科技枢纽，并以发展数据中心为其重点之一。早在 2011 年 7 月 25 日，香港政府成立了数据中心促进组，专责推广和促进更多高端数据中心在香港发展[7]。《香港人权法案条例》、《香港特别行政区基本法》以及专门性法律《个人资料（私隐）条例》中，均涉及个人信息保护的相关规定。

2015 年，中国首次提出“信息丝绸之路”的概念。中国国家主席习近平在 2017 年举办的首届“一带一路”国际合作高峰论坛上提出：“我们要坚持创新驱动发展，加强在数字经济、人工智能、纳米技术、量子计算机等前沿领域合作，推动大数据、云计算、智慧城市建设，连接成 21 世纪的数字丝绸之路”。数字丝绸之路是数字经济发展和“一带一路”倡议的结合，是数字技术对“一带一路”倡议的支撑[8]。为从宏观角度探讨香港在为全球建设数码经济的数字丝绸之路倡议中的优势和定位，香港贸易发展局委托香港理工大学的 3 个研究中心，开展了专项顾问研究，并于 2019 年 10 月 2 日发布了研究报告《香港：数字丝绸之路之超级枢纽》[9]。前述研究报告对香港在数字丝绸之路的定位建议包括：云端数据中心/平台、数字国际金融中心、数字丝绸之路仲裁中心、智慧转口港和智慧城市。

2021 年 12 月，时任香港特别行政区行政长官林郑月娥女士在出席中国移动粤港澳大湾区香港火炭数据中心动土仪式发表演讲[10]，指出《十四五规划纲要》[11]支持香港建设国际创新科技中心，更好融入国家发展大局，深化香港与内地的科创合作关系，为我们发展数据中心服务提供更大的机遇……推动香港成亚太区数据中心基地。

在前述大背景下，数据跨境流动的法律环境成为香港充分利用其优势，实现定位的重要环节。

2.1.2. 香港数据保护及数据跨境的要点简析

（1）兼顾便利营商环境，维持香港之金融贸易中心地位和保障个人隐私

香港在数据安全和个人信息保护方面的立法框架主要包括《香港人权法案条例》《基本法》《个人资料（私隐）条例》，具体内容如下：

《香港人权法案条例》 1991 年，香港法例第 383 章《香港人权法案条例》出台（2017 年修订）。该条例将《公民权利和政治权利国际公约》中适用于香港的规定收纳入香港法律，并对附带及有关连的事项作出规定。该条例第二部第十四条比照《公民权利和政治权利国际公约》第十七条对私生活、家庭、住宅、通信、名誉及信用给予保护，规定“（一）任何人之私生活、家庭、住宅或通信，不得无理或非法侵扰，其名誉及信用，亦不得非法破坏。(二)对于此种侵扰或破坏，人人有受法律保护之权利。”
《基本法》 1997 年，《基本法》正式实施（后其附件经数次修订）。 《基本法》第三十九条确认“《公民权利和政治权利国际公约》《经济、社会与文化权利的国际公约》和《国际劳工公约》适用于香港的有关规定继续有效，通过香港特别行政区的法律予以实施。” 《基本法》第三十条规定：“香港居民的通讯自由和通讯秘密受法律的保护。除因公共安全和追查刑事犯罪的需要，由有关机关依照法律程序对通讯进行检查外，任何部门或个人不得以任何理由侵犯居民的通讯自由和通讯秘密。”
《个人资料（私隐）条例》（《私隐条例》） 1995 年，香港法律第 486 章《私隐条例》制定（1997 年至 2022 年期间经多次修订，现行有效版本日期是 2022 年 10 月 1 日），是亚洲最早确立个人资料全面保障的本地立法。 《私隐条例》共 12 部分及 6 个附表，涵盖个人资料私隐专员职位的设立、资料使用者申报登记、个人资料的查阅和登记、转移、使用、调查等等。《私隐条例》适用于包括政府在内的公营机构和私营机构。《私隐条例》旨在兼顾便利营商环境，维持香港之金融贸易中心地位和保障个人隐私。

（2）港股实名制：投资者识别码制度

2022 年 12 月 12 日，香港证券及期货事务监察委员会公布，香港证券市场的投资者识别码制度将于 2023 年 3 月 20 日推出。在该制度实施后，中介人须取得客户同意，以符合证监会的规定及相关的资料私隐法例。如投资者不提供所需同意，则只能出售已持有的证券，而不得在香港联合交易所有限公司（联交所）买入证券[12]。

（3）个人资料私隐专员

根据《私隐条例》第 5 条之规定，为《私隐条例》的实施，设立“个人资料私隐专员”（“专员”）职位。该职位由行政长官委任一人，任期为 5 年，至多连任一次。

个人资料私隐专员公署（“公署”）在专员领导下执行法定职能。根据《私隐条例》第 8 条之规定，“个人资料私隐专员”的职责及权力包括就遵守《私隐条例》条文作出监察及监管等。

（4）以《跨境资料转移指引》与建议合约条文范本为参考的跨境流通规则

香港的跨境个人信息保护的监管主要由私隐专员负责，并与海外的其他保障个人信息的机构合作处理跨境个人信息保障问题。关于个人信息跨境转移的规定主要见于《私隐条例》第 33 条，虽至今尚未实施，但在 2014 年 12 月 29 日，为推动和配合《私隐条例》第 33 条的生效，公署发出《保障个人资料：跨境资料转移指引》（《2014 指引》），并特别拟备了一份建议范本条文，协助机构制定与海外数据接收者订立的跨境数据转移协议[13]。《2014 指引》澄清《私隐条例》的适用范围：“是(i)将个人资料由香港转移至境外，及(ii)在两个其他司法区之间转移个人资料，但有关转移是由香港的数据用户所控制；但如果一个位于香港的个人或实体向同样位于香港的接收者传输资料，但互联网路由经过香港以外的地方，则不属于第 33 条调整的范畴”。2022 年 5 月，公署作出更新，发布了《跨境资料转移指引》（《指引》）与建议合约条文范本（《范本》）（详见附件 1.1.2）。该等指引和范本均属于自愿遵守性质。

2.1.3. 更为健全的制度框架，无实质性障碍的跨境流通

香港地区《个人资料（私隐）条例》的核心是 6 项信息保障原则，其中限制收集、限制利用和政策公开等原则都是为机构收集和使用个人信息的过程提供价值导向，与大陆地区《个人信息保护法》（以下简称《个保法》）在保护思路上有较高的一致性。

从制度体系看，香港地区的个人信息法律保障的制度框架更为健全，除了专门性的《个人资料（私隐）条例》外，对各行业、各领域的单独规定涉及《保险公司条例》《普查及统计条例》《金融资料统计条例》《领养条例》等多项条例，形成了兼具普遍性与适应性的制度体系。而大陆地区除了《个保法》《数据安全法》《网路安全法》《征信业管理条例》外，在医疗、工业、贸易、服务等领域的数据安全、个人信息保护立法相对不足，且正向支持数据要素流通的政策与法律衔接空白较大，未来需要持续建设。

根据中国大陆地区个人信息跨境的规则，企业完成个人信息保护影响评估、

履行用户告知义务、取得个人单独同意（或其他合法依据）后，再履行相应的安全评估申报、个人信息保护认证或与境外接收方签订标准合同等手续后，可跨境传输个人信息。从大陆与香港地区的个人信息保护思路、保护强度来看，香港地区数据接收方的合规程度一般满足要求，再结合粤港澳大湾区建设的总体背景，数据跨境不存在明显的实质性障碍。

2.2. 澳门

2.2.1. 完整的个人资料保护规范，但不完善的跨境规则

与中国大陆地区所采用的名称略有不同，“个人信息”在澳门特别行政区被称为“个人资料”（葡萄牙语 Dados Pessoais，英语 Personal Data）。澳门于 2005 年制定澳门特别行政区第 8/2005 号法律《个人资料保护法》（以下简称“个资法”），于 2019 年制定澳门特别行政区第 13/2019 号法律《网络安全法》，但至今澳门仍未制定有关数据安全领域的相关法律。

根据澳门特别行政区第 83/2007 号行政长官批示，澳门于 2007 年设立专门的执法机构——个人资料保护办公室（Gabinete para a Protecção de Dados Pessoais），在行政长官的监督下独立运作。个人资料保护办公室是澳门《民法典》第 79 条第 3 款[1]及《个资法》所指之公共当局，行使该等法律赋予的职权，包括但不限于：负责监察、协调《个资法》的遵守和执行，制定并监察保密制度的实施。

澳门对公民个人资料的保护源自于澳门《民法典》第 79 条[2]；澳门《个资法》的制定早中国大陆《个保法》16 年。由于历史的渊源，澳门保护公民个人资料的意识萌芽较早且较早地制定了完整的法律规范，但从实践层面上来看，澳门对公民个人资料跨境的规定不完善，并未形成类似于欧盟白名单的具体标准，而主要是依据个人资料保护办公室的判断决定。

2.2.2. 澳门数据保护及数据跨境的要点解析

（1）《个人资料保护法》关于个人信息保护的要点

澳门《个资法》的适用范围[3]包括以下三种情形： 1）一切自动化处理的个人资料和非自动化处理的个人资料；2）对可识别身份的人的声音和影像进行的

[1] 《澳门民法典》第 79 条第 3 款

[2] 《澳门民法典》第 79 条第 3 款：（个人资料之保护）一、任何人均有权知悉载于信息化之数据库或纪录内有关其本人之资料及该等资料之用途，并得要求就该等资料作出更正或更新；但关于司法保密方面另有特别规定者除外。二、收集个人资料以便作信息化处理时，应严格依照收集该等资料之目的而进行收集，并应让当事人知悉该等目的。三、为知悉关于第三人之个人资料而查阅信息化数据库及纪录，以及与信息化数据库及纪录连接，须就每一个案获得负责监察个人信息资料之收集、贮存及使用之公共当局之许可。

[3] 《澳门个人资料保护法》第 3 条

镜像监视，以及以其他方式对其进行的取得、处理和传播（只要负责处理资料的实体的住所在澳门，或通过在澳门设立的提供资讯或电信资讯网络服务的供应商而实施）；3）以公共安全为目的处理个人资料。《个资法》不适用于自然人在从事专属个人或家庭活动时对个人资料的处理。

负责实体在处理个人资料时，应注意区分个人资料与敏感资料。以透明的方式进行处理，遵守合法、善意、目的限定、适度、准确、限期保存等原则，保障资料当事人的资讯权、查阅权、反对权等相关权利。处理个人资料的正当性条件包括：1）当事人明确同意；2）执行合同或应当事人要求准备订立合同；3）履行法定义务；4）保障无能力作出同意的当事人的重大利益；5）执行公共利益任务或行使公权力；6）负责实体或被告知资料的第三人具有优先的正当利益[4]。

（2）接收方需达到同等保护水平

澳门对个人信息跨境的一般要求，主要规定于澳门《个资法》第 19 条、第 20 条及第 23 条。

一是适当保护程度。原则上，只有在遵守澳门《个资法》的规定且接收转移资料当地的法律体系能确保适当保护程度的情况下，才可将个人资料转移到特区以外的地方[5]。根据法律规定，资料接收地是否有适当保护程度由公共当局（即个人资料保护办公室）判断及决定。通常采用的方法，是根据互惠的原则把已经达到适当保护水平的国家/地区名单列入“白名单”。但直至目前为止，个人资料保护办公室未将任何国家或地区列入“白名单”。

二是发送通知。除上述原则外，存在以下例外情形。在通知个人资料保护办公室后，实体仍可转移个人资料：1）资料当事人明确同意转移；转移是执行资料当事人和负责实体间的合同所必需，或是应资料当事人要求执行制定合同的预先措施所必需；2）转移是执行或制定合同所必需，而该合同是为了资料当事人的利益由负责实体和第三人之间所订立或将要订立；3）转移是保护一重要的公共利益，或是在司法诉讼中宣告、行使或维护一权利所必需或法律所要求；4）转移是保护资料当事人的重大利益所必需；5）转移自作出公开登记后进行。根据法律或行政法规，该登记是为公众信息和可供一般公众或证明有正当利益的人公开查询之用，但需根据具体情况遵守上述法律或行政法规规定的查询条件。

三是申请许可。当转移不满足上述适当保护程度原则要求且不符合上述发送通知的例外情形规定时，实体在确保有足够保障他人私人生活、基本权利和自由的机制，尤其透过适当的合同条款确保该等权利行使的情况下，可向个人资料保护办公室申请许可，并在获得许可后转移个人资料。

四是无需许可。当个人资料的转移成为维护公共安全、预防犯罪、刑事侦查

[4] 《澳门个人资料保护法》第 6 条
[5] 《澳门个人资料保护法》第 19 条

和制止刑事违法行为以及保障公共卫生所必需的措施时，个人资料的转移如由专门法律或适用于特区的国际法文书及区际协定所规范，则无需向个人资料保护办公室[14]申请许可。

2.2.3. 注意敏感个人信息保护，避免行政处罚

中国大陆《个保法》与澳门《个资法》所规范的处理个人资料的原则大致相同，但《个保法》对某些定义作出了更明确的规定，对违法主体的处罚更严、罚款更高、处罚手段更多。

中国大陆《个保法》与澳门《个资法》，主要在以下方面有较大差异（具体法条比详见附件 2.1）：

（1）在处理敏感资料方面，两部法律有较明显的区别。在《个保法》中，敏感资料被称为“敏感个人信息”——即一旦泄露或非法使用，容易导致自然人的人格尊严受到侵害或人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及未满十四周岁未成年人的个人信息。而《个资法》则明确规定世界观或政治信仰、政治社团或工会关系、宗教信仰、私人生活、种族和民族本源、以及与健康及性生活有关的个人资料（包括遗传资料）等六种资料为敏感资料。由此可见，《个保法》所规范的敏感个人信息较《个资法》更广，且作出了更严格的保护。值得注意的是，《个保法》将未成年人个人信息归入敏感个人信息，加强了对未成年人个人信息保护的力度。

（2）在违法处罚方面，两部法律皆按违法情节的严重程度予以规定，但《个保法》的行政处罚更具威慑力，最高罚款额以违法主体的营收总额为基准，处罚力度远高于《个资法》的规定。且相较于《个资法》，《个保法》的处罚手段更全面，例如，没收违法所得、责令暂停相关业务、停业整顿、吊销业务许可或营业执照等。

当澳门个人信息出境到中国大陆时，在遵守《个资法》规定的同时，应注意遵守《个保法》对于公民个人信息保护之规定，避免被处以高额罚款。应特别注意，对于未成年人个人信息的保护力度，应符合中国大陆的相关法律规定。

2.3. 美国

2.3.1. 美国个人信息及数据法律环境分析

（1）由联邦立法、州立法及行业自律组成的“拼凑”特色

20 世纪 70 年代，公平信息实践(Fair Information Practices, FIP)初步确立美国

信息隐私保护框架并开始主导美国信息隐私保护实践。在美国立法体系中，数据保护框架包括数据隐私和数据安全，前者涉及个人信息的收集、使用和传播，后者涉及未经授权访问和使用个人信息[15]。

与欧盟统一立法模式不同，美国数据保护立法体系带有明显的“拼凑”特色，由联邦级立法、州级立法、行业自律准则三部分构成。美国尚未形成统一的联邦数据保护立法，但许多联邦、州的法律中均涉及隐私保护的相关法律条文[15]。

从联邦立法来看，美国数据保护法采取分行业式分散立法模式，集中于特定领域和特定对象。美国在电信、金融、健康、教育及儿童在线隐私等领域均有专门的数据保护立法，例如，金融领域的《格雷姆-里奇-比利雷法》(GLBA)、医疗健康领域的《健康保险可携性和责任法案》(HIPAA)、儿童在线隐私保护领域的《儿童在线隐私保护法》(COPPA)等。

从州立法来看，各州均在积极进行数据保护领域立法。其中，最为突出的是美国加利福尼亚州，形成了以 CCPA/CPRA 为代表的“美国标准”。2018 年 6 月 28 日，加州州长批准通过《加州消费者隐私法案》(California Consumer Privacy Act, CCPA)，创设了美国历史上最为严格且全面的数据隐私保护制度。2020 年 11 月 3 日，加州选民投票通过第 24 号提案《加州隐私权法案》(California Privacy Rights Act, CPRA)，该法案实质性修订了此前里程碑式的 CCPA，因此 CPRA 亦被称为 CCPA 2.0，已于 2023 年 1 月 1 日全面生效。美国加州的 CCPA/CPRA 与欧盟的《通用数据保护条例》(GDPR)也一并成为了当前全球最突出的数据保护立法，事实上的数据保护全球标准。

从行业自律准则来看，美国数字隐私行业自律准则的兴起与 20 世纪末美国政府提倡行业自我监管的政策息息相关。相对于政府管制，行业自我监管更具效率性和灵活性。在自我监管的理念下，通过“告知和选择”程序落实消费者信息保护，企业将隐私政策纳入服务合同供用户选择，除法律明确禁止或限制外，企业可自由收集、处理和分享从客户处获取的信息[15]。

不同于欧盟严格保护个人隐私的立法态度，美国对于数据保护的立法态度更多侧重于数据流通所带来的经济价值，以期通过促进数据跨境维护自身已建立的信息优势。

（2）由 FTC、CFPB、FCC、HHS 等组成的联邦数据保护执法机构

目前，美国有多个联邦机构负责数据保护执法工作，包括联邦贸易委员会(FTC)、消费者金融保护局(CFPB)、联邦通信委员会(FCC)、卫生与公众服务部(HHS)等。

在诸多联邦机构中，FTC 在制定美国隐私标准方面发挥了突出作用，通常被视为领导性的数据保护执法机构，有权对“不公平和欺骗性贸易行为”执法，同时

亦有权对儿童在线隐私和商业电子邮件营销等问题执法。近年来，FCC 亦发挥了突出的执法作用。

FTC 和 FCC 外的其他机构则是根据具体的法规或条例，负责相关的隐私执法工作，例如，卫生与公众服务部(HHS)的民权办公室根据《健康保险可携性和责任法案》(HIPAA)负责医疗隐私的执法；美联储和货币监理署根据《格雷姆-里奇-比利雷法》(GLBA)负责金融隐私的执法。

2.3.2. 美国数据保护及数据跨境的要点解析

（1）以 CCPA 和 CPRA 为代表的“美国标准”

如前所述，美国无统一的联邦数据保护立法，因此我们选取了美国在全球最具影响力的数据隐私立法，即最具代表性的“美国标准”CCPA 和 CPRA，并结合我国《个保法》的相关规定，对美国 CCPA 和 CPRA 数据保护的一般要求予以比对分析（详见附件 3.1）。

除已生效的 CCPA 和 CPRA 外，值得注意的是，2022 年 6 月 3 日，美国众议院和参议院商务委员会主要成员联合发布《美国数据隐私和保护法案》(American Data Privacy and Protection Act，ADPPA)（详见附件 3.2）草案文本，这是首份获得美国两党、两院支持的联邦综合性隐私保护法草案。ADPPA 草案的适用范围及被涵盖主体广泛，被涵盖主体包括受其他联邦法案约束的实体，其义务范围既反映州隐私法，也存在一些例外情况。ADPPA 草案成为法律仍有很长的路要走。如 ADPPA 草案正式通过，则美国将具备联邦层面的统一数据保护立法，并将广泛地取代此前聚焦于消费者的法律，例如，加州的 CCPA/CPRA，但 ADPPA 草案将保留未受影响的 CCPA/CPRA 法规下针对安全违规行为的私人诉讼权[16]。

（2）允许境外数据流入、限制境内数据流出

由于美国对于数据的态度是希望通过数据跨境活动维护自身的技术经济优势和所拥有的数据市场，发挥数据经济价值，占据全球领先地位。因此，在数据跨境方面，美国采取“允许境外数据流入、限制境内数据流出”的跨境数据流动政策体系。简而言之，美国对于数据跨境流动采取截然相反的两种态度——强监管数据向外流动，而允许数据自由向内流动。

最具代表性的“美国标准”CCPA 和 CPRA 均为州立法，故不涉及数据跨境传输。在数据跨境活动方面，美国直接相关的法案主要有：《澄清海外合法使用数据法案》(Clarifying Lawful Overseas Use of Data Act，CLOUD Act)、《出口管理条例》(Export Administration Regulations, EAR) 和《2019 国家安全和个人数据保护法案》(National Security and Personal Data Protection Act of 2019，NSPDPA)。

目前，CLOUD Act 和 EAR 均已生效，但 NSPDPA 尚未生效。

CLOUD Act 于 2018 年 3 月 23 日生效，最核心的内容是加强美国的长臂管辖，即，无论数据是否储存在美国境内，均允许美国联邦政府强制调取服务提供者的数据，否定以数据存储位置认定数据主权的判断标准，确立以服务提供者的控制权认定数据主权的新体系，扩大美国执法机关调取海外数据的权力。这意味着，任何在美国设有办事处或子公司的外国公司均须受 CLOUD Act 的约束。同时，其他国家若要调取存储在美国的数据，则必须通过美国“适格外国政府”的审查，需满足美国设定的人权、法治、数据自由流动标准[17]。

美国对于个人信息类型的数据跨境传输持开放态度，但对于其他重要数据则采取相应的限制，严格限制关键技术与特定领域的数据出口。EAR 严格限制部分关键技术与特定领域的数据出口，受管制的技术数据传输到位于美国境外的服务器保存或处理，需取得美国商务部产业与安全局(BIS)的出口许可。美国总统 2010 年签署的 13556 号行政令界定的“重要数据”范围，包括农业、受控技术信息、关键基础设施、应急管理、出口控制、金融、地理产品信息、信息系统漏洞信息、情报、国际协议、执法、核、隐私、采购与收购、专有商业信息、安全法案信息、统计、税收等 17 个门类[17]。

NSPDPA 则针对重要数据收集、使用、传输和存储制定了严格的规则。虽尚未生效，但仍须引起中国企业注意。NSPDPA 将中国、俄罗斯等国家列为“可能威胁美国国家安全的相关国家”，将提供跨州或跨国在线数据服务的、跟有关国家有实质关联的科技公司列为“相关科技公司”[17]。 NSPDPA 体现了美国对于我国以及我国企业重点关注及严格监管的态度，本质上是一场中美经济的角逐。NSPDPA 一旦生效，势必会对中美数据跨境活动进行更为严苛的规制，给我国企业带来更大的压力。

2.3.3. 美国与中国数据保护法律之对比

（1）中美跨境数据流动政策的核心差异与分歧

虽中美两国存在互利共赢的合作空间，但两国跨境数据流动政策的核心关注、政策基调和战略诉求依然存在根本差异，主要包括以下几个方面：

（2）以中国《个保法》为例对比美国数据保护立法

美国标准 CCPA 和 CPRA 是消费者保护领域的州立法，中国的《个保法》是统一的综合性数据保护法，存在诸多不同之处，例如：（1）中国《个保法》相较于美国 CCPA/CPRA，适用的地域范围、受保护的主体范围、受规制的实体类型、适用的数据活动等均更为广泛；（2）中国《个保法》与美国 CCPA/CPRA，在定义个人信息、敏感个人信息及分类、合法性基础范围、同意机制等规定中均

存在差异。（详见附件 3.1）

总体而言，美国与中国数据保护法律规定的不同亦体现两国对于数据保护的不同立法态度，中国的数据保护立法与欧盟的 GDPR 更为相似，重视保护数据主体的个人信息，美国则致力于加强美国在数字经济中的领先优势。

2.4. 欧盟

2.4.1. 棱镜事件推动的数据立法密集时代

2013 年美国棱镜事件加速了欧盟对数字经济时代数据跨境流动规则的重新审视，欧盟认为与美国签署并生效于 2000 年的《安全港协议》已无法充分发挥在双方数据跨境流动机制中保证欧洲公民数据隐私的效用，于 2015 年由欧盟法院裁定该协议无效并撤销；随后，欧洲委员会在 2016 年初与美国达成新协议——“欧盟-美国隐私护盾”（EU-SU Privacy Shield），开创欧美数据跨境流动新秩序，开启了欧盟数据立法的密集时代，同时也对世界其他国家和地区的数据保护机制产生了深刻影响，拉开了全球数据安全立法与治理热潮的帷幕。

2016 年，欧盟议会通过了 2016/679 号条例《通用数据保护条例》（GDPR），取代 95/46/EC 号指令（欧盟数据保护指令）。GDPR 于 2018 年 5 月 25 日正式生效实施，其制定了个人数据保护的一般要求，为个人的数据在处理和数据流动方面提供保护，对欧盟及各成员国的数据保护监管机制提出了更高的要求。
2018 年，欧洲议会和理事会正式发布了第 2018/1725 号条例《在欧盟机构、团体、办公室和机构处理个人数据方面保护自然人以及此类数据自由流动的条例》，提出欧盟机构、团体、办公室和机构在处理个人数据时需遵循的基本要求，并明确了数据主要监管机关的职能和义务。同年，第 2018/1807 号条例《欧盟非个人数据自由流动条例》发布，对非个人数据的跨境流动、监管目的下的数据跨境使用等方面提出具体规定，对成员国的数据本地化要求进行限制，并对国家机关获取数据、数据自由迁移等问题作出了规定，建立了欧盟内部数据跨境流动的基本规则，以积极推进欧盟融入全球数字经济发展大势。
2019 年，第 2019/1024 号条例《开放数据和公共部门信息再利用的条例》发布，对如地理空间、地球观测、环境、气象、统计、移动出行和公司所有权数据等可重用数据的开放提出要求，以推进该类数据的跨境使用，并指出欧盟成员国可通过 API 问数据。
2021 年，欧盟 25 个成员国与挪威和冰岛签署“欧洲数据网关”部长级宣言，旨在促进国际连通性、改善初创企业和大型企业监管环境、激励绿色数字技术

的推广。
2022 年，第 2022/868 号条例《欧洲数据治理和修订 2018/1724 号条例》（数据治理法案）发布，将于 2023 年 9 月 23 日起正式实施，目标是增加企业之间的数据共享，使更多公共部门数据可供重复使用，并促进个人数据的数据共享。建立一个由每个欧盟成员国代表组成的专家组，成立欧洲数据创新委员会保障法案的实施，以促进数据共享、充分释放数据潜力为目标，推动欧洲数字经济发展。

欧盟委员会计划在战略部门资助建立欧盟范围内共同的、可互操作的数据空间。通过组合必要的工具和基础设施，通过建立空间的共同规则来解决信任问题，这些空间旨在克服跨组织间数据共享的法律和技术障碍。

2.4.2. 欧盟数据保护及数据跨境的要点简析

欧盟 GDPR 将个人数据保护当成基本人权，GDPR 的规定覆盖了包括公私部门在内的各行各业的个人信息处理行为，且处罚额度可高达 2000 万欧元或年收入 4%，以及对全球违反 GDPR 行为的严厉执法力度，在全球范围内带来了深远的影响（详见附件 4.1），以下主要结合 GDPR 进行分析。

（1）独立数据保护机构 EDPB

GDPR 正式生效的同时，欧盟数据保护委员会（EDPB）也正式成立，总部位于布鲁塞尔，是欧盟的独立数据保护机构，负责发布关于 GDPR 核心概念解释的指南，并通过对有关跨境处理活动的争议做出具有约束力的决定来做出裁决，确保在整个欧盟范围内统一应用数据保护规则，并促进欧盟数据保护机构之间的合作，以应对欧盟众多成员国在不同主权下的政策制定、理解、执行一致性难题。EDPB 由欧盟各成员国数据保护机构（国家监督机构）的代表和欧洲数据保护监管机构（EDPS）组成，EDPS 作为 EDPB 秘书处为其提供分析、行政与后勤等支持。

（2）与欧盟同等保护水平下才被允许的个人数据跨境传输

欧盟将个人数据保护视为一项基本权利，一直坚持高标准保护个人数据。在消除境内数据自由流动壁垒、建立统一数据保护标准的同时，欧盟要求其他国家只有在提供与欧盟同等水平保护的情况下，才允许个人数据跨境向其进行传输。允许数据跨境的具体措施和要求包括：

基于充分性认定的白名单制度。欧盟委员会对欧盟以外国家或地区数据保护的充分性进行评估，将与欧盟保护水平相当的国家或地区列入“白名单”，允许欧盟个人数据向上述国家或地区传输。欧盟委员会对获得认定的国家和地区至少每四年进行一次评估，以确保其满足同等保护水平要求。

约束性公司规则（Binding Corporate Rules，BCR） 适用于在欧盟设立总部或分支机构的跨国公司，由跨国公司自行拟定内部机构之间数据传输和保护的规则，经欧盟成员国数据监管机构审核批准后生效。运行多年来，共有 100 多家跨国公司申请并获得通过。BCR 解决了跨国公司内部机构之间频繁传输数据的隐私保护问题，但同时也存在适用范围有限、实施成本高等弊端。
标准合同条款（Standard Contractual Clause，SCC）。SCC 是数据传输双方采用欧盟标准合同条款，通过将 GDPR 规定的义务转化为合同义务和责任，确保对数据主体权利的保护。2021 年 6 月欧盟委员会公布了两套标准合同文本，取代了之前的三个标准合同文本：一是将个人数据从欧盟转移到第三国的新标准合同文本；二是适用于欧盟境内的控制者与处理者之间的标准合同文本。SCC 为数据跨境流动提供了一个相对宽松且安全的解决方案，有助于促进数据跨境流动规则的融合与统一。
行为准则（Codes ofconduct，CoC）。CoC 是 GDPR 新引入的机制。当欧盟以外国家未获得充分性认定时，该国的数据控制者或处理者可作出具有约束力和可强制执行的承诺，承诺遵守经批准的行为准则，则欧盟数据可向其传输。目前欧盟委员会还未批准任何 CoC。

如果欧盟以外国家未达到欧盟数据保护水平，且仍未提供适当的保障措施时，GDPR 规定数据跨境的法定例外情形，包括：数据主体同意、履行合同义务、保护重要公共利益、保护数据主体及他人的重大利益、行使或抗辩法定请求权、公共注册登记机构数据传输等情形。

2.4.3. 对 GDPR 的借鉴与发展

欧盟对数据跨境流动规制采用“内松外严”的双重标准。对内积极推动成员间数据的自由流动，禁止内部以实施保护为由阻碍数据自由流通，即“内松”政策；对外实 施严格的监管政策，对于数据的流动需满足“充分性原则”的具体标准方可出境，即“外严”政策。对个人数据接收国要求具备与欧盟保护水平相当的条件，是否达到这一水平应由欧盟委员会审查决定。截止目前，欧盟委员会认定的充分数据保护的国家包括：安道尔、阿根廷、加拿大（商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士和乌拉圭、英国。目前不包括中国。

中国倡导全球数据安全，鼓励在保护个人信息权益，维护国家安全和社会公共利益的条件下，促进数据跨境安全、自由流动。对数据接受国或地区也采取的同等保护水平的要求。

欧盟 GDPR 的个人信息保护规定为中国制定《个保法》提供了借鉴意义，

同时，中国的《个保法》也规定了更为全面的个人主体权益如死者的个人信息保护权、跨境黑名单制度等规定，以促进个人信息的自由安全的流动与合理有效的利用，推动了数字经济的健康发展。

2.5. 日本

2.5.1. 相对灵活的数据自由流通政策

日本国内数据存量较小，在促进数据自由流通方面展现出较强的灵活性。日本数字产业相关政策以“国内立法及修法、签订双多边国际协议、推广全球理念”的思想作为推进路径。在政策制度层面，日本通过外汇和对外贸易法对数字产业相关的国际贸易与投资进行管理，包括对出口的数字产业货物与技术的“清单管制”、“全面管制”机制，对涉及数字产业的外商投资进行限制行业申请制度。从日本的现行政策情况来看，日本正在通过《经济安全保障推进法案》加强对关键产业的审查，包括对数字产业相关的重要基础设施、非公开化专利管理、先端技术官民合作等层面设置审查规则,这也对涉及数据流通的关键产业的外资准入产生了一定的影响。

日本跨境数据流动治理政策主要分为三个阶段：分别是 2001—2015 年跨境数据治理的理念与规划构想阶段，2016 年后的政策落实阶段，2019 年后的政策外推阶段[18]。2019 年 1 月，在达沃斯召开的世界经济论坛会议上，日本首次提出“基于信任的自由流通体系”（Data Free Flow with Trust，DFFT）倡议，并在大阪 G20 峰会上得到欧盟、美国和其他国家的支持和认可[19]。现阶段日本的数据要素跨境主要以“基于信任的数据自由流动体系（DFFT）”为核心理念，提倡在保护个人隐私基础上，打造共享、安全、互信的数据自由流动空间，促进医疗、工业和交通等领域数据自由流动[20]。整体来看，日本致力于推动本国数字治理方式与美欧数字治理兼容和对接，并积极参与多边、双边数据跨境协定，实现与欧盟 GDPR 完成数据保护“充分性”的相互认定，并推广构建“基于信任的自由流通体系”（DFFT），签署 CPTPP、RCEP、《日欧 EPA 协定》、《日美数字贸易协定》等相关协定。

以日本与欧洲的合作机制为例，2022 年 5 月 12 日第 28 次日欧定期首脑会谈中，划定隐私权、半导体供应链、数据流通、信任技术等重点数字优先合作领域。在隐私权强化技术和半导体供应链弹性方面日欧双方商定，交换关于联合监测和供应链预期断裂的信息，交流有效的预警机制，努力实现相关政府之间的出口管制协调；在数据流通方面日欧双方商定，在专家层面加深对市场驱动举措的理解，如欧盟数据管理法之类发挥信息中介机构的职能，以及日本的信息银行认

证制度等；在信任技术方面日欧双方商定，开展试点项目，实现行政、商务活动、电子商务中关键信任服务的相互操作性，为相互承认的长期目标铺平道路。

2.5.2. 日本数据保护及数据跨境的要点简析

（1）积极参与多边国际贸易协定协定

日本在贸易协定中设立数据跨境传输条款，实现与其他国家和地区的自由流动。日本于 2017 年 5 月《个人信息保护法》正式生效，并于 2020 年发布修订版，强化了关于数据跨境流动的细则条款，其中包括要求设立个人信息保护委员会作为数据跨境流通的监管机构，负责制定数据出境的规则和指南；个人数据处理者向境外传输个人数据的时候，需获得数据主体的同意后才可传输。同时，日本在《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《日欧经济伙伴关系协定》（EPA）以及正在谈判中的《区域全面经济伙伴关系协定》（RCEP）、中日韩 FTA、日英 FTA 等多边和双边国际贸易协定中增加关于跨境数据流动的规则，表明其规则理念和政策倾向。

（2）探索建立可信赖且自由的数据流动机制

在数据跨境流通方面，日本提出 DFFT，探索建立可信赖且自由的数据流动机制。同时，日本着力于多双边协定的缔结。DFFT 内涵包含数据的自由流通和安全流通两个维度，在确保隐私权、安保、知识产权相关的前提下，推动商务及有利于社会问题解决的数据在国际间自由流通；并以“拓展国际数据流通网”为目的，促进更多国家之间数字贸易规则的形成。2021 年 1 月，日本发布了《跨境数据流动指南》，进一步细化和完善跨境数据流动的相关规则和注意事项等。另外，日本还通过采取现代信息技术（如区块链、AI、5G 技术等）措施加强监管，确保跨境数据流动过程中的数据安全[21]。

2.5.3. 与在中国（不含港、澳、台地区）法律的对比

在数据安全方面，中国主要遵循的上位法包括《网络安全法》和《数据安全法》，其中对数据的跨境转移和数据本地化都作出了限制；日本主要遵循的上位法为《个人信息保护法》，无数据本地化存储限制，但在跨境转移方面规定需取得个人同意，妥善处理数据。其中，日本侧重对个人数据的跨境保护，要求处理个人数据的经营者数据跨境转移需要满足：“事先获得个人同意的情况下，处理个人信息的经营者可向国外第三方提供个人数据”、“向个人信息保护委员会白名单中所列国家第三方提供数据时可不经个人同意直接提供（白名单：欧盟、英国）”、“个人数据保护委员会有权对在日本处理个人数据的外国经营者行使处罚的权限，包括收集报告和现场检查。”中国对个人数据和公共数据的跨境均提出数据保护要求，对于关键信息基础设施运营者，数据跨境转移需要满足“应通过

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”的要求[22]。

在个人信息保护方面，中国主要遵循的上位法为《个保法》，对个人信息保护程度相对严厉；日本主要遵循的上位法为《个人信息保护法》和《个人信息保护法相关指南》，确立对个人信息权力保护的一体化监督机制。其中，对于个人信息的定义二者略有差别，中国认为个人信息为“以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息”，日本方面则定义个人信息为“包括能够识别特定个体的内容及符号。内容自身无法识别特定个体，但参照其他相关信息后能够识别特定个体的信息也被纳入范畴内。”中日均规定匿名化的数据不属于个人信息范畴，但日本特别提出，对于假名化的信息(即只要不与其他信息对照就无法识别出特定个体的信息)，在个人信息处理者内部使用时，可改变信息获取时的使用目的。

同时，中日在个人信息保护的细节上略有偏差：例如，在管理模式上，日本实行一体化监督机制，由内阁府下设的个人信息委员会负责，个人信息委员会将原本分散在政府各个部门的各个领域的监督权回收，集中到了新设立的个人信息委员会，从而确立了对个人信息权利保护的一体化监督机制；中国实行由国家网信办统筹、各行业主管部门协同的政府主导模式，由国家网信部门负责统筹协调个人信息保护工作和相关监督管理工作。在认证机构上，日本 1998 年开始导入由经济产业省下属的日本情报处理开发协会(JIPDEC)认证的“隐私标志制度”；中国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，如 CCRC 是 APP 个人信息安全领域的认证机构[22]。

2.6. 新加坡

2.6.1. 寻求加强监管与数据开放流动直接平衡的监管体系

新加坡数据跨境流动监管体系的重点包括设置主管部门、划分责任边界、设定跨境流动条件、开展国际协调和明确基础设施要求等方面内容。监管重点关注事前和事后两个阶段，事前监管主要通过制定规则的方式提出要求和进行引导，事后监管主要根据投诉和诉讼等情况进行监管和执法。同时，新加坡围绕个人数据保护出台了专门的法律法规，明确了个人数据的内涵以及与非个人数据的边界，并对个人数据保护的关键内容和责任主体进行了明确设置[23]。

2018 年，新加坡加入了亚太经合组织主导的 CBPR（Cross-Border Privacy Rule system，跨境隐私规则体系）和 APEC PRP（Privacy Recognition for Processors system，隐私识别处理体系），目前日本、韩国、加拿大、美国和墨西哥加入了该体系。根据 CBPR 的文件，加入亚太经合组织的 CBPR 体系要评估成员国当

前的隐私保护法、隐私保护执法机构、隐私信任认证机构、隐私法与 APEC 隐私框架的一致性。新加坡个人资料保护委员会因此开发一项与 CBPR 对接的认证机制，如果在新加坡经营的企业获得这一认证，即可以与 CBPR 成员国的认证企业自由传输数据。新加坡政府提出，开放的数据流动和高水平的数据保护相结合才是一种负责任的数据管理和流通方式[24]。

2.6.2. 新加坡数据保护及数据跨境的要点解析

（1）不限制数据入境，但对数据出境有要求

为了规制数据跨境流动，新加坡设立了专门的监管部门，并通过颁布一系列的法律法规进一步加强规范。

新加坡数据跨境流动的监管部门主要是个人数据保护委员会（Personal Data Protection Commission，PDPC）和信息通信部（MInistry of Communications and Information，MCI）下属的信息通信和媒体发展局（Infocomm Media Development Authority，IMDA）。其中，PDPC 主要负责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（涉及数据获取、使用、储存、传输和跨境转移的各类私人组织）建立完善的数据传输机制、审核机制以及相应的问责工具[25]。2012 年新加坡推出《个人数据保护法》（Personal Data Protection Act, PDPA），并历经 7 年的完善和修订于 2020 年颁布修正案，其相关法案、规章制度和附属规则多达 13 部，形成了新加坡数据跨境流动监管的法规基础。

对于不同的数据流动情形，PDPA 的监管要求不同，对于入境新加坡的数据，PDPA 不做特殊要求；对于仅在新加坡中转的数据，原则上不监管，但如果涉及数据交换，则要对负责数据交换的“桥公司”按照国内同等监管要求进行监管；对于由新加坡境内流向境外的数据，需要依据 PDPA 第 26 条要求进行监管[25]：

对于跨境传输的数据，组织或机构应当按法律规定制定个人数据保护标准，确保被传输的数据得到与新加坡法律同等程度的保护，否则不得传输至新加坡以外的国家或地区。
PDPC 可以根据机构的申请，以书面形式豁免机构数据跨境传输的相关合规义务。
PDPC 以书面形式对可豁免的情形进行说明，豁免不需要在《政府公报》中公布，并且 PDPC 可随时撤销。
PDPC 可以随时增加、改变或撤销豁免的具体适用情形。

另外，对于专业领域的数据流动，PDPC 会与各专业领域的主管部门合作，制定相关咨询指引。例如《电讯行业咨询指引》《房地产中介行业咨询指引》《教

育行业咨询指引》《医疗保健行业咨询指引》等。

（2）数据跨境流动的标杆示范城市

新加坡作为数据跨境流动的标杆示范城市，监管体制机制优势明显。新加坡通过实施“智慧国家”（Smart Nation）战略，推动其国内信息基础设施的现代化发展，扩大电信业的投资与推动数据中心的建设。建立完善的个人信息保护制度和相应的监管框架，监管体系重点包括设置主管部门、划分责任边界、设定跨境流动条件、开展国际协调、明确基础设施要求等方面。构建完善、系统的数据跨境流动管理规则，有助于实现全球数据向新加坡汇聚和流动，打造成为数据融合的重要中心节点城市。

在主要监管层面，PDPC 主要制定数据跨境流动和使用规则，要求企业建立有关数据保护的制度和机制。同时，还需要征得数据主体同意、符合必要原则 。和欧盟相似，新加坡也具有评估认证制度，PDPC 会对企业进行评估认证，对符合条件的企业授予“数据保护信任标识”，受认证的企业在数据使用和传输上能够享受更加便捷的监管要求。

（3）隐私增强技术沙盒

2022 年 7 月 20 日，新加坡资讯通信媒体发展局(IMDA)和个人资料保护委员会(PDPC)推出首个隐私增强技术（PET）沙盒，为企业提供试行隐私增强科技的安全环境。2022 年 11 月 2 日新加坡资讯通信媒体发展局(IMDA)官网显示，官方鼓励适用 PET 的公司参与 PET 沙盒。申请期限已延长至 2022 年 11 月 30 日。

Privacy Enhancing Technologies，简称 PET，指的是保护敏感数据隐私的科技方法。通过这项科技，采集、储存和管理数据的过程中能确保个人数据的安全性和机密性，同时允许企业从中提取有价值的信息。即允许企业在不暴露数据本身的情况下从数据中提取价值，从而保护个人数据和商业敏感信息。PET 增加了 B2B 数据协作的选项，支持跨境数据流动，并增加用于开发 AI 系统的数据的可用性。

随着隐私增强技术的成熟，企业已经在实际应用中配备隐私增强技术解决方案。因此，隐私增强技术沙盒将提供一个安全的环境和试验场所进行试点项目。这些试点项目将帮助企业确定合适的隐私增强技术，以实现其数据共享目标。

2.6.3. 建立以“相似保护”为基础的信任机制，以争取成为亚太地区数据中心

新加坡数据跨境流动态度相对开放，数据跨境流动成为新加坡境内流向境外贸易新优势的重要途径，新加坡也积极探寻成为全球数据跨境流动规则的重要影响者甚至是规则制定者。以“相似保护”为基础，新加坡重视交易中的信任机制，

以争取成为亚太地区数据中心。

根据 PDPC 要求，新加坡原则上不允许个人数据出境，但不包括在新加坡中转的数据。新加坡的《个人数据保护法案》（PDPA）规定，境外数据接收者应为所传输的个人数据提供与 PDPA 相称的保护标准，可以通过签订合同、制定公司规程、接收国数据保护立法等途径实现，并允许数据出境的其他法律理由，包括数据主体同意、履行合同义务必要、关乎生命健康的重大情形、公开的个人数据、数据中转等[26]。

新加坡在《个人数据保护法》（PDPA）与中国《个保法》也有许多的不同之处（详见附件 6.1）。比如 PDPA 规定保存 100 年以上的个人信息和去世十年以上者的个人信息在内的信息均不视作个人数据处理，但我国《个保法》第 49 条明确规定：“自然人死亡的，其近亲属为了自身的合法、正当利益，可以对死者的相关个人信息行使本章规定的查阅、复制、更正、删除等权利；死者生前另有安排的除外。”

2.7. 尊重区域差异，做好数据跨境合规

限于篇幅，我们无法全面的分析各国在数据保护及数据跨境的具体规定，只能粗浅的向各位读者展示部分国家和地区的法律要点，作为一个引子，以期让各位读者了解到不同国家和地区在数据保护及数据跨境法律环境方面是存在很大差异的，即使是最基础的处理个人信息前的告知同意，不同国家和地区的规定不尽相同。我们不能闭门造车，需要了解和吸收各国和地区优秀的经验。

其次，正因不同国家和地区关于数据保护和数据跨境的理念、规范乃至数据的基本定义有很大差异（比如欧盟谈及数据可能更多指向的是个人信息，而中国境内的数据还包含了除个人信息外的其他数据），相关主体在涉及到数据跨境业务时，需要尊重不同国家和地区的差异，除了使自己的业务符合本国和地区的法律法规外，还需符合境外接收方所在国家和地区对数据保护的要求。

最后，通过本章的对比分析我们发现，中国境内法律对于数据，尤其是个人信息的保护力度在世界范围内也是较强的一档，我们在对境外的法律法规吸收借鉴的同时，也有属于自己的发展，走出属于中国自己的数据保护道路。对于境内的数据处理者，在面临数据跨境业务时，需要向数据的境外接收方强调提升其保护水平，以达到与境内同等的保护水平，保障数据的安全、合规。

第三章 跨境数据流通技术解决方案

《数据出境安全评估办法》指出，企业牵涉到数据出境且数据规模、数据敏感性达到一定程度时需要进行安全风险自评估。我国要求数据处理者具备数据安全管理能力和数据安全技术能力，如下表所示。并要求数据处理者在处理数据的全流程中，应以相应的技术为支撑，以合规要求为保障，为数据跨境流通保驾护航。本章对跨境数据流通技术解决方案按照行业进行分类，以区块链、隐私计算、数据网关等技术，为高效又合规的跨境数据流通提供科技思路。

表：《数据出境安全评估办法》部分条款与技术对照表

《数据出境安全评估办法》条款	**关键词**	**相关技术**
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	目标、范围、方式	/
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	数量、范围、种类、敏感程度、风险	数据分类分级
境外接收方承诺承担对责任义务，以及履行责任义务对管理和技术措施、能力等能否保障出境数据对安全	接收方承诺、管理和技术	所有可以保障网络安全、数据安全的技术
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、非法利用等风险，个人信息权益维护的渠道是否通畅等	个人信息权益维护通道	去标识化、隐私计算、数据水印、区块链存证
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	争议解决条款	/
其他可能影响数据出境安全	可能事项	/

3.1. 卫生健康：区块链助力粤澳健康码跨境互认

新冠肺炎疫情让社会治理体系面临前所未见的考验，如何兼顾疫情防控与复工复产成为社会各界共同努力的目标。区块链技术作为传递信任的新一代信息基础设施，为粤澳两地的疫情精准防控和加速复工复产提供有力的技术支撑。在此

背景下，微众银行积极履行自身社会责任，运用基于区块链的实体身份标识及可验证数字凭证技术，为粤澳健康码跨境互认系统提供了区块链开源技术支持，助力两地居民正常跨境通关。

3.1.1. 案例实施背景

（1）业务挑战

“粤康码”与“澳门健康码”跨境互认的过程中，涉及两大难题。首先，是健康码生成、使用过程中的用户信息安全和隐私保护问题，其安全隐私标准应符合两地各自用户隐私保护的相关法规要求；其次，由于居民的个人信息及核酸检测信息等只有本地权威机构有能力验证，而澳门和内地相关机构需在用户数据不直接传输和交换的前提下，验证用户提交信息的真实有效性，搭建跨地区的数据真实性核验通道。

（2）应用场景与需求

实现人群健康数据流通的一个重要前提，是建立人群健康身份的识别机制，并促成健康身份信息在机构和各地区之间的互认互通。区块链凭借与生俱来的技术优势，可以将健康码相关信息转化为加密的可验证数字凭证，两地机构在不直接传输和交换用户数据的情况下依然可以验证信息的真实有效性。当用户需要跨境验证健康码时，不需要在多个平台重复填写信息，系统在获得授权后将自动为用户转码，满足了各地不同的隐私保护条例。

3.1.2. 案例方案介绍

（1）解决方案思路

微众银行为项目提供 FISCO BCOS 区块链底层开源平台、WeIdentity 实体身份认证及可信数据交换开源解决方案支持，通过分布式实体身份标识及管理、可信数据交换协议等一系列的基础层与应用接口，充分保障实体对象（人或物）数据的安全授权与交换。为配合粤澳两地建立的跨境互认机制，澳门健康码的运作机构及粤康码的运作机构都各自注册了 WeIdentity DID（WeIdentity 方案中的术语，为每个实体在区块链上生成符合国际规范 DID 的全球唯一 ID）。

（2）系统架构与功能模块

跨境数据互认机制的流程如图 3.1-1 所示，详细流程如下：

1) 用户首先要符合转码的条件，然后申请粤康码转换澳门健康码，下载加密后的 Credential 到手机客户端，包括用户自己的个人资料，健康码颜色，及核酸检测结果等；
2) 粤康码后台将用户的粤康码信息生成 Credential 并加密，同时使用私钥签名，将哈希上链；

3) 用户自主提交，将粤康码的加密的 Credential 传送到澳门健康码；
4) 澳门健康码后台解密用户提交的信息，与链上哈希比对，验证信息和签名；
5) 当验证通过，为用户生成澳门健康码；
6) 用户在手机上接收到生成的澳门健康码，持有并可以入境澳门；
7) 当持有澳门健康码（包含核酸检测结果）的澳门市民及内地居民，可以直接使用自助通道入境澳门。

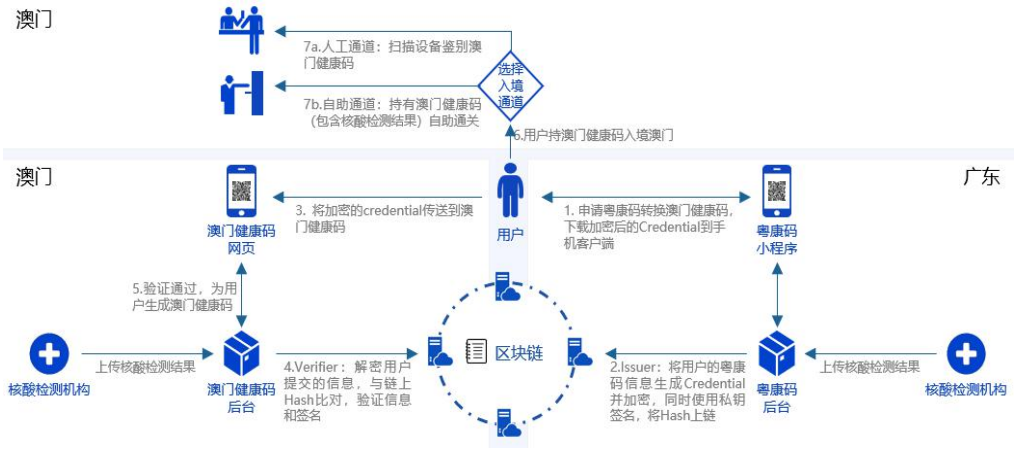

图 3.1-1 跨境数据互认机制的流程图(粤转澳)

跨境数据互认机制的流程如图 3.1-2 所示，详细流程如下:

1) 用户首先要符合转码的条件，然后申请澳门健康码转换粤康码，下载加密后的 Credential 到手机客户端，包括用户自己的个人资料，健康码颜色，及核酸检测结果等；
2) 澳门健康码后台将用户的澳门健康码信息生成 Credential 并加密，同时使用私钥签名，将哈希上链；
3) 用户自主提交，将澳门健康码的加密的 Credential 传送到粤康码；
4) 粤康码后台解密用户提交的信息，与链上哈希比对，验证信息和签名；
5) 当验证通过，为用户生成粤康码通关凭证；
6) 用户在手机上接收到生成的粤康码通关凭证，持有并可以入境广东省；
7) 持有粤康码通关凭证的澳门市民及内地居民，可以选择使用自助信道或人工信道入境广东省。

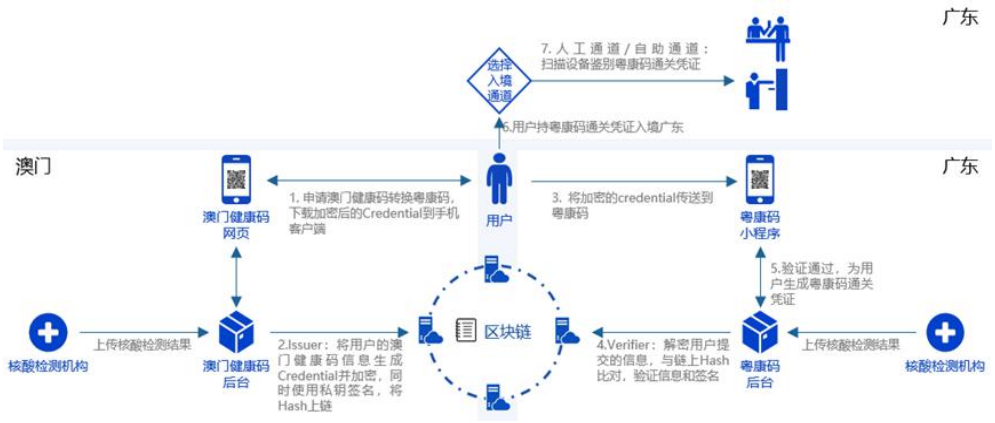

图 3.1-2 跨境数据互认机制的流程图(澳转粤)

流程中的跨系统数据交换模块的方案采用使用 Credential〔WeIdentity 方案中的术语，将物理世界中的纸质证明文件电子化，并利用区块链不可篡改的特性，将原始数据的 Hash 上链，并附上权威机构 Issuer 的签名，确保数据不可伪造，可验证权威性）作为申报信息的载体，服务端将加密后的 credential 传送给客户端，由客户端转发给对方（广东）。Credential 的哈希值会存入 FISCO BCOS 中作为存证之用。

（3）方案创新点

方案利用区块链技术优势，既能实现健康码跨境互认，支持两地居民往来互通，又确保符合隐私保护等相关法律法规要求，不会造成数据跨境传输等安全合规问题；通过分布式数字身份和可验证数字凭证技术，两地机构在不直接传输和交换用户数据的情况下依然可以验证信息的真实有效性。

方案让用户成为关键参与者，由用户主动发起个人信息数据传输并自行上传，从而实践个人数据可携带权。这种由用户个人自主驱动的数据提交和核验机制，确保在符合隐私保护等相关法律法规要求的前提下，实现了数据在用户知情、授权和主导下的跨地区流通。

3.1.3. 应用效果

粤澳健康码跨境互认系统在支持粤澳两地人员的正常流动和经济社会交流恢复中发挥了关键作用，推动了粤澳防疫数据互信互认，助力粤澳两地居民恢复正常往来和加速复工复产。

2020 年 5 月起，“粤康码”与“澳门健康码”互认系统正式启用。同年 7 月 15 日，两地居民通关可免除 14 天医学观察期。目前，持健康码通关凭证通关人员已累计超 2 亿人次。

该跨境互通互认机制还被写入 2021 年出版的《中国共产党简史》。

3.2. 跨境供应链金融：基于区块链的数字化跨境贸易和融资平台

联易融基于区块链的数字化跨境贸易和融资平台（以下简称“平台”），主要面向的用户是供应链条上的核心企业、服务于这部分核心企业的金融机构，以及相关的政府平台、物流机构、第三方支付机构、海外供应链服务平台等生态机构。

平台引入区块链技术，从贸易流程中的订单、发票、物流、库存等信息到贸易融资中的资产信息及多机构审核信息进行上链，实现全流程防篡改、透明化，将供应商的交易场景和融资场景无缝对接，打造一站式跨境贸易和金融服务平台，为中小企业提供跨境贸易和金融服务。

3.2.1. 业务痛点

（1）跨境贸易涉及多方，交互都为线下交互，信息流不对称

跨境贸易由于其业务复杂性，一笔交易涉及到的交易方包括工厂、卖方、船公司、物流机构、报关行、海关、检验机构、保险公司等各个主体，目前各主体直接的交互都为线下交互，信息流无法及时同步导致效率低下。

（2）跨境贸易单据都为纸质单据，处理和审核的成本较高

跨境贸易各主体信息化程度参差不齐，目前涉及到的跨境贸易单据比如订单、发票、提单、检验单等都为纸质单据，企业之间结算需要寄送单据时间较长，影响了企业结算效率。同时银行也要处理大量的纸质单据，审核效率较低，而且操作和运营风险高。

（3）跨境贸易核心企业应付账款管理效率低下

上述提到的跨境贸易数字化程度较低以及单据都为纸质化单据，对于核心企业来讲，要与自身数字化战略相融合的成本较高。而且由于整个流程线下完成，供应链透明度低，供应商管理水平较低，因此相关的流动资金解决方案也很难惠及核心企业。

（4）跨境贸易中小企业面临融资难，融资贵的问题

从事跨境贸易的中小企业大多为贸易型企业，不符合传统银行授信要求，加之跨境业务的复杂性，银行流动资金贷款很难满足。同时如果是在核心企业深层次供应链条上的中小企业，也无法借力与核心企业的交易关系获取融资。跨境贸易中小企业普遍面临融资难问题，只能转向保理公司小贷公司等 成本较高的资金渠道寻求资金支持。

3.2.2. 案例方案介绍

（1）平台的整体思路

通过与海外 B2B 平台以及其他跨境参与方的数据交互和流程整合，基于大数据、AI 和区块链等先进技术，实现以下内容：

1) 平台整合贸易生态系统各合作伙伴交易数据，实现跨境贸易数字化，还可延伸到不同贸易方之间的电子化单据交互；实现数据溯源可控，方便跨境贸易的生态系统参与方可随时追踪货物情况，在线管理跨境供应链流程，确保贸易真实性；

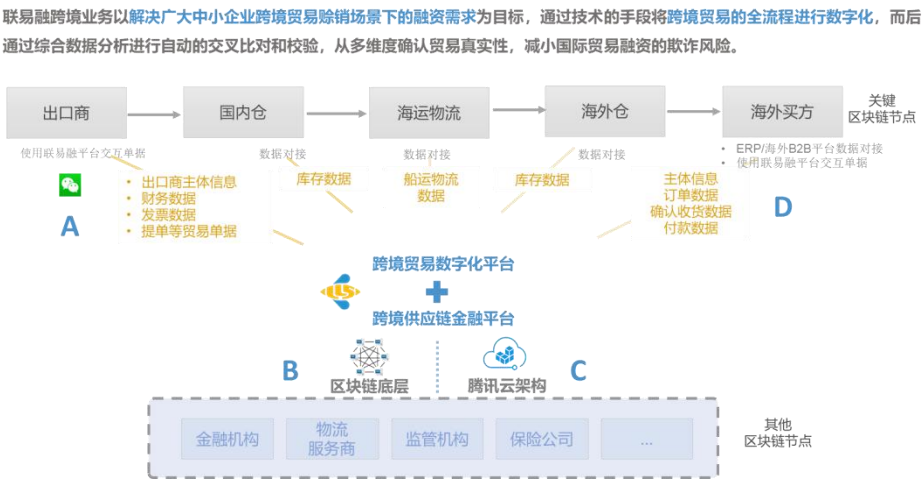

图 3.2-1 基于区块链平台的数字化跨境贸易平台概览图

2) 基于数字化的跨境贸易流程，平台打造了数据风控引擎，为中小企业授信。追踪还原贸易流程，核实贸易真实性，解决债项审核困难，贸易真实性难以确认的问题；实现多方共同维护共享账本、互信互认、精准控制授信额度。

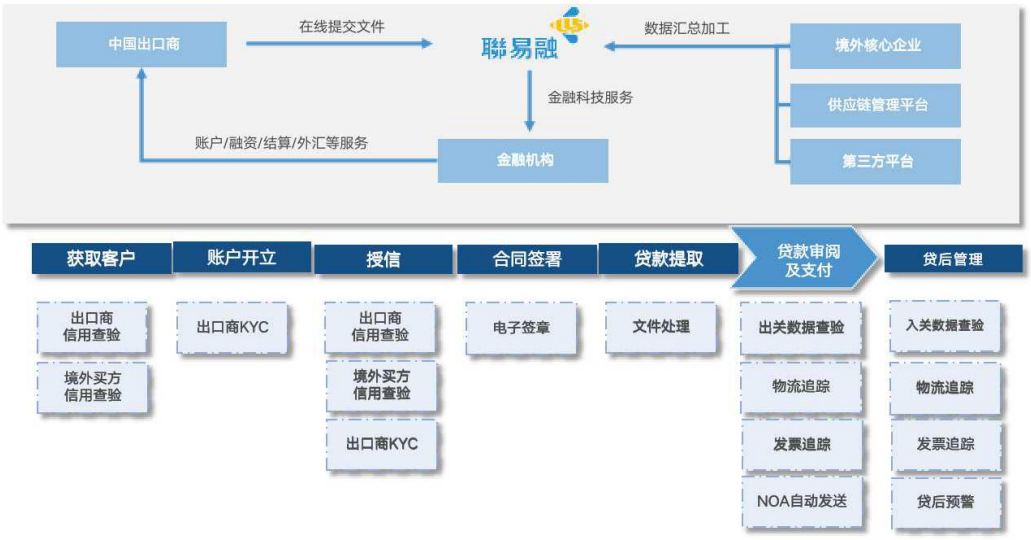

图 3.2-2 数字化跨境融资平台关键数据

（2）平台的业务流程

1) 数字化跨境贸易平台业务流程

以最典型和核心企业与供应商之间交互为例，联易融跨境贸易数字化平台可通过 API 或者 H2H 方式直连核心企业的 ERP 或者内部订单系统或者 OA 审批系统，实现订单在线同步，审批流，对账在线同步，并支持供应商在线订单管理，同时所有同步的数据及交易状态通过转化为可验证文档数据，并在用户侧签名后使用 BeeTrust 的文档智能合约进行上链，进行电子文档存证。

2) 数字化跨境贸易融资平台业务流程

海外供应链管理平台上的中小企业可以在完成与买方的日常供应链流程交互后，在供应链管理平台一键发起融资申请，供应链管理平台通过与联易融区块链的数据对接，把交易对应的支持文件（订单、发票、承兑通知等）全部记录在区块链上，并向联易融发送融资申请。联易融收到融资申请，通过区块链数据、大数据、AI 方式审核单据无误后即可操作付款，中小企业平均收款时限为提起融资申请内 2 小时即可到账。

（3）平台的创新亮点

1) 模式创新：平台整合了跨境贸易交付过程中的多环节信息，实现了跨境贸易单据数字化，更进一步推动了跨境贸易全流程的线上化；
2) 获客创新：可批量准入中小出口企业，提高入驻和融资效率；
3) 流程创新：无缝衔接中小企业的交易和融资场景；
4) 产品创新：相比市场上其他传统银行融资和保理融资产品，融资节点提前，更进一步满足中小企业实际的融资需求；
5) 科技创新：运用区块链技术将贸易流程透明化可视化，解决了之前交易流程因为人工效率低而无法动态掌握的难题；
6) 风控创新：独创平台+买方准入+卖方数据风控+流程管控的新型贸易融资风控思路，从根本上降低贸易融资的主体风险和债项风险。

3.2.3. 案例应用成效

（1）支持了大湾区和全国的中小出口企业

项目上线以来，为中小企业融资规模约为 42 亿人民币，服务中小企业 180 多户，覆盖的国家和地区包括：粤港澳大湾区城市 62%，中国内地其他城市 22%，以及越南，泰国，孟加拉等中国出口商产业外移国家 16%。使用区块链技术使得融资机构核验贸易真实性，提供线上授信的时间大大缩短，帮助中小企业将授信时间从市场平均 1-3 个月提高到 1 周，提款时间由市场平均 1-2 天提高到 2 小时之内。该项目支持外贸出口实体经济的同时，也利用创新型的跨境金融服务，加强了深港市场联动，促进跨境供应链金融市场的创新发展。

（2）媒体和相关奖项

项目开创了与海外互联互通的创新供应链融资模式，也荣获 2019 年亚洲财资服务奖，该奖项为财资领域全球知名奖项，历届获奖机构皆为知名金融机构。在 2020 年 10 月份香港金管局举办的金融科技周上，获得了初创企业金奖项目称号。同时在 2020 年深圳前海优秀金融创新案例评选中荣获跨境业务唯一奖项。此外，此案例也应用在深圳-新加坡智慧城市项目中。

3.3. 跨境金融：区块链助力粤澳跨境数据验证

针对实现数据关键生产要素便捷跨境流通，助力粤港澳大湾区一体化发展的重要命题，区块链技术与分布式数据传输协议(DDTP)的结合应用提供了较佳的解决方案。微众银行基于助力“粤澳健康码跨境互认”的成功实践及区块链技术领域的沉淀，与合作伙伴共同推进“粤澳跨境数据验证平台”建设，探索跨境数据领域的新模式。

3.3.1. 案例背景

（1）数据互联互通是促进高水平跨境合作的必要前提

随着数字经济的深化发展，数据要素在中央文件中被列为五大关键生产要素之一，国家层面也密集出台了相应政策鼓励数据要素流通。国务院印发《“十四五”数字经济发展规划》，对数据要素作出专章部署，提出强化高质量数据要素供给、加快数据要素市场化流通、创新数据要素开发利用机制等重点任务举措。立足于深化大湾区一体化融合的发展格局，实现跨境数据的互联互通是促进高水平跨境合作的必要前提。

（2）大湾区融合发展亟需可信数字基础设施

粤港澳大湾区在“一国两制三法域”的背景下，三地监管存在显著差异，机构间直接跨境传输个人数据门槛较高，过去也缺乏可信的数字基础设施支持协同创新。同时，当前跨境资料一般通过线下临柜面对面、邮寄信函材料等传统方式进行，不但居民往来操作繁琐、效率低下，而且存在信息篡改、隐私泄露的风险，难以满足日益增多的跨境业务需要，也不利于大湾区互融互通。

（3）技术与方案沉淀推进平台建设

平台具体由横琴粤澳深度合作区金融发展局和澳门科学技术发展基金分别作为粤澳两地政府指导单位，珠海华发金融科技研究院有限公司及深圳联合金融控股有限公司作为横琴侧运营方，南光（集团）有限公司作为澳门侧运营方、万高信息科技有限公司作为平台技术供应方，微众银行为方案设计及区块链开源技

术支持方。

3.3.2. 技术方案

（1）方案思路

在粤澳跨境数据验证平台中，用户成为个人信息数据传输的核心——基于个人数据可携带权，用户从数据提供者处下载个人信息数据，并自主传输数据至数据接收者，同时对使用范围和使用目的等进行授权，平台并不传输或存储任何敏感个人数据。用户下载数据的同时，数据提供者将下载的文件或是数据独有的哈希值（由源文件计算而来的一串字符串或数据凭证，可以理解为“数据的指纹”）存储到粤澳跨境数据验证平台的区块链上。数据接收方接到用户提交的数据后，通过同样的算法验证哈希值的一致性，以确保数据未被篡改、真实有效。这样既符合政策合规要求，又能解决跨机构、跨行业、跨场景数据协同生产的问题。

（2）方案流程实现

平台方案的客户端服务由场景机构提供，以下内容仅做示意，落地实现以场景机构实践为准。

图 3.3-1 粤澳跨境数据验证实现流程图

如图 3.3-1 所示，数据流向为自澳门传递至横琴（反向亦可）：数据凭证由客户在应用端中，完成身份识别(左 1)后，选择跨境服务项（左 2）。客户向数据发出机构授权（左 3）提取该用户凭证的数据，用户将凭证下载储存至手机本地（左 4）。用户通过澳门应用端的引导跳转至横琴应用，从手机本地上传数据凭证（右 2），完成操作（右 1）。

（3）验证技术说明

平台的核心功能是向场景机构提供数据凭证的可信验证服务。验证流程为场景机构中的数据发出方将用户的数据凭证处理为“数据指纹”(不可逆的、唯一

的哈希值字符串符)存证于平台上，场景机构中的数据使用方将收到的数据凭证做同样的“数据指纹”处理，与平台中已存证内容比对一致即验证数据凭证可信。

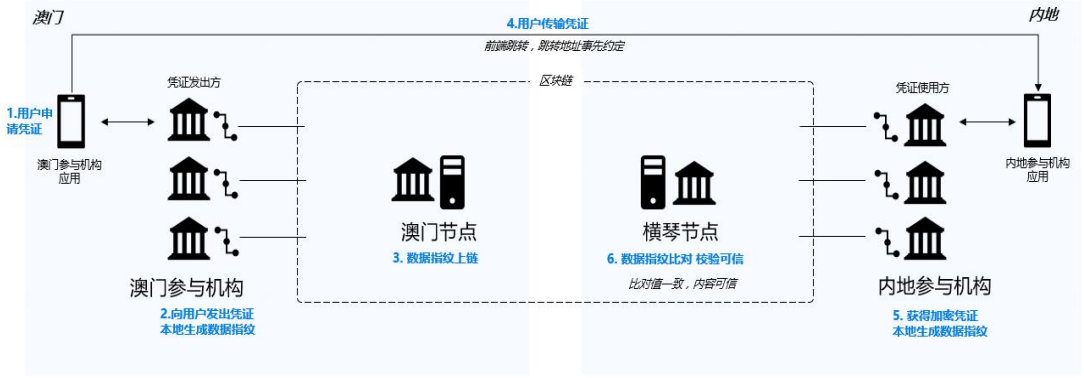

图 3.3-2 粤澳跨境数据验证平台的可信验证服务

平台的核心模块基于微众银行牵头研发的金融级区块链底层平台 FISCO BCOS 开发，是由有限节点组成的区块链联盟链，由指定的平台运营方部署、管理、准入的区块链集群。场景机构通过接口方式接入平台，无需部署、运营及管理平台。在联盟链中，每个节点存储都是独立的、地位等同的，依靠共识机制保证各方存储的一致性。因此，场景机构对数据凭证的摘要存证即是平台中的多方共识，任一方处理凭证可信验证时可使用。

平台为参与机构提供“数据指纹”，即哈希函数(将凭证处理成一串唯一的、不可逆的 64 位字符串)的标准，参与机构将所生成发出或接收的凭证的哈希值，通过平台接口处理上链/链上验证，以此完成凭证可信验证流程。由此，链上仅留存哈希值，无数据原文。

3.3.3. 方案创新点和亮点

（1）数据可信

数据凭证是可信的。利用链的共识特性验证数据指纹，有效解决了跨境场景中机构数据直连门槛较高的条件下，数据使用方难以验证数据真实性的难题。

（2）方案合规

数据凭证原文是由用户自主操作，自主携带跨境的。这项特性受中国大陆地区《个保法》及澳门《个人资料保护法》等法律法规要求个人信息处理者提供信息查阅、复制及转移的途径所启发设计，体现方案在数据处理中关注人格权、数据财产权及主动权的合理思路。同时，方案充分考虑用户的隐私保护意识、适用于对待个人隐私资料更为谨慎的用户群体，契合该群体的心理需要。

平台建设期间，参与各方与粤澳两地数据及场景涉及行业监管均做了沟通，平台涉及的跨境数据验证服务，不违反现有相关法律法规及监管条例，对平台运

行无反对意见。

（3）保护数据隐私

数据凭证隐私可靠。流程中平台不留存任何数据凭证原文，仅记录其经技术处理后所得到的唯一不可逆字符串符。将数据凭证的使用约束在经用户指定的机构及场景中，保护用户的数据隐私，有效规避了数据凭证在传输过程中的滥用风险。

（4）接入成本低

无需场景机构参与部署区块链模块服务。方案由粤澳两地指定的运营方搭建区块链网络，提供平台服务，场景机构仅需通过低成本的接口方式实现“一点接入”核验服务。接口方案标准化，技术相对简单，工作耗时低，可激发相关各方参与的积极性。

（5）多方共建共治跨境基础设施

为避免传统解决方案下，因系统单边部署而引发跨境场景中系统归属等问题，平台的服务由粤澳两地的运营方分别在本地区部署区块链节点及其前置等服务，组成跨境的、共建的对等互信网络。每个节点都是独立的、地位等同的，可以此实现跨境的联盟治理，构建跨境的基础设施及公共产品。

（6）支持多方协同和场景拓展

平台支持多场景拓展。包含但不限于：跨境开户、跨境保险理赔、跨境不动产抵押认证等。对金融、民生，甚至医疗场景均具备适用条件。

平台支持多机构间协同合作。方案不依赖于数据提供方和接收方双方合作，也不依赖中心化机构推动。具体来说，无需单个机构两两处理协议，可凭借接入平台连接多个数据发出/使用方。新的加入者能够很容易地参与其中，满足大范围数据协作的需要。

平台支持跨链拓展。可通过与多个不同区块链平台扩展以支持数据验证的需求，这项特性可支撑平台连接粤港澳大湾区甚至国际化平台，实现更多层次的协同合作。

3.3.4. 应用效果

目前，粤澳跨境数据验证平台的首个应用场景——个人资产证明跨境验证，已经于 2022 年 4 月正式落地。澳门居民通过该服务，在横琴侧银行申请业务时，使用手机银行下载个人在澳门侧银行的资产数据，自行上传至横琴侧银行，银行后台通过粤澳跨境数据验证平台存证的“数据指纹”确认上传资料的真实性。通过使用本平台，粤澳两地的银行将原需耗时数天的业务，缩短到 5 分钟完成，大幅

提升了客户体验及银行运营效率。

粤澳跨境数据验证平台作为粤澳探索建立开放型、合作型、示范型跨境数字服务融合的重要创新实践，亦得到中华人民共和国中央人民政府官网、国家发改委、中联办、央视、新华社等权威平台和媒体的关注及报道。

3.4. 跨境贸易：基于区块链的无纸化跨境贸易流转平台

联易融基于区块链的无纸化跨境贸易流转平台（以下简称平台），通过深圳-新加坡（深新）双方进出口企业、银行、船公司以及 TradeTrust 平台、中国（深圳）国际贸易单一窗口等多方参与，将所有国际贸易单据的提交及转让均可通过电子形式接收处理，实现在信用证结算交易流程中，完全无纸化，方便深新商业机构之间开展跨境贸易。

3.4.1. 案例实施背景

（1）传统跨境贸易模式存在信任缺失问题

跨境贸易中各数据源即参与方不仅数量众多、类型复杂，还因跨境的业务特点，分布在不同国家和地区的管辖区，在没有可靠电子化流程系统的情况下，业务链中任意一方想要确认其他各环节的参与方身份的真实性面临着巨大的挑战。贸易流程中监管所需的大部分数据通常来自于报关行等贸易服务商，或经认证经营者企业（即 AEO 企业）。然而这些企业的数据并非全为一手获得，数据经过层层传递，其可信度大打折扣，导致跨境贸易过程中仅信息核实环节便需要投入大量的时间和人力成本。

（2）传统国际贸易全流程中协同繁琐低效

跨境贸易全流程中参与方间、流程间协同合作十分繁琐。其中大部分环节涉及不同国家多个参与方，甚至不同国家监管机构间的协同合作。由于跨境贸易的业务特殊性，企业和银行之间的单据传递基本都是用线下纸质方式进行，导致整条业务流程的协同低效，进而直接影响贸易结算效率。

（3）传统跨境贸易数字化平台无法核实货权单据的有效性

在未使用区块链技术的环境前提下，几乎所有能够实现跨境贸易数字化的技术方案，均为中心化的服务或平台。这类系统在技术层面和治理层面都具有高度集中的特点，每一个使用者都与中心相连，因此无法判断电子货权凭证的货权归属，转让路径，从而无法利用货权凭证的转让实现国际贸易结算的线上流程。

3.4.2. 案例方案介绍

（1）平台整体架构

无纸化跨境贸易平台结合了国际上被广泛接受的基于区块链的连接政府以

及其他商业机构的交互标准以及基础架构，通过对接 Tradetrust 实现可信的跨平台电子交易单据互操作和交易流通。Tradetrust 具备公开且无任何准入条件、没有中心化政府及机构、链下数据保证数据真实性、无标准格式限制、符合新加坡对于电子单据法规要求、一切皆开源等特性。

无纸化贸易平台整体架构由基础设施层、平台架构层和商业应用层组成，隔层之间以灵活解耦方式联通，具有很好的扩展性和灵活性，具体如下：

1) 商业应用层：包括国际贸易单据流转，国际贸易结算，国际贸易融资等在内的商业化应用、平台、生态。
2) 平台架构层：支持多类型跨境电子单据交易标准、语义、合规性，实现电子单据标准化交互。
3) 基础设施层：区块链服务网关提供了标准化接口，并实现应用与底层平台的解耦，并且通过开源方式与社区合作共建，并提供了相应的标准化交互协议及开发工具。

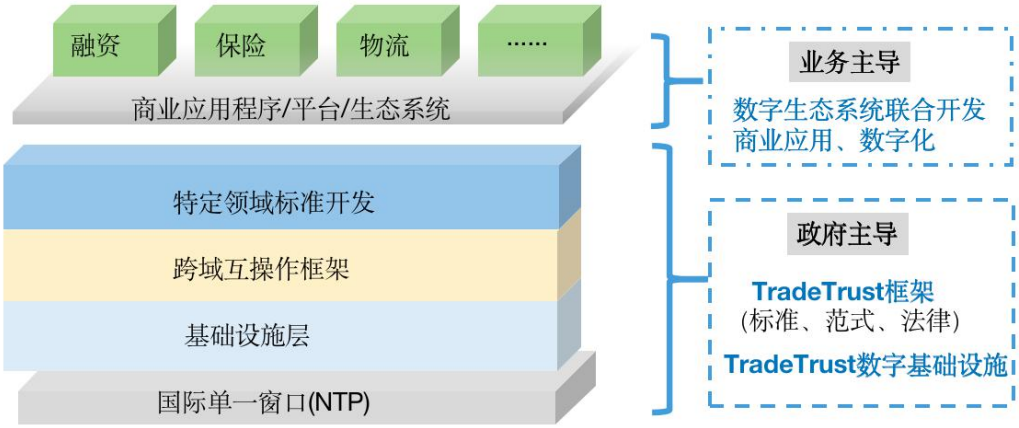

图 3.4-1 无纸化跨境贸易平台整体架构图

（2）平台的业务流程

进口商和出口商可以通过无纸化贸易平台完成主要业务交易流程，具体如下所述：

1) 进口商以及出口商线下约定并签署商业合同；
2) 进口商向进口方银行申请开立信用证；
3) 进口商银行通过 swift 将信用证转给出口商银行，同时完成信用证在无纸化贸易平台上的流转；
4) 出口商将货物（海运/空运）发给进口商，取得电子提单；
5) 出口商登录无纸化贸易平台，在线发送信用证项下单据，验证电子提单

真实性，并将其转让给出口商银行；

6) 出口商银行登录无纸化贸易平台，审核单据无误后，验证电子提单真实性，并转让 title 给进口方银行，并将整套单据发送给进口方银行；

7) 进口商银行登录 GUUD 平台，审核单据无误后，验证电子提单真实性，并将整套单据发送给进口商；

8) 进口商确认单据后，进口方银行将提单 title 转让给进口商，进口商完成提货付款；

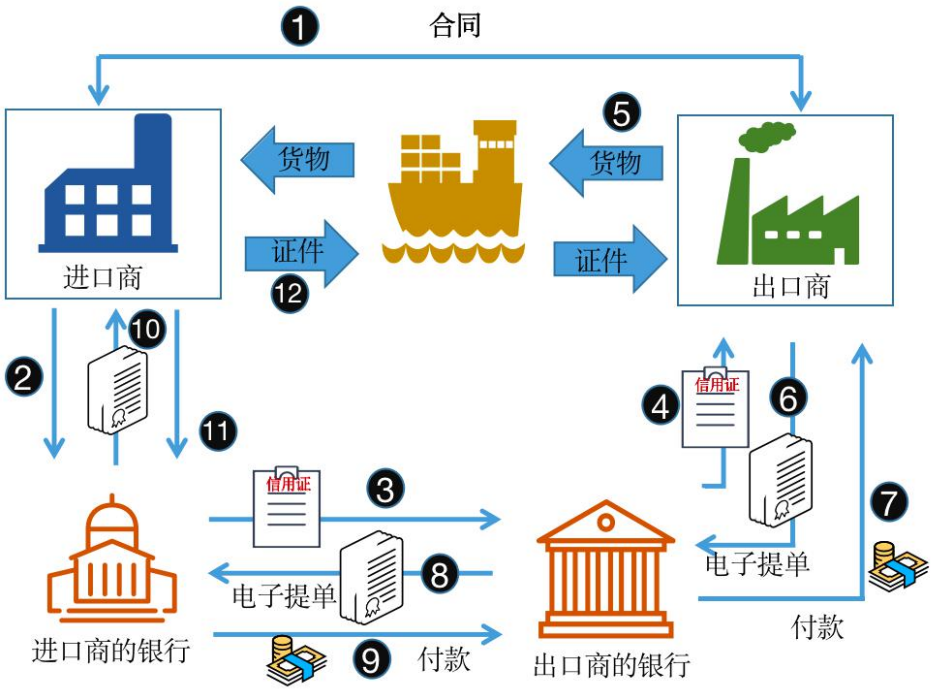

图 3.4-2 无纸化跨境贸易平台业务流程图

（3）平台的技术架构

平台在从技术层面可划分为应用层、服务层、区块链层和协议标准层，每个层级之间均具有很好的稳定性和兼容性，具体说明如下：

1) 应用层：国际贸易无纸化相关的各类商业化应用；

2) 服务层：为各类应用提供接入其他商业技术的能力；

3) 区块链层：支持多类型区块链底层平台；

4) 协议标准层：定义标准单据交互协议标准。

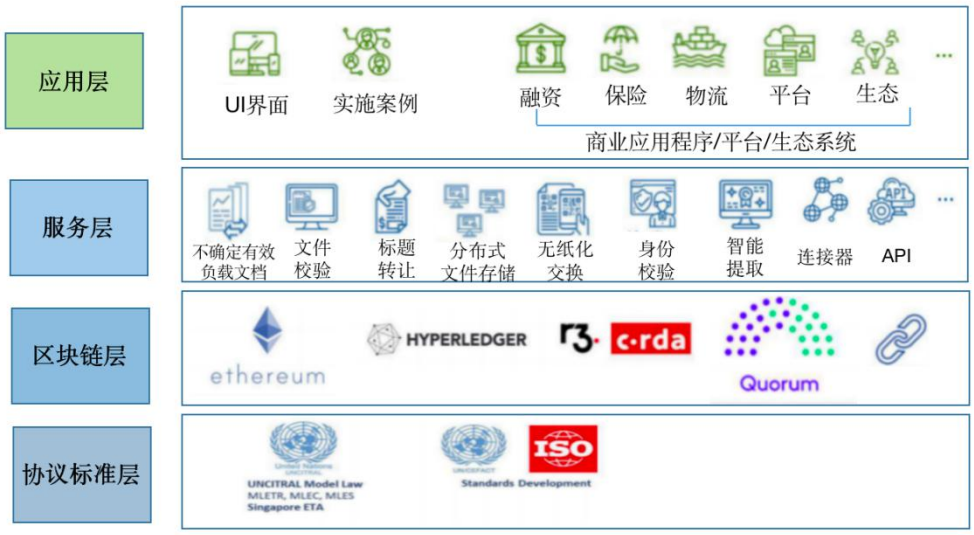

图 3.4-3 无纸化跨境贸易平台技术架构图

3.4.3. 平台的创新和亮点

（1）模式创新

平台使用标准交互协议将跨境贸易中的单据从纸质变为电子化，提升贸易流程中的单据处理效率。

（2）流程创新

流程中的所有参与方均可在平台上进行相应操作，流程更加透明化和细节化，有利于电子提单和其他单据的追踪和溯源。

（3）技术创新

提供了标准化的单据交互协议方案以及从三个层面链上校验（Issuer 身份合法性、单据完整性、单据状态有效性）电子提单的货权，保证整个提货流程的安全性。

3.4.4. 案例应用成效

（1）推动贸易流程节能减排

联易融将 ESG 因素融入到产品和增长决策中，把科技解决方案设计为数字化和云原生，使其客户和合作伙伴实现贸易流程无纸化，大量减少碳足迹，并促成更精简和可追踪的工作流程，以推动长远效益、透明度和生产力。

（2）减少贸易流通的成本和风险

跨境贸易无纸化平台，可以使得贸易流各方在互相认证的区块链平台线上接

收数据，大大降低处理时间，免去的纸质文本的寄送节点，同时降低文件丢失风险，帮助平台企业将贸易成本降低 20%以上。

3.5. 绿色金融：碳配额交易跨境人民币结算系统

碳配额交易跨境人民币结算系统（以下简称“系统”），依托清算机构并与碳交易场所连接，实现信息流、碳要素流、资金流的互联互通，致力于服务实体企业跨境结算便利化需求。

3.5.1. 案例实施背景

为响应国家做好碳达峰、碳中和工作的战略部署，进一步发挥跨境金融市场基础设施作用，服务实体企业跨境结算便利化需求，深圳市雁联计算系统有限公司（雁联）为香港人民币清算行中国银行（香港）（以下简称“港中银”）创新研发了碳配额交易跨境人民币结算系统。

图 3.5-1 碳配额交易跨境人民币结算系统

3.5.2. 案例方案介绍

（1）系统总体业务流程

该系统配合银行间市场清算所（以下简称“上清所”）对接广州碳排放权交易所（以下简称“广碳所”），依托人民币跨境支付系统（CIPS）完成了中国碳排放配额的跨境交易结算，有利于吸纳境外投资者投资中国碳排放市场。

投资者在交易场所发起的交易指令，包括卖方挂牌、买方议价、交易成交等，均通过上清所传送至结算银行；除交易指令信息流外，还涉及投资者银行账户资金冻结、解冻、成交款划账、手续费扣收、结算货款等资金流处理。上述资金清结算处理，基于银行对买卖投资者严苛的反洗钱甄别。

1) 跨境结算（买入流程）

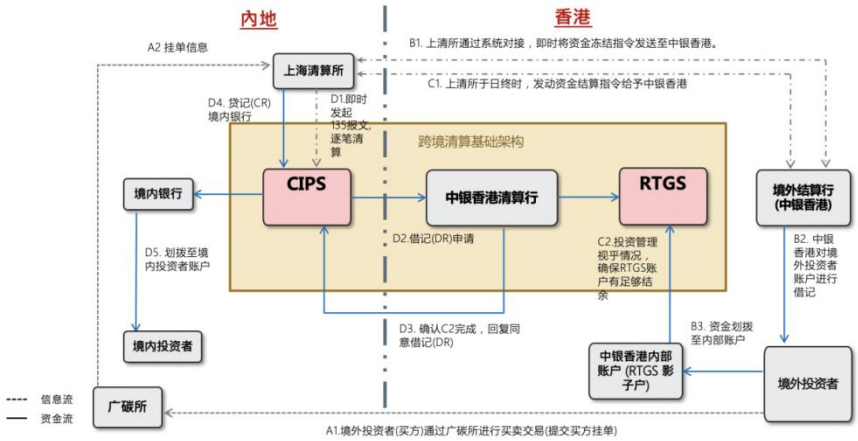

图 3.5-2 跨境结算-买入流程图

2) 跨境结算（卖出流程）

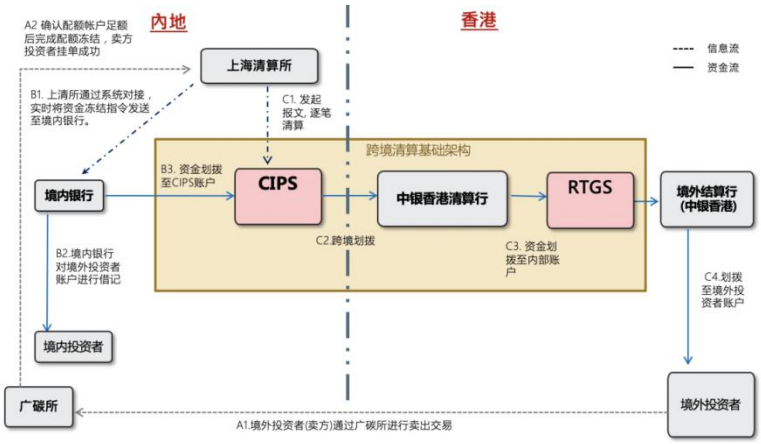

图 3.5-3 跨境结算-卖出流程图

（2）系统技术架构

系统采用分布式微服务架构，基于雁联自主知识产权的低代码平台开发。结合业务功能需求及非功能性要求进行规划，将系统进行层级划分，以开放服务层、渠道层、应用层、数据访问层等组成。层级技术实现为系统提供较高的规范化和灵活性应用基础。

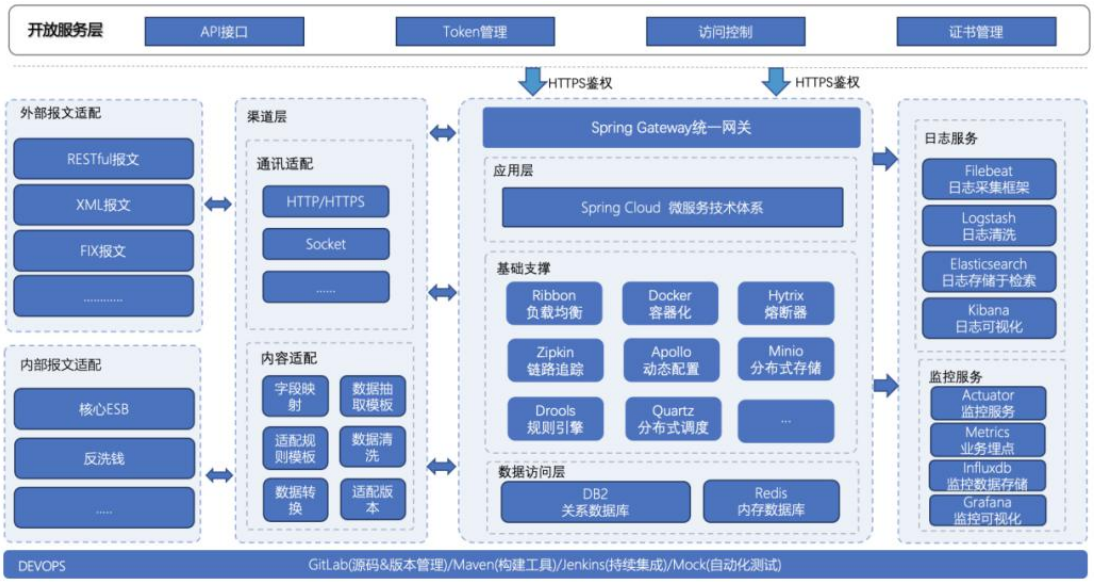

图 3.5-4 碳配额交易跨境人民币结算系统架构图

1) 开放服务层

开放服务层提供外部接入方的对接，平台为其提供统一标准的业务服务。

2) 渠道层

该层级规划为平台与外部合作方的对接，也提供数据安全访问的支持，包含有数据签名的管理，数据加密传输协议的支持，以及安全访问控制等技术支持。

3) 应用层

应用层以 SOA 的方式，涵盖核心业务处理的所有服务；该层结合外围系统数据接口、后台数据库以及高效计算处理的缓存数据，实现整个平台的业务逻辑处理。

4) 基础支撑层

基础支持层涉及高可用性服务支撑，包括前端负载和服务器负载；针对海量请求的熔断、限制流量处理机制；多层级服务依赖调用的链路追踪等。

5) 数据访问层

数据访问层提供高效的数据访问处理，提供了关系数据库连接池管理服务，数据持久化服务，分布式事务管理服务以及多数据源访问服务。

（3）数据跨境传输流程

系统的数据在香港和内地之间流动，包括境外投资者身份信息、碳配额交易信息、银行账户资金信息等。

碳配额交易信息涉及卖方挂牌、买方议价、交易成交、交易取消等，均由广

碳所发起，经上清所中转，最终传输至中银香港。涉及境外投资者银行账户冻结、解冻、划转以结算操作，由中银香港处理完成后，向广碳所反馈资金处理结果。涉及境内境外银行间的资金清算，由上清所向 CIPS 发起指令，数据由 CIPS 流转至作为人民币清算行的中银香港。

3.5.3. 案例应用成效

本系统是在中国人民银行和银行间市场清算所指导下，服务实体企业跨境结算便利化需求的战略试点项目。取得的社会效益如下：

（1）率先在大湾区内实现了碳要素流、资金流、信息流的跨境互联互通。探索为国内外碳市场联通打通渠道、为我国碳市场国际化发展夯实基础。

（2）推动内地碳金融交易的对外开放，吸引国际投资者参与碳期现货市场，形成有国际影响力的碳排放权定价机制，助力我国人民币国际化战略。

3.6. 跨境零售：奢侈品零售跨境数据安全防护系统

奢侈品零售跨境数据安全防护系统（以下简称系统），保障数据依法合规流动，为数据资产、API 资产提供统一安全的网关出口，实现全链路数据隐私合规管理，致力于服务国际奢侈品零售行业对个人信息和重要数据出境的安全性需求。

3.6.1. 案例实施背景

某国际奢侈品零售公司为保证业务正常运转需要对境内个人数据进行访问，具体场景如下：境外门店为保障 VIP 客户权益，需要将 VIP 客户信息同步到全球；境外总部需要按需访问境内销售数据。依据 GB/T35273《信息安全技术个人信息安全规范》规定，个人信息的处理需要遵守：最小必要和确保安全的原则。规范也明确指出对个人信息的处理需要进行去标识化等保护措施，因此，为保障客户业务的合规开展，符合对个人信息和重要数据出境的安全性需求，星环科技提供了奢侈品零售跨境数据安全防护系统解决方案。

3.6.2. 案例方案介绍

该系统可以帮助企业梳理出境数据资产，通过自动化和人工标记相结合的手段，识别其中的个人敏感信息和行业重要数据，并通过安全网关对个人信息出境提供事中防护控制与留痕，为出境合规提供技术保障。

（1）系统总体业务流程

系统核心功能模块包括数据安全管理平台 Defensor、数据 API 网关 Midgard

等，提供重要数据与个人信息识别、数据安全生产、动态安全防护、出境链路监测等安全服务。基于分类分级规则，通过 Defensor 批量任务实施对数据资产的分类分级扫描识别，完成待出境数据的敏感数据资产地图。Midgard 数据 API 网关通过引入流计算、SQL 解析、分布式缓存等技术，解决传统模式下存在的开发规范不统一、多数据源适配难等问题、对 API 统一进行发布管理，为数据资产、API 资产提供统一安全的网关出口。

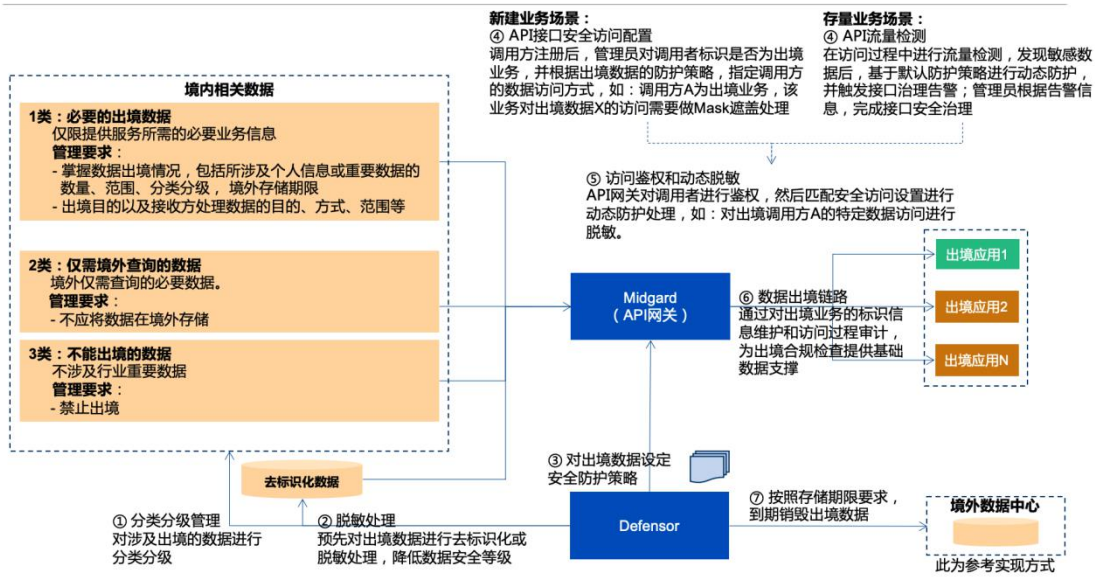

图 3.6-1 奢侈品零售跨境数据安全防护系统的业务流程图

针对国际奢侈品零售行业的跨境业务特性与数据治理需求，系统帮助企业建设数据安全合规平台和安全流通网关，实现技术落地；并从实施角度，持续进行数据安全日常运营和建设。同时依据相关法律法规，帮助企业周期自查，出具合规检查报告，实现预先发现问题，优化数据治理工作并进行技术平台及工具的建设。

（2）系统实现流程

以某国际奢侈品零售行业数据出境风险及解决方案为例，实现步骤如下：

1）敏感数据的分类分级

数据安全管理平台 Defensor 通过正则、关键字内容、算法识别以及机器学习等手段对企业敏感数据进行识别，结合人工复核等实施步骤，梳理出境数据，生成出境数据清单，为后续个人数据出境的安全防护提供指导。

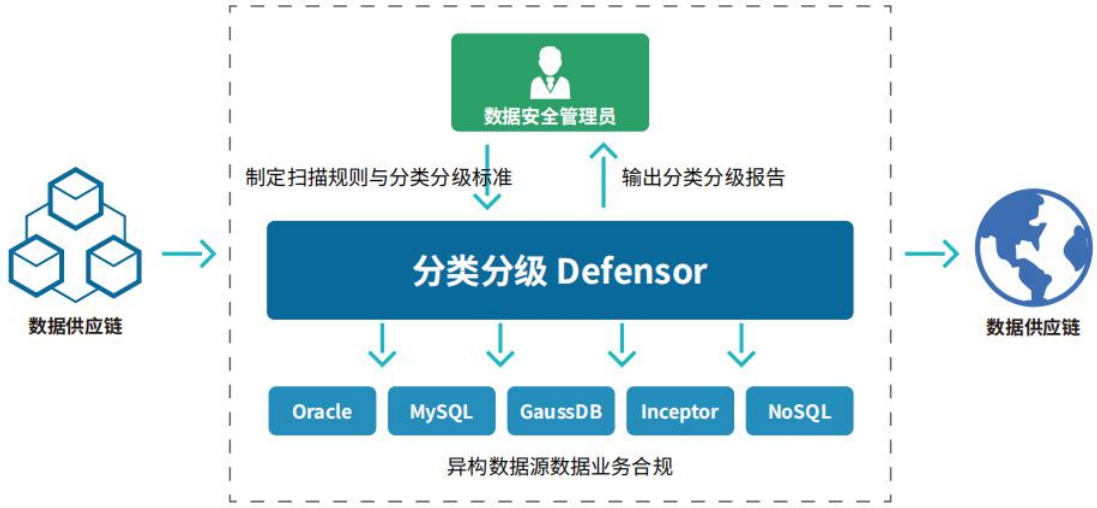

图 3.6-2 敏感数据分类分级流程图

2）个人敏感数据的存储和管理

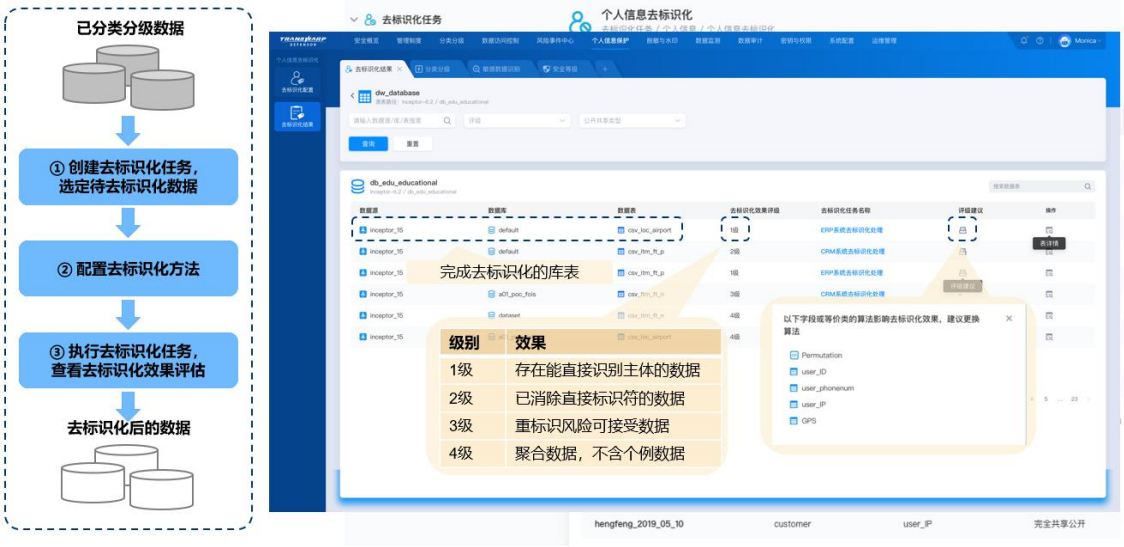

图 3.6-3 敏感数据存储管理流程与系统展示图

本案例中的某国际奢侈品牌公司内的数据库储存数亿条客户记录和内部日志，包括用户支付数据和员工敏感信息。该数据出境前，为保证这些敏感数据在业务使用或共享中的安全性，系统根据业务要求，实施个人信息去标识化，消除或降低个人信息重标识风险；根据业务要求，实施静态脱敏，降低敏感信息的数据定级或去除敏感信息。

系统通过去除或降低数据集中个人主体信息（直接标识和间接标识）的区分度，使得数据集中的信息不能对应到特定个人，同时保留数据集所需的使用价值。去标识化操作发生在涉及个人信息保护的各个环节，如终端侧显示个人手机号是

只显示后四位，API 共享数据时对个人信息去标识化。

3）安全可信场景下的数据安全网关

星环 Midgard 提供统一安全的网关出口并提供 API 层的动态脱敏，为数据资产、API 资产提供从数据源接入、数据指标开发、指标发布、服务授权等全生命周期管理。如图 3.6-4 所示，为保证境外系统通过 API 接口调用数据时的业务能够稳定进行，平台将服务按业务分类、重要等级、响应时间等维度划分成多组，再按每个分组的资源消耗情况绑定相应数量的网关执行单元。通过业务分组，做到不同类型服务的资源隔离，实现服务 SLA，保证高优先级服务持续可用，避免部分慢响应服务超载导致整个系统雪崩。

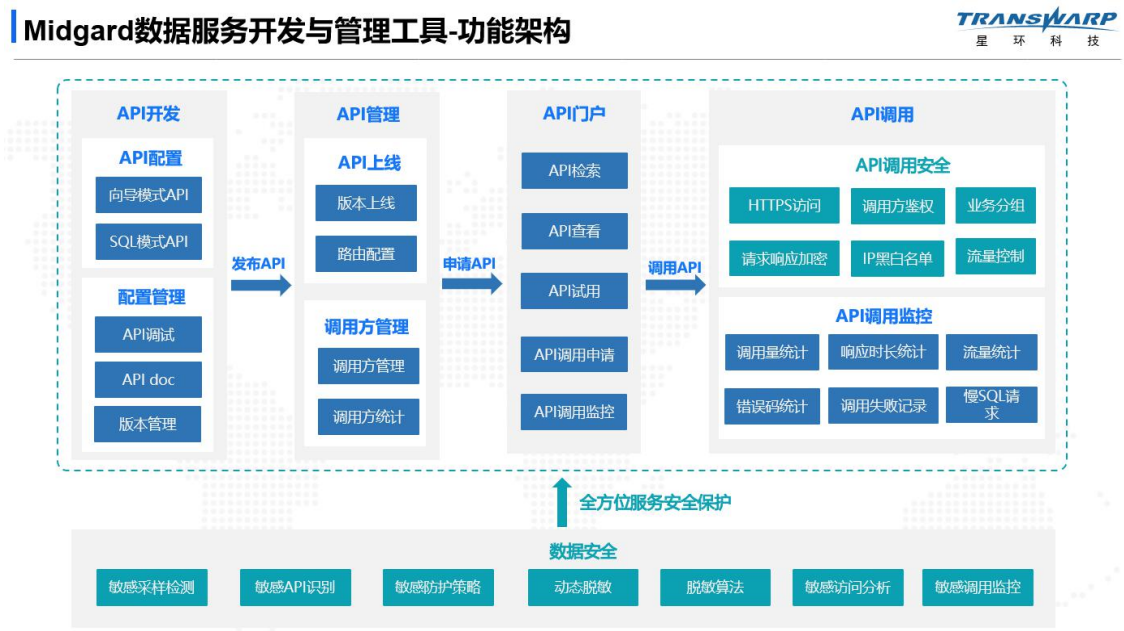

图 3.6-4 Midgard 数据服务开发与管理工具-功能架构图

经过实际案例验证，数据安全网关能够识别并拦截可疑请求，防止敏感数据泄露，跟踪溯源泄露数据。

3.6.3. 案例应用成效

本系统是根据《数据安全出境评估办法》的指导，服务国际奢侈品零售行业对个人信息和重要数据出境安全性需求的试点项目。为探索国内外奢侈品零售市场的数据安全防护机制起到示范作用，运用技术手段，解决了数据跨境流动过程中，基础设施关键信息安全保护方面出现的实际业务问题。

3.7. 数据流通基础设施：跨境数据安全与数据要素化工程系统

为了促进数据跨境安全流通，中国电子的跨境数据安全与数据要素化工程系

统以数据金库和数据要素加工中心为核心，建设自主可控、安全可靠的新型数据要素基础设施数据金库，保障跨境数据的安全存储，强化数据资源监管；建设数据要素加工中心，对数据要素化流程以及数据金库的硬件资源、软件资源、数据资源和数据元件进行调度管理，并实现从数据归集到数据元件加工交易全生命周期的数据要素开发和管控。通过跨境数据安全与数据要素化工程系统，有效化解数据安全和数据流通的矛盾，实现“原始数据不出域、数据可用不可见”的数据流通交易范式。

3.7.1. 案例实施背景

当前，数据流通交易主要面临两大类问题：

（1）数据安全问题

一是本质安全难以保障，我国数据安全的底层技术与产品依然存在“卡脖子”现象，尚未实现自主可控，本质安全难以保障；二是过程安全日益严峻，数据流通交易与隐私保护的矛盾日益突出，亟待从外挂式安全向主动安全、从被动防御向主动防御转变；三是制度安全权责不清，数据治理主体安全权责不清，数据安全管理制度尚不完善，数据在不同机构之间流动、共享和交换过程中的权责边界模糊。

（2）数据流通问题

一是数据权属关系复杂，权力主体分散，导致数据确权难。二是数据格式非标、多变，计量维度多样，数据计量难。三是数据存在“双向不确定性”，亦缺乏清晰定价规则，导致数据交易定价难。四是缺乏合适的交易标的物，导致数据交易难以规模化。

因此，需以可析权、可计量、可定价且风险可控的数据元件为安全流通对象，实现原始数据与数据应用“解耦”，破解数据安全与数据流通难题，让数据“供需两端”贯通。

3.7.2. 方案介绍

（1）方案思路

基于数据安全与规模化流通面临的难题，中国电子联合清华大学率先开展数据治理的研究，提出通过“中间态”数据元件实现数据安全与数据要素化的解决思路。数据元件是通过对数据脱敏处理后，根据需要由若干相关字段形成的数据集或由数据的关联字段通过建模形成的数据特征。以数据元件作为主要交易标的物，有效实现原始数据和数据应用“解耦”，实现数据的风险隔离与安全管控。同时，发挥数据全生命周期追溯管理的关键节点作用，推动数据低成本、高效率的流通和交易，实现数据流通交易的精准监管、数据资源的产品化流通和规模化

应用。因此，围绕数据元件作为数据交易的主要标的物，建设数据金库和数据要素加工中心，保障数据安全，促进数据规模化开发，构建数据安全与数据要素化工程系统。

（2）方案架构

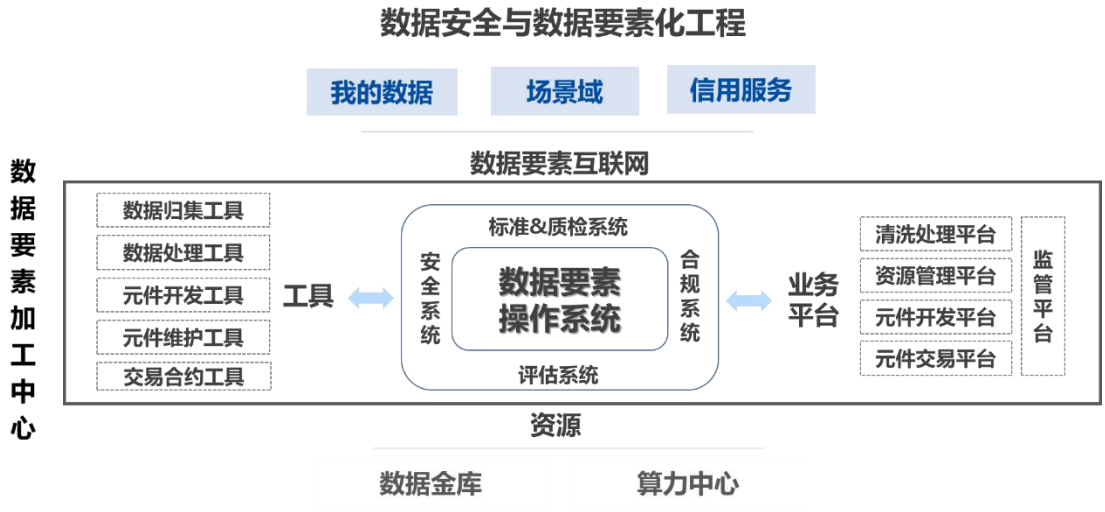

图 3.7-1 数据安全与数据要素化工程框架图

如图 3.7-1，数据安全与数据要素化工程包括数据要素基础设施、数据要素加工中心、数据要素互联网和数据要素创新应用。数据要素基础设施主要包含数据金库和算力中心，数据金库是由政府主导建设、自主可控、安全可靠，存储核心数据、重要数据、敏感数据和数据元件的数据存储设施；算力中心是基于 PKS 体系构建的计算和存储基础设施。数据要素加工中心是整个工程系统的核心，包含数据要素操作系统、五大支撑体系（标准系统、安全系统、合规系统、质检系统和评估系统）、五大业务平台（数据清洗处理平台、数据资源管理平台、数据元件开发平台、数据元件交易平台和监管平台）以及五大数据要素工具箱，负责对数据要素化流程以及数据金库的硬件资源、软件资源、数据资源和数据元件进行调度管理，并实现从数据归集到数据元件加工交易全生命周期的数据要素开发和管控。同时，以数据元件作为流通对象，构建一张数据要素互联网，实现数据元件标识、检索和流通协议管理。通过数据元件创新数据产品开发方式，基于要素化工程体系打造数据要素创新应用，构建“我的数据世界”、信用服务以及场景域等创新应用。

（3）方案技术流程

基于全自主的 PKS 底座、中国电子云和高标准的安全体系，构建数据金库和数据要素操作系统，有序开展数据归集、数据清洗处理、数据元件开发、数据元件交易等数据治理工艺全流程。数据金库作为存储和管理数据资源和数据元件的载体，依托数据要素操作系统实现资源和流程的高效管理。数据要素操作系统

负责对数据要素化流程以及数据金库的硬件资源、软件资源、数据资源和数据元件进行调度管理。数据治理工艺流程涵盖数据归集、数据清洗治理、数据元件开发、数据元件交易，有序开展数据治理 20 道工序。最终，数据要素加工中心可对接跨境数据交易平台，实现数据元件流通交易。

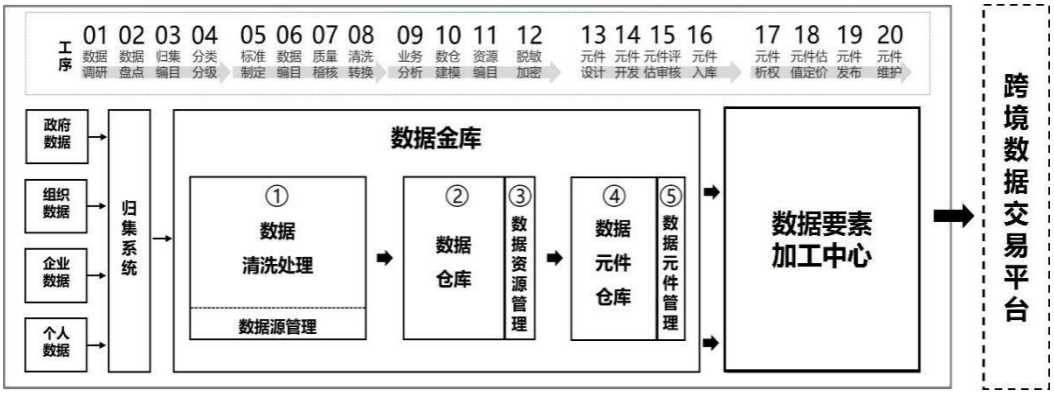

图 3.7-2 数据要素化流程图

3.7.3. 案例应用成效

四川省德阳市于 2021 年 7 月与中国电子启动合作，共同开展德阳市数据安全与数据要素化工程，以“一库双链，三类市场”为核心思路，从制度、技术和市场三方面协同推进，取得了如下丰硕成果：

（1）强化数据制度保障

中国电子配合德阳市设计完成了“1+4+N”核心制度体系（1 项顶层规划、4 项管理制度及 N 项配套细分制度），为德阳市组织机构改革、数据要素管理、三类市场运行管理、数据安全保障等工作提供制度保障。

（2）打造新型基础设施

建设德阳市数据金库、数据要素加工交易中心等新型基础设施，为有序开展数据归集、安全存储、数据清洗处理、数据元件开发、数据元件交易等数据要素市场化流通全流程提供基础支撑能力。

（3）构建要素三类市场

中国电子依托自身丰富完善的数据生态资源，协助德阳市人民政府引育数据生态企业近 50 余家，初步构建起数据资源、数据元件、数据应用三级市场，共同参与德阳市数据要素市场化配置改革。

（4）培育全新数据产业

坚持以场景为牵引，推动德阳市数据产业链上下游的专业化、精细化分工，吸引各类数据企业聚集，形成完善的数据产业生态圈。根据市场需求，已开发各类数据元件 332 个。

（5）赋能社会经济发展

为使数据要素有效赋能实体经济，中国电子协助德阳市已设计了 37 个应用场景。通过数据元件的流通推动政企银、预付费卡监管、新市民保险、科创贷等场景，产生了巨大的经济价值。

3.8. 跨境电商：智能化技术实现跨境电商数据合规高效使用

近年来，跨境电商业务数据应用日益成为企业关注的焦点，通过对数据的分析，企业能够更好地了解跨境电商业务的运作情况，从而提高业务效率和盈利水平。 本案例介绍九鑫智能通过智能化技术，实现高效合规获取、使用和分析跨境业务数据，帮助跨境电商在满足数据使用需求的同时，合规提升运营效率。

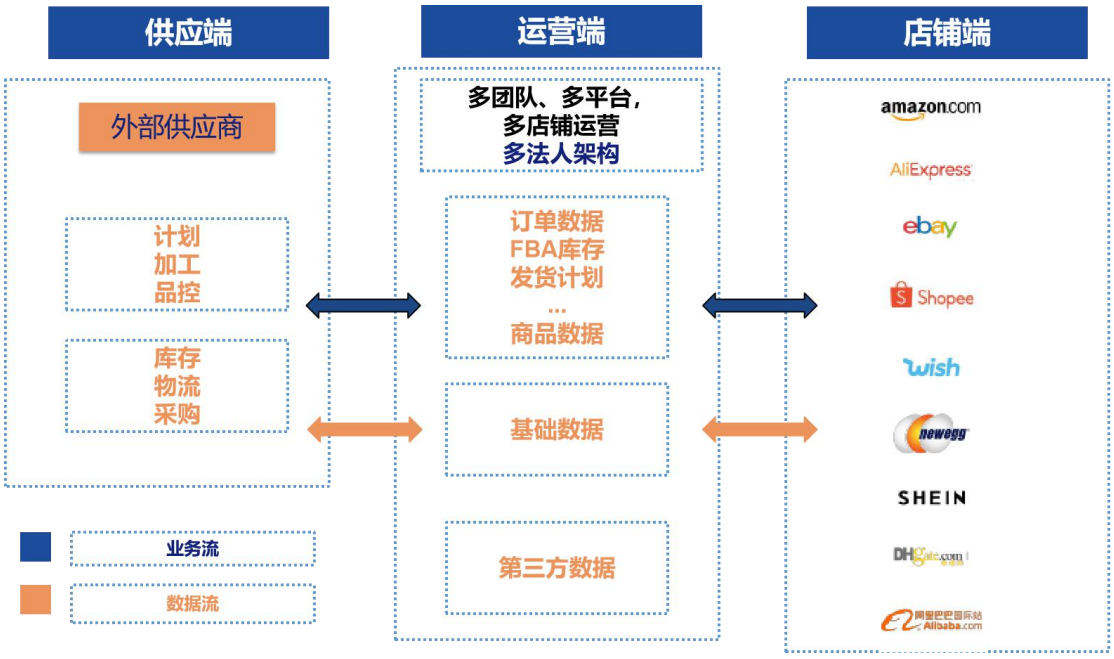

图 3.8-1 跨境电商业务数据传输示意图

3.8.1. 案例实施背景

目前在全球电商贸易环境，数据信息准确和公平竞争是保障跨境电商合规运营主要关键词，运营流程和数据处理的高效和高质量是保证市场竞争力的必要条件。由于各个跨境电商平台都出台了规范卖家运营行为的准则，传统的爬虫等方式，无法帮助跨境电商获得鉴权的数据，这为使用系统庞杂数据和管理、回溯业务流程带来了巨大风险和成本压力。

基于多个电商平台系统、供应链系统、运营工具等都是相对独立的系统和各自特有的数据管理标准，同时海量数据也带来运营和分析的挑战，当前跨境电商数据的采集仍主要依赖大量的人工统计或各类小工具导入，或者依赖某个平台提供的部分有条件的数据支持能力，这种分散且低效的运营流程和数据处理，难以

满足实际业务和市场竞争需求。在采集、传输、分析等多个环节都需要能够适应全球跨境电商业务快速发展需要的技术保障。

3.8.2. 案例方案介绍

（1）方案思路

跨境电商企业多平台、多国家，多站点的业务运营场景，带来多维及复杂的数据处理合规问题，带来成本和质量及高效的运营效率问题。本案例介绍了九鑫智能的智能自动化解决方案，以流程自动化 RPA 及 AI、BI 等自有知识产权的流程及数据处理平台为核心，为跨境电商提供包括素材维护管理、商品发布计划管理、商品自动上架及广告自动投放等关键业务能力为核心的智能自动化解决方案，实现跨境电商高效且合规获取、使用和分析全渠道跨境业务数据，同时提供具备人工智能特点的运营自动化工具，实现运营质量和效率的提升，满足跨境卖家规模发展、快速响应、创新领先、成本可控、合规稳健的诉求。

（2）方案功能

图 3.8-2 数字化业务系统结构图

为解决此跨境业务场景实现运营和数据处理的智能自动化，通过超自动化平台可以提供全链路的数据自动获取、流通、分析和追踪：

1) 可通过智能数据平台实现通用知识库和分类商品知识库的生成和录入；可实现多平台、多店铺客服渠道和订单数据聚合归档；
2) 可通过机器人智能客服进行咨询回复，并支持人工介入、新知识入库，逐步丰富知识库并持续提升客服能力，提升客服效率和满意度，为选品智能分析提供数据来源；
3) 可通过跨系统登录、跨境数据下载及跨境数据处理对多平台、多系统数据进行采集；结合 AI 和自动化的方式 包括 OCR 识别、定时扫描、共

享表单填写、邮件通知等模块进行辅助采集；并将非结构化数据转为结构化数据，实现全链路的数据采集和应用；

4) 跨境数据采集和处理流程可通过平台实现自动监测和执行，在高效、高质量的前提下，保证数据获取鉴权管理完整，数据来源和流通过程可见并进行签名处理，在数据流通过程形成数据资产，为业务数据分析提供更丰富维度和内容；

5) 可持续扩展和积累数据源连接和高质量数据业务模型，在全域数据和全链路流程的基础上从流程自动化向业务智能化演进，最终实现数据智能辅助决策；

3.8.3 案例应用成效

通过智能数据平台技术推动我国跨境电商在复杂多变的跨境平台和数据规范法规要求上走向数据合规驱动业务。通过数据和流程汇聚跨界行业最佳实践，提升跨境电商发展质量，保障我国对外贸易企业及生态竞争力。以某多电商平台跨境电商头部卖家为例，本方案替代了 85%的人工操作，时间和培训成本下降 55%，峰值时每日节省工作时间约 1100 分钟，月平均节省人力约 18.75 人天，自动化流程可随业务发展需求快速调整。通过智能数据平台技术推动我国跨境电商在行业数据规范和法规要求下实现数据合规驱动业务。提升跨境电商发展质量，保障我国对外贸易企业及其生态的竞争力。

3.9. 智能汽车：车联网数据跨境安全合规整体方案

车联网数据跨境的合规性及安全性备受行业关注。智能汽车在行驶过程中收集了大量环境、个人及行驶数据，一旦在跨境使用的场景中缺乏管控或出现安全问题，对各方而言都是极大的威胁。勤达睿（Kyndryl）通过一系列的合规框架体系落地服务，结合区块链和隐私计算技术平台，实现车联网数据跨境流通全过程的合规可控，降低攻击、泄密等数据安全风险，也极大提升了传统合规管理模式下数据跨境流转的时效和管理效率。

3.9.1. 案例实施背景

（1）发展趋势

随着全球互联的场景和新能源变革的驱动，智能汽车已经成为除手机以外移动互联的新型载体。在智能与网联的双轮驱动下，车联网已经是各大车企的战略竞争制高点。智能汽车行驶所产生的数据不仅仅是车载平台迭代升级的关键数据资源，其分析应用及价值挖掘对智能汽车的产品研发、车辆仿真模拟、全球市场

的营销分析等业务领域和数字化转型都具有重大价值。目前车联网数据服务具有以下的三大特点：

1) 全球化的汽车产业布局带来数据跨域跨境的诉求。汽车企业各机构及相关的上下游产业链遍及全球，随着车企的全球化和出海策略，车联网数据呈现了跨行业跨域跨境共享交换的趋势和需求；
2) 车联网数据及跨境跨域管理服务需求海量涌现。中国车联网行业渗透率已超过 48.8%，车联网用户规模在 2022 年将达 20890 万辆，同时多元化的车联网生态也使得单台车的车联网数据暴增。如何实现数据资产在跨域跨境领域的有效管理、透明可溯，逐步成为数据管理服务需求的标配；
3) 汽车数据安全及合规要求日益严格。车联网通信方式的开放性、车联网数据的特殊性带来了各种安全和隐私保护问题。目前各个国家和地区针对数据安全相继出台和落地的各项政策和法规，使得车企传统的数据跨境跨域方案面临日益严格的监管挑战和惩处力度；

（2）业务挑战

车联网数据跨境的核心挑战在于：

1) 数据跨境场景面临安全风险。如何应对车联网数据在跨境传输和访问时数据窃取和篡改的威胁，从而能够保障车联网数据在跨境场景下的安全性并实现数据隐私保护；
2) 跨境跨域存在法律合规的挑战。车联网数据包含着行车环境和用户的隐私敏感信息，如何在满足各个国家和区域的法律法规要求，并且实现车企对数据跨境全过程的自主可控可追溯，避免高额处罚和法律风险是面对的困难和挑战；
3) 实时性和管理效率不能满足要求。车联网数据跨境使用的实时性要求较高，而在现有法律法规和数据跨境管理模式下，往往很难满足跨国车企对大量数据跨境时的实时性和管理效率的要求。因此在数据跨境实施落地的过程中，如何利用技术手段提升效率，并通过体系化的建设实现可持续高效运营是车联网数据跨域跨境的落地挑战之一；

3.9.2. 整体解决方案

（1）方案思路

目前针对车联网数据的管理，尤其是涉及车联网数据出境问题，我国已出台相关法律规定和行业标准。本方案的数据管理流程参考了《网络安全法》《汽车数据安全管理若干规定（试行）》《数据出境安全评估办法》《关于车联网网络安全和数据安全标准体系建设指南》等中相关要求。结合分布式强一致性、不可

篡改、防伪溯源的区块链技术和可实现数据可用不可见的隐私计算技术，在车联网数据跨境流动的场景中，基于数据安全治理及数据脱敏、数据分级分类、数据跨境安全评估等多环节路径落地，提供创新性整体解决方案。

（2）车联网数据跨境整体解决方案

基于某车企客户的实际数据流转情况，勤达睿给出以下解决路径：

1) 跨境数据治理

从系统或相关应用中抽取相关需要跨境的车联网数据，将原始数据传输至企业数据中心的数据平台进行汇集治理，避免对车载系统、车联网通信链路及相关营销服务平台产生扰动和资源耗费。在数据汇集的基础上进行车联网数据的治理工作。企业数据中心依据跨境数据平台的内生标准对原始数据进行处理，对于有需求且可以跨境的数据生成索引信息。

2) 数据分级分类

基于对于车联网数据的分类，结合车企的实际需要，对三类车联网数据即车辆自身数据、车辆环境数据和用户数据进行定义及分类。

基于客户实践对于车辆周边数据，包括智能汽车行驶的周边道路、天气条件数据、行车区域及地理位置数据等，可能涉及国家安全数据。

对于车辆自身数据，包括但不限于智能车运行状态数据，如车速、里程、耗电/油、刹车、电池使用和变化情况等和车辆的操作数据，如启动、转向、加速、制动等操作及与此相关数据，车载电子系统的中控数据，维修、维保、故障数据等则绝大部分为非限制数据。

对于用户数据，包括个人数据，如基本资料、个人身份信息、个人生物识别信息以及用户行为数据，例如汽车温控设置、巡航设置、常用目的地设置、车载娱乐数据及偏好等则需要更多的脱敏处理或隐私访问。对每一类数据的基本属性包括字段名、定义、数据来源、提供必要性、参数定义、有效范围等多个维度进行标识，并按照是否可以出境将各类数据分为禁止出境、统计分析及算法使用结果出境、脱敏处理后可出境、无限制出境标定涉密等级。

3) 数据跨境安全评估

伴随着车联网技术的快速迭代和车联网应用的迅速增长，数据出境的发生频次可能较高，面对业务层面随时可能触发的数据出境安全评估需求。对于不同等级的涉密数据，通过区块链系统节点记录后将其广播给区块链系统集群中的其它节点，主管部门、第三方机构和境外企业可通过数据跨境用户端检索相关数据索引。同时，数据跨境相关企业将备案评估情况发送给监管职能部门进行审核与备案。其中备案评估情况包括但不限于企业资质情况、数据字段描述、企业自评估、第三方安全评估、传输需求情况以及由跨境原始数据所生成的数

据索引等信息。在监管职能部门完成审核与备案将“传输许可”发送给境内企业数据中心以及跨境平台后，便可开展数据跨境相关活动。

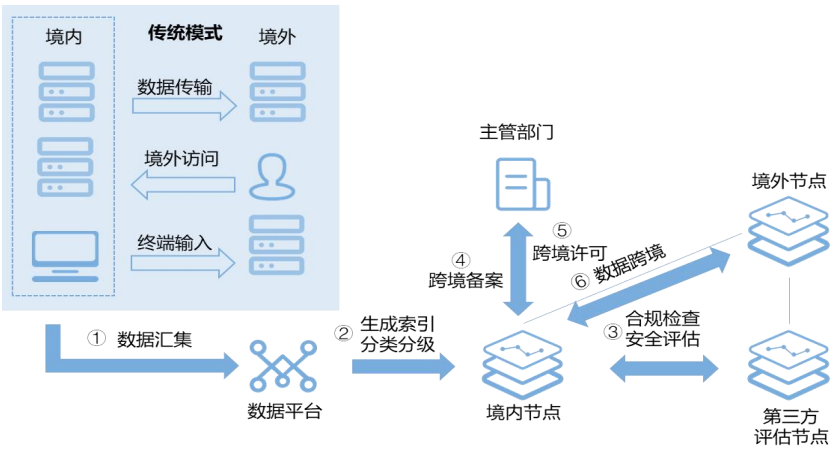

图 3.9-1 数据安全评估服务流程图

4) 数据跨境服务平台方案

勤达睿尝试提供平台化的工具来支撑繁杂的跨境数据治理、跨境合规管理及数据协作等工作。数据处理规则可配置并具有开放性，确保可以根据行业规范细则的变化对自评估流程与政策进行同步调整。平台支持在数据安全评估后直接进行脱敏匿名数据，无限制数据直接跨境。对于不能够直接出境的数据，根据车联网数据用户对数据使用范围和使用目的的授权约定，勤达睿数据跨境平台在不传输任何原始数据的前提下，由境外数据需求方请求相关的模型计算，通过模型源或数据源的加密分片、及算法源的相关配置，实现车联网数据的密文分片交互计算，境外数据需求方在不获取原始数据的前提下，可以直接通过数据唯一的哈希值溯源确认数据质量，可以直接获取密文计算结果，确保数据可用不出境及数据有效性，未被篡改，实现跨主体跨境的数据使用。

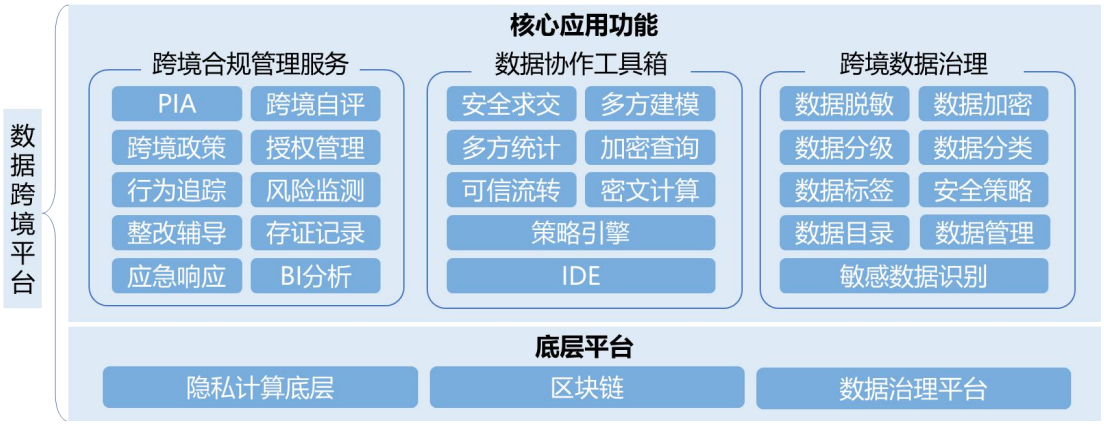

图 3.9-2 数据跨境平台结构图

3.9.3. 案例应用成效

图 3.9-3 数据跨境合规治理流程图

该方案结合了线下合规管理与线上技术创新，提供了从车联网数据跨境的框架体系和路径规划，到流程制度的治理、合规风险治理并最终落地到平台工具的一站式服务。车联网数据跨境方案融合了区块链和隐私计算，其中，区块链技术保证跨境数据的一致性和透明度，用隐私计算来保证境内原始数据不泄露，以同态加密、差分隐私等其他密码学技术为辅助的成熟技术体系，对数据进行分析计算，有效提取数据价值。方案从咨询到技术实施，完整地实现了车联网数据跨境全生命周期的管理，解决了车联网数据跨境的安全风险、合规风险和管理低效的问题，使车企在数字全球化浪潮中，更自如地掌控车联网数据的跨境流转和更高效的使用。

3.10. 数据流通基础设施：跨国企业跨境数据中心建设方案

顺丰协助某跨国企业（以下简称“客户”）通过建设以国内及海外两个一级数据中心、多个海外二级数据中心的大型跨境数据中心及跨境数据中心平台，解决其跨境业务的数据合规、安全管理等难题。

3.10.1. 案例实施背景

客户总部位于中国大陆，业务遍布全球五大洲。近几年，客户跨境业务面临着新的挑战：一方面，随着欧盟 GDPR、美国 UPDPA 等数据保护法案法规的相继出台，全球隐私合规条例愈发趋严，境外其它国家原始明细数据存储在中国大陆境内存在合规风险，有必要构建独立运作的境外数据中心，境外数据中心也需要基于境外国家的合规政策进行改造，以满足当地的合规要求。另一方面，随着业务的拓展和用户的快速递增，原有数据中心无法满足企业需求，希望通过重建海外数据中心实现数据流通、数据入境合规、安全且数据分析应用方便、高效等目标。

3.10.2. 技术方案介绍

（1）跨境数据中心布局架构

根据业务分布建设两个一级数据中心(国内一级业务中心、海外一级业务中

心)及多个海外二级业务中心。考虑到政策和地域访问响应速度等因素，国际业务系统在某公有云上采用多域部署，国内业务系统部署在混合云上。海外合规脱敏业务数据统一传输至海外一级数据中心。在满足合规要求前提下，海外业务合规脱敏数据自海外一级数据中心同步至国内一级数据中心。

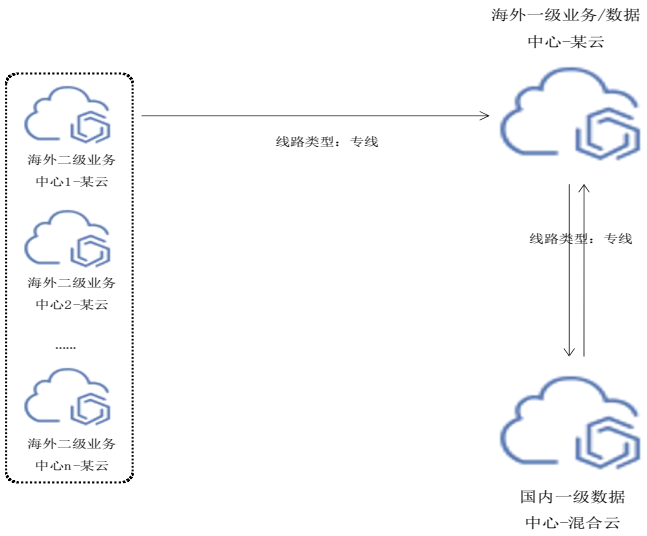

图 3.10-1 跨境数据中心布局架构图

（2）跨境数据中心平台建设原则

综合考虑企业的业务布局及管理需求，跨境数据资产管理平台的建设以“四个统一”为原则，即：

1） 统一数据管理，数据体系、元数据、指标口径、数据安全等进行统一管理；

2） 统一权限管理，系统权限、功能权限，数据权限的严格管控；

3） 统一大数据底盘，多地域统一建设的大数据底盘、统一的大数据管理门户；

4） 统一基础架构，多云混合的数据中心基础架构。

（3）跨境数据中心平台基础架构

平台架构则自底向上分为 4 层：资源层、通信层、服务层和产品层，如图 3.10-2 所示：

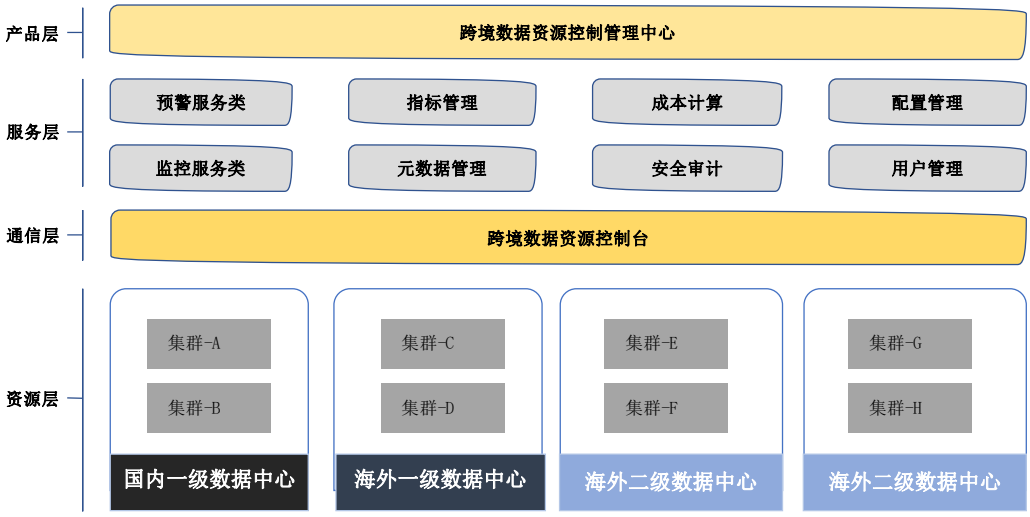

图 3.10-2 跨境数据中心平台基础架构图

1） 资源层：包括两个一级数据中心(国内、海外)和多个海外二级业务中心，如图 3.10-3 所示；

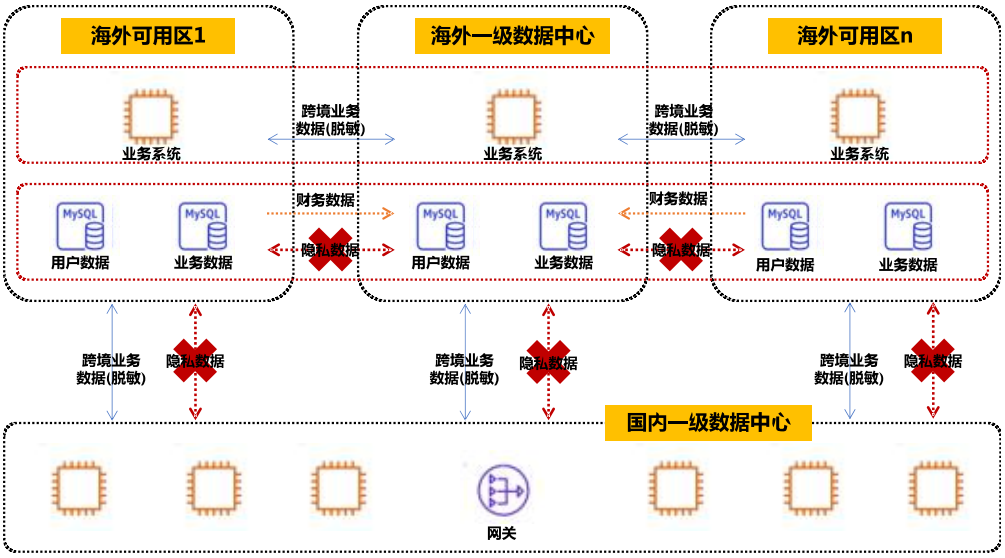

图 3.10-3 跨境数据中心平台资源层结构图

2） 通讯层：负责数据接入和传输，通过专业工具快速识别敏感数据，并进行敏感数据标识，在数据接入前设置审核节点，进行数据迁移审批，规避数据跨境同步的法律风险；

3） 服务层：一方面对数据资源进行统一数据管理，数据权限、数据体系、元数据、指标口径、数据安全等进行统一管理；另一方面，为上层的产品应用层，提供统一大数据底盘能力服务；

4） 产品层：面向业务应用体系提供与之相匹配的数据服务。

（4）跨境数据传输合规管控

业务数据传输分为海外本地业务数据及跨境业务数据两种类型，并遵从不同的数据传输原则。

图 3.10-4 跨境数据传输流程图

如图 3.10-4，为符合 GDPR 及境外相关合规条例要求，规避因误操作导致的明细数据回流带来的风险，通过专业工具快速识别敏感数据，并进行敏感数据标识，在数据接入前设置审核节点，进行数据审批，防范数据跨境同步的法律风险。

3.10.3. 案例应用成效

客户跨境数据中心落地运行过程中，从数据采集、数据存储、数据使用方式等均满足业务当地的合规要求；客户国内总部对全球业务及数据的管理效率得到极大提升。

在该跨境数据中心建设案例中，两个一级数据中心及多个二级数据中心的布局架构设计，及针对数据传输过程中所采取的技术工具及传输路径均实现数据采集地和数据落地国家的数据合规。

第四章 我国跨境数据流通合规与技术应用建议

随着数字经济时代的到来，数据跨境已成为全球发展的必然趋势。为促进数据跨境流动、保护数据跨境安全，我国制定并颁布的数据领域的法律、法规、规章及标准中，均对数据跨境予以规定。同时，应充分发挥技术保障作用，运用技术手段构建安全风险防控体系，促进数据安全有序跨境流通。

4.1. 法律合规层面

我国当前数据跨境的合规体系，包括了《网络安全法》《数据安全法》《个人信息保护法》三部法律，这奠定了我国对于规制数据跨境行为的立法态度及总体指引；另外，2022 年，国家互联网信息办公室公布了《数据出境安全评估办法》及《数据出境安全评估申报指南（第一版）》，进一步细化并明确了数据跨境的相关规定。围绕以上数据跨境合规体系，建议如下：

（1）确定拟出境的数据是否为需申报的数据类型

重要数据和符合条件的个人信息出境前需主动申报。从我国向境外提供数据，需要进行数据出境安全评估申报的数据类型有两类：一类是重要数据，另一类是满足条件的个人信息。如图 4.1-1 所示：

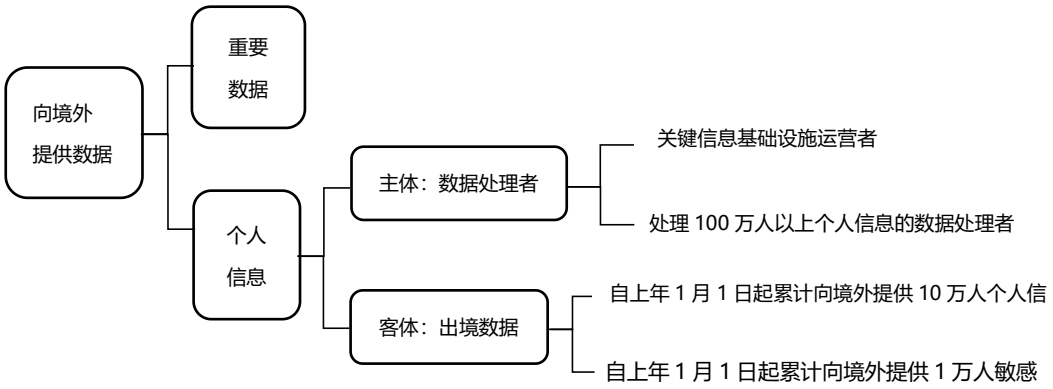

图 4.1-1 需进行数据出境安全评估申报的数据类型

从立法层面来看，我国已明确规定数据出境前需主动申报的数据类型及相关情形；但从实践角度来看，如何判断待出境的数据是否为重要数据仍具有不确定性。我国《数据安全法》第 21 条规定，国家数据安全工作协调机制统筹有关部门制定重要数据目录，但目前相关部门并未出台重要数据目录。2022 年 1 月 13 日，全国信息安全标准化技术委员会公布了国家标准《信息安全技术 重要数据识别指南（征求意见稿）》，该意见稿从数据泄漏的后果角度确定了重要数据识

别因素及基本原则。总体而言，当前虽已明确重要数据出境需进行申报，但识别重要数据的具体标准仍有待明确。

（2）合规开展数据出境风险自评估与数据出境安全评估工作

如为需申报的数据类型，数据出境前，数据处理者应按照合规要求，完成数据出境风险自评估及数据出境安全评估。数据处理者应首先开展风险自评估，在完成风险自评估后继而申报数据出境安全评估。数据出境风险自评估与数据出境安全评估的重点评估事项大体相同，主要考核评估以下几个方面：1）客体角度：出境数据本身，包括规模、范围、种类、敏感程度、潜在风险；2）行为角度：数据出境行为，主要指数据出境的目的、范围、方式等是否合法正当必要；3）主体角度：境外接收方，包括境外接收方当地的保护政策及保护水平是否达到我国标准；4）技术保障角度：数据出境中及出境后数据安全和个人信息权益保护途径是否畅通有效；5）法律文件角度：与境外接收方拟订立的数据出境相关合同或其他法律文件。

4.2. 技术应用层面

（1）数据分类分级技术帮助企业梳理出境数据

《数据出境安全评估办法》明确指出，企业在数据出境过程中，需要评估出境数据的规模、范围、种类、敏感程度。随着企业的数据资产规模越来越大，基于人工梳理方式的分类分级工作投入巨大，已经无法满足企业安全合规的要求。因此，企业需要建立（半）自动化数据分类分级体系，定期梳理出境数据资产，数据识别技术能够识别个人隐私数据和行业重要数据，依照各行业标准、国家标准、地方标准等（见附录），将识别的数据与数据分类和安全等级进行关联。

（2）数据脱敏去标识化保证敏感数据最小使用和安全防护原则

数据脱敏或去标识化是指对敏感信息通过脱敏规则进行数据的变形，实现敏感隐私数据的可靠保护。个人信息去标识化过程一般涉及个人数据预处理，数据去标识化，去标识化结果评级这几个阶段。数据预处理阶段可以采用数据抽样，减小数据集的规模，减少结果集中的个人信息。数据去标识化阶段可以采用统计技术、密码技术、抑制技术、假名化技术、泛化技术、随机化技术、数据合成技术等。去标识化评级则是对结果集进行重标识风险评估，需要根据个人信息的公开程度、环境的安全风险等级等因素进行综合判断，得出 1-4 级的等级，级别越高则代表去标识化程度越高，重标识风险越低。

（3）数据安全网关构建安全可控的数据出境链路

境外系统可能通过 API 接口的方式访问境内数据中心，在此过程中为了合法合规，一般需要引入数据安全网关对接口进行纳管。数据安全网关能够对涉及

敏感数据流量接口进行识别，并对敏感数据接口的动态防护，通过对相关调用进行脱敏、拦截、限流、限频等事中控制措施，确保个人隐私数据、行业重要数据得到安全保障。

（4）数据安全加密技术保障出境数据存储安全

针对出境业务数据，数据处理者应当在与境外接收方订立的法律文件中明确约定数据安全保护责任义务，包括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。为确保数据在存储侧的安全，需要数据存储加密技术，一方面对数据库存储层透明加密，另一方面对应用层的数据进行加密。

（5）隐私计算保护数据出境场景中的原始信息

隐私计算是指在保证数据提供方不泄露原始数据的前提下，对数据进行分析处理与计算的一系列信息技术，保障数据在流通与应用过程中“可用不可见”。隐私计算由于其技术特性，可在数据跨境场景中提供原始数据不出域的解决方案。通过跨境部署的隐私计算节点间的密文计算来完成重要或个人隐私数据分析目标，从而实现安全的数据交互，为保证数据出境信息的最小化提供一种技术路径。

（6）基于区块链存证的出境事件稽核溯源

区块链存证在数据要素流通场景上，可将数据在采集、存储、流通、分析、应用等各个环节的行为进行存证上链，达到防篡改、可追溯、可信任的目的。在数据跨境的场景中，涉及重要数据、个人数据等敏感信息需要评估与审查后，方可实施数据出境，但数据送审与数据出境是不同的行为，可能存在送审数据与出境数据不一致的情况。而区块链技术可对数据全程进行存证与溯源，可确保送审数据与出境数据的一致性，并可以对其数据使用目标、使用范围等信息进行存储，为后续的数据审计提供有效的技术保障。

参考文献

[1] 李昀谖. 数字贸易中跨境数据流动法律规制问题的研究[D].甘肃政法大学

[2] 张茉楠.跨境数据流动：全球态势与中国对策[J].开放导报,2020(02):44-50.

[3] 赵高华,姜伟,王普.数据跨境流动治理与对策研究[J].网络安全与数据治理 2022,41(09):23-27.

[4] 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.

[5] 李艳.有效应对数据跨境流动规则挑战[N]. 中国社会科学报，2022-10-13(005).

[6] 中国企业如何实践业务价值驱动型安全投资 Mia Yu, Paul Proctor, Jie Zhang, Anson Chen (G00775329)

[7] https://www.ogcio.gov.hk/sc/our_work/business/industry_support/ict_hub.html

[8] http://finance.people.com.cn/n1/2019/0422/c1004-31041928.html

[9] https://beltandroad.hktdc.com/tc/insights/hong-kong-digital-silk-road-super-hub

[10] https://www.news.gov.hk/chi/2021/12/20211208/20211208_132755_301.html

[11] 《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》

[12] https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=TC&refNo=22EC69

[13] https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20141229.html

[14] https://www.gov.mo/zh-hans/entity-page/entity-59/

[15] 彭岳. 数据隐私规制模式及其贸易法表达[J].法商研究，2022 年 05 期.

[16] https://mp.weixin.qq.com/s/MuYsf_wFEM1ajQQQBcUYkA

[17] 赛智时代.《中欧美数据跨境流动研究》,2020 年 11 月 3 日.

[18] 陈海彬,王诺亚.日本跨境数据流动治理研究[J].情报理论与实践, 2021,44(12):197-204.DOI:10.16353/j.cnki.1000-7490.2021.12.025.

[19] 张晓磊.日本跨境数据流动治理问题研究[J].日本学刊,2021(S1):155.

[20] 于晓,叶申南.欧日韩数字经济政策、发展趋势及中国策略[J].财政科学,2021(06):135-141.DOI:10.19477/j.cnki.10-1368/f.2021.06.015.

[21] 邓灵斌.日本跨境数据流动规制新方案及中国路径——基于“数据安全保障”视角的分析[J].情报资料工作,2022,43(01):52-60.

[22] 野村综合研究所/中国信通院报告书联合报告书《中日数字产业的合作与展望》

[23] 王念.新加坡数据跨境流动管理的经验与启示[J].财经智库，2020 年 04 期.

[24] 张伯超.数据跨境流动的全球标杆城市：新加坡[J].上海信息化,2021(03):54-56.

[25] 张敖,王欢雪.新加坡个人数据跨境流动安全规制及执法实例分析[J].中国标准化,2022(20):47-50.

[26] 梁正,张栋,于洋.数据出境安全治理国际经验比较与启示[J].中国信息安全,2022(03):57-60.

附录 A：数据跨境流通域外法律解析

1. 香港

1.1. 香港数据跨境的规定及简析

1.1.1. 《保障个人资料：跨境资料转移指引》与建议合约条文范本简析

（1）《保障个人资料：跨境资料转移指引》对法律规定的概要[6]

根据《保障个人资料：跨境资料转移指引》（以下简称“《指引》”）：“《私隐条例》的保障数据第 3 原则旨在针对不当使用个人资料的情况。该原则订明，除非获得资料当事人的订明同意，否则个人资料不得用于新目的。「新目的」主要是指原本收集数据之目的或与其直接有关的目的以外之任何目的。「订明同意」指资料当事人明确和自愿给予及没有以书面撤回的同意，而「使用」指引数据报括披露及转移数据。因此，如为新目的而把个人资料转移至香港以外的地方，除非有关转移是属于《私隐条例》第 8 部下的豁免范畴，否则保障数据第 3 原则规定需要就有关转移获得数据当事人的订明同意。”

《私隐条例》在跨境数据转移规定的适用范围包括：如数据用户聘用数据处理者在香港境外代为处理个人资料，该资料用户须采取合约规范方法或其他方法以保障个人资料；数据用户在转移数据到香港境外的同时亦需要确保符合《私隐条例》的规定。

（2）范本的适用范围

公署提供给了两套范本，分别供两种不同的跨境数据转移的情况应用，包括：

第一套：由一个数据用户转移个人资料予另一个数据用户的情况，当中数据转移者和数据接收者均分别使用有关个人资料作其业务用途；

第二套：由数据用户转移个人资料予数据处理者的情况，当中数据接收者只会为数据转移者指定的用途处理个人资料。

（3）第一套《范本》的主要要求：

根据《指引》，第一套《范本》要求资料接收者（即一名香港境外的数据用户）应遵从的建议最佳行事方式，并把下述的要求纳入于合约中：

1) 只为与数据转移者协议的转移目的（或直接有关的目的）及数据转移者原本收集有关个人资料的目的使用个人资料，但《私隐条例》容许更广阔的使用范围则除外（第 4.1 条）；

[6] https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/guidance_model_contractual_clauses.pdf

2) 确保就与数据转移者协议的转移目的（或直接有关的目的）而言，个人资料属足够但不超乎适度（第 4.2 条）；
3) 采取协议并载列于数据用户转移数据予数据用户的建议合约条文模板的数据转移一览表中的保安措施使用个人资料（第 4.3 条）；
4) 保留个人资料的时间只会是达致转移目的所需的时间或双方协议的特定保留时期（第 4.4 条）；
5) 采取所有切实可行的步骤，在保留时期届满或不再需要保留转移的个人资料时，删除有关数据（第 4.5 条）；
6) 采取所有切实可行的步骤，以确保在顾及与数据转移者协议的转移目的（或直接有关的目的）下，个人资料是准确的（第 4.6 条）；
7) 采取所有切实可行的步骤，以确保任何不准确的个人资料（i）在更正前不会被使用或（ii）会被删除（第 4.7 条）；
8) 采取所有切实可行的步骤，以确保资料当事人能查阅其有关个人资料的政策及做法（第 4.8 条）；
9) 不会继续转移个人资料予任何第三方，但双方在数据转移一览表作出协议或数据转移者给予同意则除外（第 4.9 条）；
10) 确保继续转移个人资料是符合数据用户转移数据予数据用户的建议合约条文模板或数据用户转移数据予数据处理者的建议合约条文范本的规定（如适用）（第 4.10 条）；
11) 不会继续转移个人资料至任何其他司法管辖区，但双方有协议则除外（第 4.11 条）；
12) 就数据当事人的查阅及改正数据权利，履行作为数据用户的责任（第 5 条）；及
13) 在收到数据转移者有关停止使用个人资料作直接促销的书面通知后，履行其责任停止该等行为，但《私隐条例》容许如此直接促销则除外（第 6 条）。

（4）第二套《范本》的主要要求

根据《指引》，第一套《范本》要求数据转移者（作为一名数据用户）有责任遵从《私隐条例》的要求，以确保数据处理者依从《私隐条例》的规定，并要求数据处理者的接收数据一方满足以下要求：

1) 只为数据转移者指示的目的（或直接有关的目的）及资料转移者原本收集有关个人资料的目的处理个人资料（第 3.1 条）；
2) 确保就数据转移者指示的目的（或直接有关的目的）而言，个人资料属足够但不超乎适度（第 3.2 条）；

3) 采取协议的保安措施处理个人资料，正如数据用户转移数据予数据处理者的建议合约条文模板中的数据转移一览表所载列（第 3.3 条）；
4) 保留个人资料的时间只会是达致数据转移者指示的目的（或直接有关的目的）所需的时间或任何协议特定的保留时期（第 3.4 条）；
5) 采取所有切实可行的步骤，在保留时期届满或不再需要保留个人资料时（或按数据转移者的指示），删除有关资料（第 3.5 条）；
6) 采取所有切实可行的步骤，以确保在顾及数据转移者指示的目的（或直接有关的目的）下，个人资料是准确的（第 3.6 条）；
7) 采取所有切实可行的步骤，以确保任何不准确的个人资料（i）在更正前不会被处理或（ii）会被删除（第 3.7 条）；
8) 不会继续转移个人资料予任何第三方，但双方在数据转移一览表作出协议或数据转移者给予同意则除外（第 3.8 条）；
9) 确保若继续转移个人资料予任何第三方，会符合数据用户转移数据予数据处理者的建议合约条文范本的规定（第 3.9 条）；及
10) 不会继续转移个人资料至任何其他司法管辖区，但有数据转移者事前的书面同意则除外（第 3.10 条）。

1.2. 《个人资料（私隐）条例》与《个人信息保护法》部分要点对比分析

序号	对比项目/内容	《个人资料（私隐）条例》	《个人信息保护法》	对比分析
1	个人信息	**个人资料** (personal data) 指复合一下说明的任何资料——(a)直接或间接与一名在世的个人有关的；(b)从该资料直接或间接地确定有关的个人的身分是切实可行的；及 (c)该资料的存在形式令予以查阅及处理均是切实可行的；	**第四条** 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。	中国境内关于个人信息的定义以识别和关联为依据，更为广泛，香港需要能识别出具体个人。应注意香港未对匿名化处理后的信息做规定
2	个人信息处理者	**1.资料使用者** (data user)，就个人资料而言，指独自或联同其他 人或与其他人共同控制该资料的收集、持有、处理或使用的人； 2.如某人纯粹代另一人持有、处理或使用的任何个人资料，而该首述的人并非为其任何本身目的而持有、处理或使用（视属何情况而定）该资料，则（但亦只有在此情况下）该首述的人就该个人资料而言不算是资料使用者。 3.**资料处理者** (data processor) 指符合	**第七十三条** 本法下列用语的含义： （一）个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。 **第二十一条** 个人信息处理者委托处理个人信息的，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督。	中国境内个人信息处理者的含义与香港资料处理者的定义有明显区别，香港和境内个人信息处理者相似的概念为资料使用者，而资料处理者更偏向于境内受托处理个人信息的角色。

		以下两项说明的人 —— (a) 代另一人处理个人资料；及 (b) 并不为该人本身目的而处理该资料。		
3	敏感个人信息	未做明确规定	第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。	**低于中国境内保护水平**，境内对敏感个人信息做出了特别规定，对敏感个人信息需要有更高的保护水平，香港未做出明确规定
4	同意	根据第 30 条、第 35 条、第 64 条、附表 1 第一原则、第三原则等的规定，香港只在核对程序、直接促销、披露、将个人资料用于新目的等少数情况下才需要征得个人同意	根据第十三条、第十四条等的规定，在无十三条第一款（二）至（七）的情形下，处理个人信息前均需取得个人同意。	**低于中国境内保护水平**，境内处理个人信息以告知同意为基础，特殊情况下需要单独同意或书面同意。
5	本地化存储	未做明确规定	第三十六条及第四十条规定，国家机关、关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。	**低于中国境内的保护水平**，境内对特殊主体的本地化存储有明确要求，香港未有明确规定

6	罚款力度	香港关于违反《个人资料（私隐）条例》的散见于条例中，处罚系针对具体某一行为规定的，最高罚款金额为 100 万。	第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	**香港在罚款力度低于中国境内保护水平**，境内最高可处以五千万元以下或者上一年度营业额百分之五以下罚款
7	合法性基础/豁免	第 8 部豁免规定了 21 种豁免情形，分	第十三条规定了七种可以合法处理个人信息的	**与境内保护水平持平**

		别是执行司法职能、家居用途、雇佣-职工策划、雇佣-过渡性条文、有关程序、个人评价、关于香港的保安等、罪行等、《截取通讯及监察条例》所指的保护成果及有关记录、健康、未成年人的照顾及监护、法律专业保密权、导致自己入罪、法律程序等、新闻、统计及研究、第 18（1）（a）条的豁免、人类胚胎等、尽职审查、危急处境及转移记录于政府档案处，每种情形所针对的豁免范围由具体条款予以规定	情形，分别是取得个人的同意；为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需；为履行法定职责或者法定义务所必需；为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需；为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息；法律、行政法规规定的其他情形。 第七十二条规定了两种豁免情形，不适用个人信息保护法，分别是自然人因个人或者家庭事务处理个人信息的；法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的。	虽然香港对于豁免情形规定得更多更具体，其中如雇佣、个人评价、《截取通讯及监察条例》所指的保护成果及有关记录、法律专业保密权、尽职审查等情形是中国境内未做具体规定得，但境内的规定在外延上可能会大于香港规定。

2. 澳门

2.1. 《澳门特别行政区个人资料保护法》与《个人信息保护法》要点对比分析

序号	对比项目/内容	《澳门特别行政区个人资料保护法》	《个人信息保护法》	对比分析
1	敏感个人信息范围	第七条 敏感资料的处理 一、禁止处理与世界观或政治信仰、政治社团或工会关系、宗教信仰、私人生活、种族和民族本源以及与健康和性生活有关的个人资料，包括遗传资料。 二、在保障非歧视原则以及第十六条所规定的安全措施的前提下，得对上款所指的资料在下列任一情况下进行处理： （一）法律规定或具组织性质的规章性规定明确许可处理上款所指的资料； （二）当基于重大公共利益且资料的处理对负责处理的实体行使职责及权限所必需时，经公共当局许可； （三）资料当事人对处理给予明确许可。 三、当出现下列任一情况时，亦得处理第一款所指的资料：	第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。 只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，个人信息处理者方可处理敏感个人信息。	**低于与中国境内保护水平，**澳门特别行政区法律与中国境内法律对比，中国大陆法律规定的敏感个人信息更广，更严格，特别是增加了对未成年人的保护。

		（一）保护资料当事人或其他人重大利益所必需，且资料当事人在身体上或法律上无能力作出同意； （二）经资料当事人同意，由具有政治、哲学、宗教或工会性质的非牟利法人或机构在其正当活动范围内处理资料，只要该处理仅涉及这些机构的成员或基于有关实体的宗旨与他们有定期接触的人士，且有关资料未经资料当事人同意不得告知第三人；		
	敏感个人信息范围	（三）要处理的资料明显已被资料当事人公开，只要从其声明可依法推断出资料当事人同意处理有关资料； （四）处理资料是在司法诉讼中宣告、行使或维护一权利所必需的，且只为该目的而处理资料。 四、如处理与健康、性生活和遗传有关的资料是医学上的预防、诊断、医疗护理、治疗或卫生部门管理所必需的，只要由负有保密义务的医务专业人员或其他同样受职业保密义务约束的人进行，并根据第二十一条规定通知公共当局和采取适当措施确保信息安全，得处理有关资料。	同上	同上
2	对企业的行政处罚	第三十二条 履行义务的不作为或有瑕疵的履行 一、基于过失，实体未履行第二十一条第一款和第五	第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定	**低于中国境内的保护水平**中国境内法律对违反

		款规定的将个人资料的处理通知公共当局的义务、提供虚假信息或履行通知义务时未遵守第二十三条的规定，或者经公共当局通知之后，负责处理个人资料的实体继续让没有遵守本法规定者查阅其传送资料的公开网络，属行政违法行为并处以如下罚款： （一）对自然人科处澳门币 **2,000 至 20,000 元罚款；** （二）对法人或无法律人格的实体，**科处澳门币 10,000 至 100,000 元罚款。** 二、当处理的资料根据第二十二条规定受预先监控约束时，**罚款的上下限各加重一倍**	的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；**拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。** 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，**并处五千万元以下或者上一年度营业额百分之五以下罚款**，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；**对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款**，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	个人信息保护义务的企业处罚力度更大、处罚额度更重。
3	对直接负责的主管人员和其他直接责任人员的行政处罚	未做规定		**低于中国境内的保护水平**中国境内的个人信息保护法规定了对企业直接负责任等的行政处罚，但澳门并未做规定

3. 美国

3.1. 中美个人信息保护要点对比分析

序号	对比内容/项目	域外规定		《个人信息保护法》	对比分析
		《加州消费者隐私法案》CCPA	《加州隐私权法案》CPRA		
1	管辖范围	美国 CCPA/CPRA 均为州级立法，适用于处理加利福尼亚州消费者（居民自然人）个人信息的情形。CCPA 和 CPRA 的执行机关分别为：加州总检察长办公室、加州隐私保护局。		《中华人民共和国个人信息保护法》第三条 在中华人民共和国境内处理自然人个人信息的活动，适用本法。 在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动，有下列情形之一的，也适用本法： （一）以向境内自然人提供产品或者服务为目的； （二）分析、评估境内自然人的行为； （三）法律、行政法规规定的其他情形。	**低于中国境内保护水平** 中国《个人信息保护法》相较于美国 CCPA/CPRA，适用的地域范围及受保护的主体范围均更为广泛。
2	适用主体	在加利福尼亚州开展相关业务收集加州消费者个人信息的营利性实体，其本身及其母公司或者子公	在加利福尼亚州开展相关业务收集加州消费者个人信息的营利性实体，其本	《中华人民共和国个人信息保护法》第九条 个人信息处理者应当对其个人信息处理活动负责，并采取必要措施保障所处理的个人信息的安全。	**低于中国境内保护水平** 中国《个人信息保护法》受规制的实体类型，包括个人信息处理者和个人信

		司，满足下列情形之一的，需要遵守 CCPA 所规定的各项要求： （1）年总收入超过 2500 万美元； （2）基于商业目的，每年单独或合计购买、接收、出售或分享超过 5 万消费者、家庭或设备的个人信息； （3）年收入的 50%或以上来自于出售消费者个人信息。	身及其母公司或者子公司，满足下列情形之一的，需要遵守 CPRA 所规定的各项要求： （1）年总收入超过 2500 万美元； （2）基于商业目的，每年单独或合计购买、接收、出售或分享超过 10 万消费者、家庭或设备的个人信息； （3）年收入的 50%或以上来自于出售消费者个人信息。	《中华人民共和国个人信息保护法》第五十九条 接受委托处理个人信息的受托人，应当依照本法和有关法律、行政法规的规定，采取必要措施保障所处理的个人信息的安全，并协助个人信息处理者履行本法规定的义务。	息的受托人；而美国 CCPA/CPRA 仅规制符合一定条件的企业。
3	敏感个人信息	未规定敏感个人信息。	企业须向消费者披露如何收集、使用其敏感个人信息，消费者可以要求企业停	《中华人民共和国个人信息保护法》第二十八条 敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人	**与中国境内保护水平持平。** 虽然 CCPA 未对敏感个人信息作出规定，但 CPRA

			止出售、共享和使用该等信息。 敏感个人信息包括： （1）显示社会保障、驾驶执照、州身份证或护照号码的信息； （2）帐户登录、金融帐户、借记卡或信用卡号以及访问代码、密码或凭据； （3）精确定位； （4）种族或族裔血统、宗教或哲学信仰或工会会员身份； （5）邮件、电子邮件和短信的内容； （6）基因数据； （7）用于识别某人的生物特征信息； （8）收集和分析的	信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。	新增对敏感个人信息的规定，并予以细化分类。中国《个人信息保护法》亦规定了敏感个人信息的定义及分类

			有关个人健康、性生活或性取向的信息。		
4	处理活动	美国 CCPA/CPRA 仅包括收集、出售、共享的数据处理活动。		《中华人民共和国个人信息保护法》第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的**收集、存储、使用、加工、传输、提供、公开、删除等**。	**低于中国境内保护水平** 中国《个人信息保护法》适用的数据活动包括个人信息的全流程处理活动，而美国 CCPA/CPRA 仅包括收集、出售、共享。
5	不属于个人信息的清形	美国 CCPA/CPRA 对于个人信息的定义排除了： （1）去识别化信息； （2）汇总的消费者信息； （3）可公开获取的信息； （4）合法获得的、引起公众关注的真实信息。		《中华人民共和国个人信息保护法》**第四条** 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，**不包括匿名化处理后的信息。**	**低于中国境内保护水平** 《个人信息保护法》对于个人信息的定义仅排除了匿名化信息。美国 CCPA/CPRA 对于个人信息的定义排除了去识别化信息、汇总的消费者信息、可公开获取的信息以及合法获得的、引起公众关注的真实信息，对个人信息的定义进行了限缩。

6	合法性基础	美国 CCPA/CPRA 规定的合法性基础仅适用于企业收集、出售和披露个人信息的场景。	《中华人民共和国个人信息保护法》第十三条第一款 符合下列情形之一的，个人信息处理者方可处理个人信息： （一）取得个人的同意； （二）为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需； （三）为履行法定职责或者法定义务所必需； （四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需； （五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息； （六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息； （七）法律、行政法规规定的其他情形。	**高于中国境内保护水平** 中国《个人信息保护法》规定的合法性基础更为广泛，而美国 CCPA/CPRA 仅适用于企业收集、出售和披露个人信息的场景。

				依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。	
7	同意机制	美国 CCPA/CPRA 采取选择退出模式(opt-out)为主要机制。		在同意机制方面，中国采取须取得信息主体同意(opt-in)的模式。《个人信息保护法》第十三条第二款 依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。	**低于中国境内保护水平** 在同意机制方面，中国《个人信息保护法》采取须取得信息主体同意(opt-in)的模式，而美国 CCPA/CPRA 采取选择退出模式(opt-out)为主要机制。
8	救济途径	强调私权利的救济。当缺乏合理的安全措施导致侵权时，消费者可以提出私人诉讼。	强调私权利的救济。在 CCPA 的基础上，如发生数据泄露，包括消费者的电子邮件地址和密码或安全问题，消费者也可提出私人诉讼。	中国强调公权力的救济，国家公权力对于侵犯个人信息的惩处。《中华人民共和国个人信息保护法》第七十条 个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。	**不具备可比性。** 虽侧重点不同，均为对权利的救济。
9	行政处罚力度	（1）一般过失侵权每次处以 2500 美元的罚款，若为故意侵权每次处以最高	（1）特别加重了对 16 周岁以下未成年人的隐私权侵权行	《中华人民共和国个人信息保护法》第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人	**低于中国境内保护水平。** 在处罚力度方面，中国《个人信息保护法》的处罚力

		7500 美元的罚款。 （2）给予企业在接到总检察长发出涉嫌违规行为的正式通知后30日补救期的规定。	为的处罚规定。 （2）如涉及对 16 周岁以下未成年人隐私权的侵犯，无论是故意还是过失，均可每次处以最高 7500 美元的罚款。 （3）CPRA 取消了 CCPA 中给予企业在接到总检察长发出涉嫌违规行为的正式通知后 30 日补救期的规定。	信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。	度更大。

3.2. 美国《数据隐私和保护法案》(ADPPA) 进展以及可能对我国企业境外合规工作的影响

3.2.1. 法案背景

2022 年 6 月 3 日，美国众议院和参议院商务委员会的主要成员联合发布《美国数据隐私和保护法案》（American Data Privacy and Protection Act，以下简称“《法案》”）草案文本，这是首份获得两党、两院支持的美国联邦层面规制私营部门的综合性隐私保护法草案。

6 月 22 日，众议院将法案草案交能源和商业委员会消费者保护和商业小组听证，7 月 20 日，能源和商业委员会决定将法案发回修订。本文将结合法案中的与隐私及个人数据保护相关的重要内容，在介绍法案的同时，分析我国企业在未来的合规工作需要注意的细节。

3.2.2. 法案中的重要制度介绍

（1）概念解释

1) covered data：适用数据
   a. 基础内涵：具有可识别性的与个人相联系或者具有合理联系的信息/设备；包括派生数据和唯一标识符。
   b. 例外：适用数据不包括——去标识化数据、员工数据、公开获得的信息。员工数据包括：
      a) 由作为潜在员工的潜在雇主的实体在申请或雇用过程中收集的与潜在员工有关的信息，但这些信息由潜在雇主收集、处理或传输，仅用于与该员工作为该雇主的当前或前工作申请人的身份有关的目的；
      b) 员工的业务联系信息，包括员工的姓名、职位或头衔、业务电话号码、业务地址或业务电子邮件地址，这些信息是由以专业身份行事的员工提供给雇主的，但这些信息的收集、处理或传输仅用于与该员工的专业活动有关的目的；
      c) 雇主收集的与该雇主的员工有关的紧急联系信息，但这些信息的收集、处理或传输仅仅是为了在档案中为该员工建立一个紧急联系方式；或
      d) 与员工（或该员工的亲属或受益人）有关的信息，而这些信息是雇主收集、处理或传输的必要条件，目的是管理该员工（或该员工的

亲属或受益人）因在该雇主任职而有权享受的福利。

c. 去标识化数据：

a) 不具有可识别性，不与个人或设备具有联系或者合理联系的信息。

b) 禁止重标识：要求适用主体保证信息在任何时候都不被重新识别至特定的个人或设备；同时要求适用主体清晰的承诺不从事任何重新识别的行为，并且以合同的方式规制数据流转方的重识别行为。

2) 大型数据持有者的界定

a. 年总收入为[250,000,000 美元]或以上；[和]

b. 收集、处理或传输：

——超过 5,000,000 个人或设备的适用数据，这些设备可以识别、关联或合理地可关联到 1 人或多人；或

——超过 100,000 个人或设备的敏感涵盖数据，这些设备可以识别、关联或合理地可关联到 1 人或多人，不包括适用实体仅因处理下列数据而符合为大型数据持有者要求的情况——个人电子邮件地址、个人电话号码；或个人或设备的登录信息，以允许该个人或设备登录到由适用实体管理的账户。

（2）明示同意制度

1) 基本内容

“肯定的明示同意”是指个人以清晰确定的方式，给予的数据收集主体关于数据的收集、处理和传输等行为以具体、明确的授权。

2) 前提：

a. 同意请求应当清晰、显著地披露在应用/网页等的显目位置；

b. 同意请求应当包括每项行为所收集、处理、传输的数据的具体类型；

c. 同意请求应当区分必要和非必要；

d. 同意请求应当以简单易懂的文字展示，确保数据主体可以理解请求所载的内容；

e. 同意请求应当明示数据主体的有关“同意”的各项权利，如表示同意、拒绝同意、撤回同意等；

f. 同意请求的语言文本应当包含任何可能收集、处理、传输的数据对应之主体所使用的语言；

3) 禁止推定同意

不得从个人的不作为或者继续使用相关产品/服务的行为中推定数据主体给予了“同意”。

4) 禁止事先同意

不得通过一下方式获得或者试图获得数据主体的同意——

a. 使用任何虚假、虚构的、欺诈性的或具有重大误导性的陈述或表述；或
b. 通过设计、修改或操纵任何用户界面，以掩盖、颠覆或损害合理数据主体的自决权。

5) 敏感数据的同意规则

未经同意不得收集处理传输任何敏感数据。敏感数据包括：

a. 个人身份信息，如社会保险号码、护照号码、驾驶照号码；
b. 个人健康信息，包括任何描述个人现在、过去、未来的身体健康、精神健康、疾病、诊断或保健治疗的信息；
c. 个人金融信息，包括金融账户卡密、借记卡、信用卡密码或任何必要的安全或访问代码、密码，或允许访问任何此类账户或卡的凭证。
d. 个人生物识别信息。包括指纹、声纹、虹膜或视网膜扫描、面部或手部的图像、步态或个人识别的身体动作。
e. 个人遗传信息。包括对个人完整提取或部分提取的 DNA 进行检测而得到的原始序列数据或者通过分析原始序列数据得到的基因型和表现型信息。
f. 精确的地理位置信息，表明个人或设备的过去或现在的实际物理位置，可识别或关联或合理关联到一人或多人。
g. 个人的通信信息，包括语音邮件、电子邮件、短信、或识别此类通信方的信息、电话账单中包含的信息、语音通信，以及与传输语音通信有关的任何信息，包括被呼叫号码、呼叫号码、呼叫时间、通话时间，以及通话方的位置信息，除非适用实体是通信的预期接收者。
h. 个人帐户或设备登录凭证信息。
i. 表明个人的种族、民族、国籍、宗教或工会成员或非工会身份的信息，其方式与个人对披露此类信息的合理预期不一致。
j. 识别个人性取向或性行为的信息，其方式与个人对披露此类信息的合理预期不一致。
k. 识别个人在一段时间内的在线活动信息，或跨越第三方网站或在线服务。
l. 保存在个人设备上供私人使用的日历信息、地址簿信息、电话或文本记录、照片、录音或视频，无论这些信息是否被备份在一个单独的位置。
m. 显示个人裸体或穿着内衣的隐私部位的照片、电影、录像或其他类似媒介。
n. 识别或表明任何个人访问或观看或使用其他任何电视服务、有线电视服务或流媒体服务的程度或内容的信息。
o. 【17 岁以下】的儿童和未成年人的个人信息。

p. 为识别上述数据类型而收集、处理或传输的任何其他适用数据。

（3）忠诚义务

1) 最小化原则：

要求适用主体收集、处理、传输数据的行为不得超出合理必要、适当、有限的范围。

2) 禁止和限制的数据处理行为：

a. 除为信贷延期、认证或税务工作外，不得收集、处理、传输个人的社会保险号；

b. 收集、处理受保护的敏感数据，但以下情形除外：收集、处理受保护的敏感数据是为了提供或维持数据主体所需求的特定产品或服务或符合本法第 101 条（b）款 1-10 项规定的目的。

c. 向第三方传输受保护的敏感数据，但以下情形除外：

a) 传输经过数据主体的明示同意；

b) 为履行法律义务或者与法律相关的必要的传输行为；

c) 善意主体为防止个人生命健康危险而为的传输行为；

d) 为保障数据安全、身份验证而为的传输个人生物识别信息的行为；

e) 向指定的密码管理器或专门用于识别跨网站或账户重复的适用实体传输密码类敏感信息的；

f) 为医疗诊断、医学研究等目的而为的遗传信息传输行为。

3) 合理定价

a. 适用实体不得拒绝提供服务或者收取不同的价格/费率，

b. 适用实体不得已以个人同意放弃本法案及根据本法案颁布的其他法规所保障的隐私相关权利作为提供产品或服务的条件；

c. 适用实体不得以个人拒绝放弃隐私权利为由拒绝提供产品/服务或者终止服务。

（4）消费者的数据权利

1) 隐私政策的透明度

隐私政策的透明度要求适用实体以清晰、显著和容易获取的方式公开发布隐私政策，并在隐私政策里详细说明数据收集、处理、传输等的相关活动。

a. 隐私政策的内容：适用实体的身份和联系信息；所收集、处理信息的类型和处理目的；是否有数据传输行为（传输的目的、对象）；适用实体保留数据的具体时限；数据主体的具体权利和行权方式；适用实体的安全措施；隐私政策的生效日期；

b. 特殊要求：法案要求，隐私政策必须表明适用主体收集的数据是否传输、提

供或以其他方式提供给中国、俄罗斯、伊朗、朝鲜。

c. 大型数据持有者的简短声明：法案要求，大型数据处理者除了上述隐私政策外，还应当向用户提供一份简短声明，声明应当简洁、清晰、易于访问；声明内容包括对个人权利和披露的概述；声明字数应不超过 500 字。

2) 数据的访问、纠正、删除和可携带权

a. 权利内容：

可携带权：法案规定，在技术上可行的情况下，适用主体可以通过以下形式输出其处理的用户个人数据：个人可以从互联网上下载的可读格式；或者是可携带的、结构化的、可交互操作的、机器可读的格式。

b. 权利行使：

法案规定，适用主体应当向个人提供行使上述相应数据权利的机会，就费用而言，法案固定需要给予用户免费行使相应权利的机会（12 月内 2 次机会）；在免费的机会之外，允许适用主体向个人收取行使数据权利的合理费用。

c. 权利实现：

大型数据持有者应当在用户发出请求后 30 天内完成相应访问、纠正、删除等的请求；不属于大型数据持有者的主体应当在用户发出请求后的 60/90 天内完成相应请求。

3) 儿童保护

a. 禁止向儿童和未成年人（17 岁以下）推送定制化广告服务。

b. 对于年龄在 13-17 岁之间的用户相关的任何个人数据传输行为，应当经过其本人或其父母、监护人的明示同意。

c. 法案规定将成立专门的青少年隐私和营销部门，处理儿童隐私保护和控制针对儿童的营销行为。

4) 第三方收集

a. 法案要求，第三方收集实体的应向美国的专门部门登记并注册。满足登记的条件是作为第三方收集主体处理超过 5000 人以上的数据信息。

b. 美国将建立统一的第三方收集实体登记网站，供公民公开检索、查询所有登记的第三方收集主体的信息，并使个人可以便利的通过该网站行使相应的数据权利。网站内设置专门的“不收集”系统，个人通过身份验证后即可通过该系统向第三方收集主体发送不收集信息的请求，并要求相关主体删除未经其明确同意而收集的信息。

5) 禁止算法歧视

a. 该义务要求适用主体在收集、处理、传输数据时，不得因种族、肤色、宗教、民族血统、性别、性取向或残疾而歧视用户，导致其无法平等的

享受适用主体提供的产品或服务。

b. 法案要求适用主体应当定期完成算法影响评估和算法设计评价，算法设计评价应当交由外部独立审计师或研究人员完成。

6) 数据安全保护

a. 数据安全保护的具体措施包括：安全漏洞评估；采取预防和纠正措施并评估相应措施的实施效果；永久性的销毁法律要求删除或者收集、处理、传输目的已经完成的数据；进行员工培训

b. 法案要求企业应当任命一名或多名员工来维护和实施前述的数据安全保护措施。

（5）公司问责

1) 隐私和数据安全官的指定

a. 法案要求，适用主体应当指定一名或多名合格员工担任隐私官、数据安全官；

b. 对于大型数据控制者，法案额外要求再指定一名直降向大型数据控制者首席执行官回报的隐私保护官，由其负责大型数据控制者的隐私安全政策、实践的评估和更新、进行员工培训、作为大型数据控制者和执法机构之间的联系人。

2) 隐私影响评估

法案规定，大型数据持有者应当每两年一次进行隐私影响评估，评估内容包括大型数据控制者收集、处理、传输的数据的性质、量级以及对个人隐私构成的潜在风险，评估需要形成书面的评估报告，并经大型数据控制者的隐私官批准。

3.2.3. 对我国企业合规工作的影响

（1）不同的数据分类标准和处理原则

法案对于“covered data”的定义仍以“可识别性”为中心，但是在具体范围上与国内的数据存在较大差异。

一方面，对于员工数据的认定，国内尚未法律/法规明确界定员工数据的性质和范围，对于其的保护一般参照通常的个人信息保护进行。但是美国《数据隐私和保护法》中直接在法案涵盖数据范围内排除了员工数据。我国企业可以参照该法案对员工数据的界定，整理、确认其所拥有的各类员工数据，单独分类，便于后续的合规工作展开。

另一方面，对于去标识化数据的保护，法案强调了禁止重标识的义务。这一点在我国法律中也有明确体现，《信息安全技术 个人信息去标识化指南》中规定去标识化的目标之一就是要控制重标识的风险，“根据可获得的数据情况和应

用场景选择合适的模型和技术,将重标识的风险控制在可接受范围内，确保重标识风险不会随着新数据发布而增加，确保数据接收方之间的潜在串通不会增加重标识风险”。基于控制重标识风险的受控公开共享是平衡数据安全保护与数据流转利用的重要手段，企业应当充分认识到控制重标识风险对于提升企业数据利用效率的重要性，及时跟进相应的技术标准和要求。

除此之外，企业也应注意到该法案中对于敏感信息的界定，其中所包含的与性相关的信息，如性取向、性行为等，并不属于我国目前法律中的敏感信息，因此在数据收集、处理、传输的构成中涉及前述与性相关的数据时，应区分域内域外的不同合规要求。

（2）隐私政策修订

法案在隐私政策透明度部分中明确要求企业应当在隐私政策内明确告知其所收集、处理、传输的数据是否会提供或者以其他方式提供给包括中国、俄罗斯、伊朗、朝鲜在内的国家，企业应当注意这一单独要求，并调整隐私政策中的相关内容。

（3）儿童保护

法案对儿童保护进行了专条规定，明确禁止向 17 岁以下的用户提供定向化广告服务。法案对于定向化广告的定义为：向个人或唯一标识符展示的在线广告，该广告是根据随着时间的推移或在第三方网站或在线服务中收集的涵盖数据得出的已知或预测的偏好、特征或兴趣而选择的。以下情形不属于定向化广告：

1) 根据个人对信息或反馈的具体要求，向个人投放广告或营销。
2) 上下文广告，即根据广告出现的位置和内容显示广告，不会因为不同的观看主体而出现内容变化
3) 仅为衡量或确认广告效果、覆盖范围或频率而处理相关数据。

(1) 公司内部制度

法案对数据控制者内部设立隐私官、数据安全官提出了相应的要求，对于大型数据控制者，法案要求其设立供公司与行政机构联络的，类似于 GDPR 的数据保护官职位，系对公司内控制度建设提出的具体要求。在此方面，可以结合 GDPR 的合规要求展开内控合规的相应工作。

4. 欧洲

4.1. 欧盟 GDPR 处罚案例

GDPR 从生效至 2022 年 6 月 10 日，累计罚款执法案例 1186 件，罚款总额累计 20.4 亿欧元，其中，至少有 65 个针对因违反 GDPR 导致的个人罚款案件，罚款金额从 100 欧元到 6000 欧元不等[7]。2021 年，美国在线零售商亚马逊由于“未遵守数据处理原则，以及其他”，被卢森堡国家数据保护委员会判处 7.46 亿欧元罚款[8]，是迄今为止单笔最高的 GDPR 罚款。同年，字节跳动旗下短视频社交平台 TikTok 由于“不遵守信息义务”违反 GDPR 第 12 条要求，被处以 75 万欧元罚款，成为首个中国企业违反 GDPR 的执法案例。

整体而言，GDPR 生效四年来，呈现出执法案件数量增加、年度罚款总额升高的趋势，如图 A-1、图 A-2 所示。

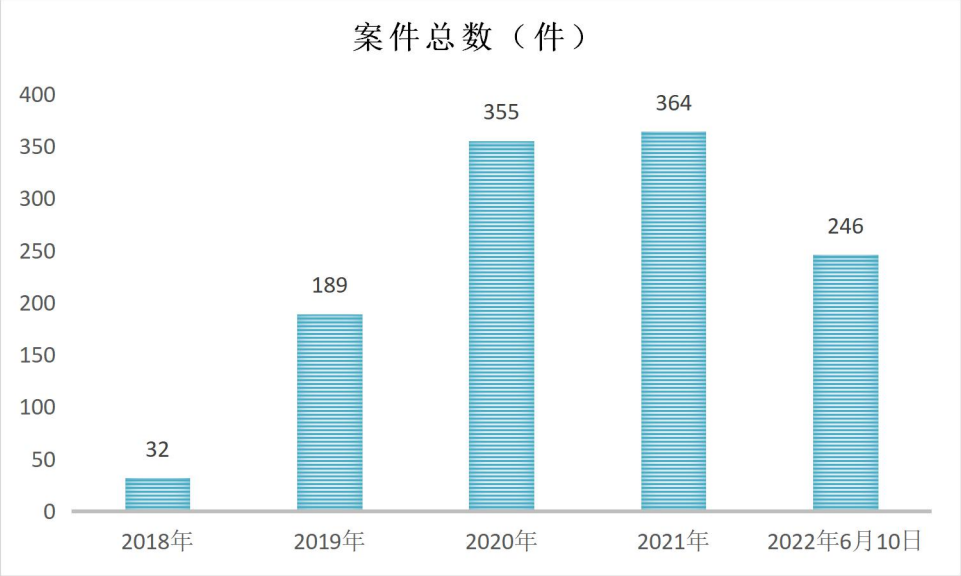

图 A-1 GDPR 执法案件数量走势

[1] Privacy Affairs. At Least 65 Private Individuals Were Fined for GDPR Violations Since 2018［EB/OL］. https://www.privacyaffairs.com/private-individuals-gdpr/.
[2] Privacy Affairs. GDPR Fines Tracker & Statistics［EB/OL］. https://www.privacyaffairs.com/gdpr-fines/.

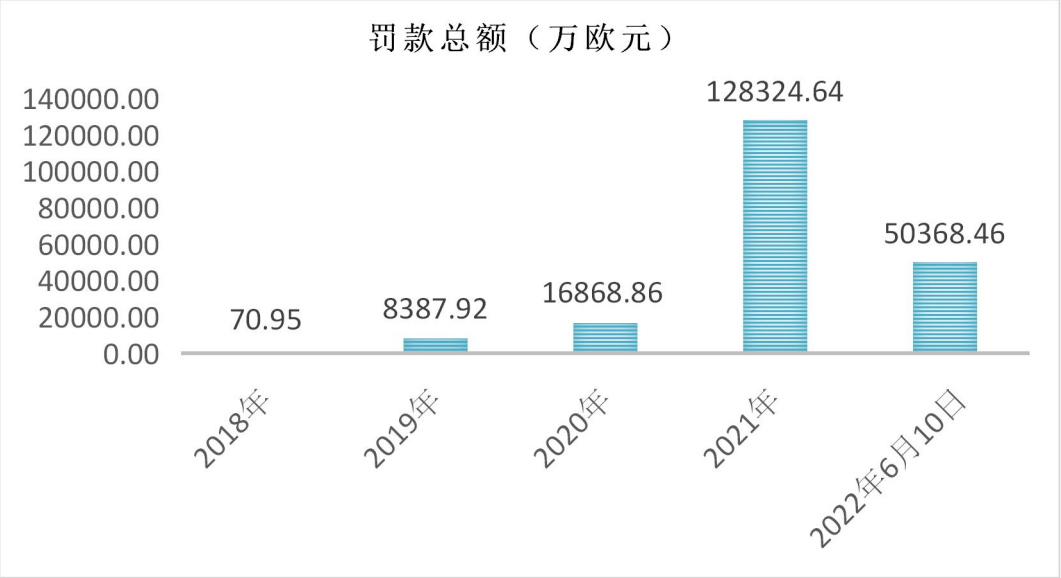

图 A-2 GDPR 年度罚款总额走势

其中，GDPR 执法案件中出现过至少 20 次的处罚依据有 7 个，如下表所示：

表 A-1: GDPR 执法案件常见处罚依据

序号	处罚依据	案件数量（件）
1	不遵守数据处理的合法依据	358
2	未遵守数据处理原则	326
3	未采取足够措施确保信息安全	194
4	不遵守主体权利保护保障措施	113
5	不遵守信息义务	50
6	不与数据保护机构合作	35
7	未能实施足够的措施确保信息	22

GDPR 的颁布对欧盟及各成员国的数据保护监管机制提出了更高的要求，此后欧盟向着建立统一、健全、严厉的数据保护监管体系不断发展。

4. 2. GDPR 与《个人信息保护法》要点对比分析

序号	对比项目/内容	欧盟 GDPR	个人信息保护法	对比分析
1	调整范围	GDPR 不在欧盟范围内对各国执法部门的个人信息处理进行统一协调，而由欧盟成员国自行制定法律对这一类个人数据处理进行规制。该条件不适用于自然人在不涉及任何职业或商业的纯个人或家庭活动中对个人数据的处理活动。个人或家庭活动可以包括通信、保存地址，或者社交活动以及类似活动背景下进行的线上活动。	个人信息保护领域的一个综合性法律。既调整私法主体、也调整公法主体的个人信息处理行为，在公法调整领域也包括调整以制止刑事犯罪和维护公共安全为目的的个人信息处理活动。自然人因个人或为家庭事务处理个人信息的，不受法律调整。	**低于中国境内保护水平。**
2	法域管辖	第 3 条 1.“经营场所原则”既带有属地管辖、也兼有属人管辖的成分：在欧盟境内设有经营场所（establishment）的控制者或处理者所开展的个人数据处理行为，无论该行为是否发生在欧盟境内； 2、“目标指向原则/保护管辖原则”：(a)向欧盟境内的数据主体提供商品或服务，无论是否需要数据主体支付对价；(b)对发生在欧盟境内数	第三条 1.“属地管辖原则”：在中华人民共和国境内处理自然人个人信息的活动”，无论处理者是组织还是自然人，也无论该组织或自然人是我国的还是外国的； 2.“保护管辖原则”：以向境内自然人提供产品或者服务为目的或分析、评估境内自然人行为的处理境内自然人个人信息的活动， 3.“普遍管辖原则”：法律、行政法规规定的其他情形。	**与中国境内保护水平持平**

		据主体的行为进行监控 3、“普遍管辖原则：非在欧盟境内设立经营场所的控制者的个人数据处理活动，只要控制者所在地的欧盟成员国的法律根据国际公法对其具有管辖权。		
3	个人信息	第 4 条第 1 款 是指与一个已识别或可识别的自然人（数据主体）相关的任何信息。可识别的自然人是指能够被直接或间接加以识别的人，尤其是借助姓名、身份证号码、位置数据、在线身份识别码这类标识，或通过特定于该自然人的一个或多个身体、生理、遗传、心理、经济文化或社会身份等要素。	第四条第二款 以电子或其他方式记录的与已识别或可识别的自然人有关的各种信息，不包括匿名化处理后的信息”	**与中国境内保护水平持平**
4	敏感个人信息	第 9 条第 1 款 这类数据高度涉及个人隐私，需要采取特殊的措施加以保护，包括种族、政治观点、宗教或哲学信仰、工会成员的个人数据，以及以唯一识别自然人为目的的基因数据、生物特征数据、健康数据、自然人的性生活或者性取向数据。	第二十八条 指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。	**高于中国境内保护水平**

5	信息的处理	第 4 条第 2 款 针对个人数据或个人数据集合的任何一个或一系列操作，无论该等操作是否采用自动化方式，例如收集、利用、排列或组合、限制、删除或销毁。 采用自动化方式全部或部分或某些情况下用手工文档系统对处理个人数据的处理。	第四条第二款 个人信息处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。	**与中国境内保护水平持平**
6	信息处理者	第 4 条第 7 款、第 8 款分别对数据控制者和处理者进行了界定。 数据控制者是指“能单独或联合决定个人数据的处理目的和方式的自然人、法人、公共机构、代理机构或其他组织”，数据处理的主要责任归属于控制者，包括联合控制者； 数据处理者为“为控制者处理个人数据的自然人、法人、公共机构、代理机构或其他组织”，例如，数据存储人、外包数据处理商、云服务提供商、服务平台或基础设施等。云计算服务出现后，对控制者和处理者的区分更加困难，特别是位于欧洲的控制者将数据交由欧洲以外的云服务商存储和处理，如果由数据控制者承担主要责任，对欧洲数据主体权利保护会面	第七十三条 没有区分控制者和处理者。所谓个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。而将需要第三方处理信息的情形视作委托处理，由作为委托人的信息处理者委托第三方处理个人信息。	**低于中国境内保护水平**

		临更大的风险。		
7	个信息保护负责人	第37条 只要符合规定情形的数据控制者与处理者，无论是公权力部门或机构还是企业或企业集团，都必须设立数据保护官（DPO）	第五十二条　处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督。 网信部门规定数量参见：《信息安全技术 个人信息安全规范》（GB/T35273-2020)规定，处理超过100万人的个个信息或者处理超过10万人的个人敏感信息的处理者。	**高于中国境内保护水平**
8	信息处理合法性基础	第6条 1、基于同意的处理 2、无须同意即可处理个人数据的情形： （一）为了履的数据主体作为一方当事人的合同或在订立合同时为实施数据主体要求的行为所必需的数据处理； （二）为履行数据控制者的法定义务所必要的数据处理； （三）为保护数据主体或另一自然人的重大利益所必要的数据处理； （四）为履行涉及公共利益的职责或实施已经	第十三条 可以处理个人信息的情形： （一）取得个人的同意； （二）为订立、履行个人作为一方当事人的合同所必需，或者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人力资源管理所必需； （三）为履行法定职责或者法定义务所必需； （四）为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需； （五）为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；	GDPR对儿童进行了特别保护，中国允许突发事件或紧急情况处理，以及新闻报道等合理使用

		授予数据控制者的职务权限所必要的数据处理； （五）数据控制者或第三方为追求合法利益目的而进地的必要数据处理，但当该利益与要求对个人数据进行保护的数据主体的基本权利和自由相冲突时，尤其是当该数据主体为儿童时，则不得进行数据处理。	（六）依照本法规定在合理的范围内处理个人自行公开或者其他已经合法公开的个人信息； （七）法律、行政法规规定的其他情形。 依照本法其他有关规定，处理个人信息应当取得个人同意，但是有前款第二项至第七项规定情形的，不需取得个人同意。	
9	主体权利	第 18 条第 15 条 第 20 条 第 12 条第 17 条 （一）限制处理权(Ringht to restriction of processing),（与知情决定权对应）； （二）数据主体访问权（Right kf access by the data subject)（与查阅复制权对应） （三）可携带权（Right to data portability); （四）更正权（Right to Rectification); （五）删除权（Right to Erasure)与被遗忘权（Right to be forgotten); 导言 27 条：本条例不适用于已故人士的个人数据，成员国可以对已故人士个人数据的处理进行规定。	第四十四条——第五十条 （一）知情权与决定权； （二）查阅复制权与可携带权； （三）更正补充权； （四）删除权； （五）解释说明权； （六）死者个人信息保护权； （七）权利行使请求权。	**低于中国境内保护水平。**2018 年，谷歌公司发起“数据转移计划”（DTP)开源项目，以实现个人信息通过服务器进行转移。意大利依据 GDPR 通过《数据保护法》规定了死者的个人信息保护权。

10	信息处理者基本义务	第 24 条第 1 款 第 32 条第 1 款、第 2 款 （一）控制者应当实施适当的技术性和组织性措施，以确保并能够证明处理活动是根据 本条例规定进行的，这些措施应在必要时进行审查和更新； （二）控制者、处理者应当实施适当的技术性和组织性措施，以确保与风险相适应的安全等级……安全帐记等级评估应当特别考虑处理过程中的风险，特别在个人数据的传输、存储以及其他方式的处理过程中的间外或非法销毁、灭失、变更、未经授权披露或者访问。	第五十一条 个人信息处理者应当根据个人信息的处理目的、处理方式、个人信息的种类以及对个人权益的影响、可能存在的安全风险等，采取下列措施确保个人信息处理活动符合法律、行政法规的规定，并防止未经授权的访问以及个人信息泄露、篡改、丢失： （一）制定内部管理制度和操作规程； （二）对个人信息实行分类管理； （三）采取相应的加密、去标识化等安全技术措施； （四）合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训； （五）制定并组织实施个人信息安全事件应急预案； （六）法律、行政法规规定的其他措施。	**与中国境内保护水平持平**
11	重要平台“守门人”的特殊义务	无	第五十八条 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行下列义务： （一）按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；	**低于中国境内保护水平** 中国借鉴欧盟《数字市场法》《数字服务法》关于大型在线平台和数字

			（二）遵循公开、公平、公正的原则，制定平台规则，明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务； （三）对严重违反法律、行政法规处理个人信息的平台内的产品或者服务提供者，停止提供服务； （四）定期发布个人信息保护社会责任报告，接受社会监督。	中介服务提供者的规定。
12	跨境传输个人数据途径	第五章 合法数据跨境流动的方式： （一）数据接收国已经达到充分保护水平 的数据跨境流动； （二）控制者或者处理者提供了适当的保障且已提供可执行的数据主体的权利和给予数据主体有效的法律救济时的数据跨境流动，如公共机构或公司规则，标准数据条款，批准的主证机制和第三国数据控制 者或处理者与适当保护措施相适应的有法律约束力和控制力的承诺，包括相应的数据主体权利等。	第三十八条 （一）依照通过国家网信部门组织的安全评估； （二）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； （三）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； （四）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。	**与中国境内保护水平持平**

13	关基运营境内出境评估义务	无	第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。确需向境外提供的，应当通过国家网信部门组织的安全评估；法律、行政法规和国家网信部门规定可以不进行安全评估的，从其规定。	**低于中国境内保护水平**
14	国际司法协助	无	第四十一条 中华人民共和国主管机关根据有关法律和中华人民共和国缔结或者参加的国际条约、协定，或者按照平等互惠原则，处理外国司法或者执法机构关于提供存储于境内个人信息的请求。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。	**低于中国境内保护水平**
15	黑名单制度	无	第四十二条 境外的组织、个人从事侵害中华人民共和国公民的个人信息权益，或者危害中华人民共和国国家安全、公共利益的个人信息处理活动的，国家网信部门可以将其列入限制或者禁止个人信息提供清单，予以公告，并采取限制或者禁止向其提供个人信息等措施。	**低于中国境内保护水平**

16	对等原则	无	第四十三条 任何国家或者地区在个人信息保护方面对中华人民共和国采取歧视性的禁止、限制或者其他类似措施的，中华人民共和国可以根据实际情况对该国家或者地区对等采取措施。	**低于中国境内保护水平**
17	泄露补救措施与通知	第 33 条 第 34 条 控制者应当至迟在 72 小时内将个人数据泄露告知有权监管机构，对于不能在 72 小时以内告的，应当提供延迟告知的原因。 无须告知情形： （一）如果个人数据泄露不可能给自然人的权利和自由造成风险的，控制者无须向监管机构报告的法定情形； （二）无须通知数据主体的法定情形： a)控制者已经采取适当的技术性和组织性保护措施，且该等措施已被用于受个人数据泄露影响的个人数据之中，特别是那些使用得未获访问授权的人无法理解个人数据 的措施如加密技术；	第五十七条 发生或者可能发生个人信息泄露、篡改、丢失的，个人信息处理者应当立即采取补救措施，并通知履行个人信息保护职责的部门和个人。通知应当包括下列事项： （一）发生或者可能发生个人信息泄露、篡改、丢失的信息种类、原因和可能造成的危害； （二）个人信息处理者采取的补救措施和个人可以采取的减轻危害的措施； （三）个人信息处理者的联系方式。 个人信息处理者采取措施能够有效避免信息泄露、篡改、丢失造成危害的，个人信息处理者可以不通知个人；履行个人信息保护职责的部门认为可能造成危害的，有权要求个人信息处理者通知个人。	**低于中国境内保护水平**

		b)控制者已采取后续措施确保上述自然人权利和自由受到高风险侵犯的情形不会出现； c)进行告知需要不适当的努力，在此情况下，应该有能够使得数据主体在同样有效的方式下获得公开告知或者相类似的举措。 如控制者未就个人数据泄露向数据主体进行告知监管机构在考虑个人数据泄露所可能带琮的高风险可能生后，可以要求控制 者进行告知或确定 是否存在无须告知的情形。		
18	行政处罚	第 83 条 （一）违反条款可以施加 1000 万欧元的行政罚款，如果是企业，最高可处相当于其上一年全球总营业额 2%的金额的罚款，两者取其高的一项罚款； （二）情节严重的，可以施加 2000 万欧元的行政罚款，如果是企业，最高可处相当于其上一年全球总营业额 4%的金额的罚款，两者取其高的一项罚款。	第六十六条 违反本法规定处理个人信息，或者处理个人信息未履行本法规定的个人信息保护义务的，由履行个人信息保护职责的部门责令改正，给予警告，没收违法所得，对违法处理个人信息的应用程序，责令暂停或者终止提供服务；拒不改正的，并处一百万元以下罚款；对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。 有前款规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额百分之五以下罚	**与中国境内保护水平持平**

			款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照；对直接负责的主管人员和其他直接责任人员处十万元以上一百万元以下罚款，并可以决定禁止其在一定期限内担任相关企业的董事、监事、高级管理人员和个人信息保护负责人。 第六十七条　有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。	
19	无过错责任	第 82 条 任何因违反本条例之行为而遭受财产损失或非财产损失的人，有权就其所受之损害请求控制 者或处理者予以赔偿 。	第六十九条　过错推定原则 处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。 前款规定的损害赔偿责任按照个人因此受到的损失或者个人信息处理者因此获得的利益确定;个人因此受到的损失和个人信息处理者因此获得的利益难以确定的，根据实际情况确定赔偿数额。	**与中国境内保护水平持平**

20	民事公益诉讼/治安处罚及刑事责任	无	第七十条　个人信息处理者违反本法规定处理个人信息，侵害众多个人的权益的，人民检察院、法律规定的消费者组织和由国家网信部门确定的组织可以依法向人民法院提起诉讼。 第七十一条　违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任	**低于中国境内保护水平**

5. 日本

5.1. 中日个人信息保护法部分要点对比分析表

序号	对比项目/内容	日本《个人信息保护法》	中国《个人信息保护法》	对比分析
1	个人信息跨境的要求	事先获得个人同意的情况下，处理个人信息的经营者可向国外第三方提供个人数据	第三十八条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： （一）依照本法第四十条的规定通过国家网信部门组织的安全评估； （二）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； （三）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； （四）法律、行政法规或者国家网信部门规定的其他条件。	**低于中国境内保护水平**
2	境内存储的要求	无境内存储特殊要求	第三十六条 国家机关处理的个人信息应当在中华人民共和国境内存储； 第四十条 关键信息基础设施运营者和处理个人信息达到国家网信部门规定数量的个人信息处理者，应当将在中华人民共和国境内收集和产生的个人信息存储在境内。	**低于中国境内保护水平**

3	出境前征得个人同意	向个人信息保护委员会白名单中所列国家第三方提供数据时可不经个人同意直接提供（白名单：欧盟、英国）	《个人信息保护法》第三十九条个人信息处理者向中华人民共和国境外提供个人信息的，应当向个人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、个人信息的种类以及个人向境外接收方行使本法规定权利的方式和程序等事项，并取得个人的单独同意。	**低于中国境内保护水平**
4	假名化/匿名化	假名化信息：在个人信息处理者内部使用时，可改变信息获取时的使用目的	《个人信息保护法》第四条第一款 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。	**低于中国境内保护水平**

6. 新加坡

6.1. 新加坡与中国境内数据保护相关法律部分要点对比分析表

序号	对比项目/内容	新加坡	中国境内	对比分析
1	适用范围	《个人数据保护法案》（PDPA）4. -(1)第 3、4、5、6、6A 和 6B 部分不对下列主体施加任何义务 (a)以个人或家庭身份行事的任何个人; (b)受雇为某机构工作的任何雇员; (c)任何公共机构;或 (d)为本规定的目的而规定的任何其他组织或个人数据，或组织类别或个人数据。(40/2020) (2)第 3、4、5、6 部分(第 24 和 25 条除外)、6A 部分(第 26C(3)(a)和 26E 条除外)和 6B 部分并不就数据中介机构根据以书面证明或订立的合同代表另一组织和为其目的处理个人数据而对其施加任何义务。(40/2020) (3)在本法项下，对于由数据中介机构代表其处理的个人数据和为其目的处理的个人数据，组织负有相同的义务，就如同个人数据是由该组织自己	《个人信息保护法》 第三十三条 国家机关处理个人信息的活动，适用本法；本节有特别规定的，适用本节规定。 第七十二条 自然人因个人或者家庭事务处理个人信息的，不适用本法。 法律对各级人民政府及其有关部门组织实施的统计、档案管理活动中的个人信息处理有规定的，适用其规定。	**低于中国境内的保护水平。**关于不适用个人信息保护法的范围，PDPA 做了更广的规定，特别是公共机构、保持 100 年以上的个人信息或者过世 10 年以上个人的个人信息

		处理的一样。		
		(4)本法不适用于- (a)包含在存在至少 100 年的记录中的有关个人的个人数据;或(b)关于已故个人的个人资料，但有关披露个人资料的规定和第 24 条(个人资料保护)适用于已故 10 年或 10 年以下的个人的个人资料除外。 (5)除明确提及业务联系信息外，第 3、4、5、6 和 6A 部分不适用于业务联系信息。(40/2020) (6)除非本法另有明确规定- (a)第 3、4、5、6、6A 和 6B 部分的任何内容都不影响法律授予的任何权力、权利、特权或豁免，或法律赋予的义务或限制，包括法律特权，但履行合同义务不是违反本法的理由除外;和 (b)在第 3、4、5、6、6A 和 6B 部分的任何规定与该其他成文法的规定不一致的情况下，以其他成文法的规定为准。(40/2020)	同上	**同上**

2	个人信息的定义	PDPA“个人资料”系指有关可被识别为个人的信息，不论真实与否 (a)从该数据;或 (b)来自该组织已获得或可能获得的该数据和其他信息; “处理”，就个人信息而言，指进行与该等个人资料有关的任何操作或一组操作，并包括下列任何一项:(a)记录;(b)存储;(c)组织、改编或变更;(d)检索;(e)组合;(f)传输;(g)删除或销毁;	《个人信息保护法》第四条 个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。 个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。	结合《民法典》第六章“隐私权和个人信息保护”的相关规定，中国《个保法》所定义的“个人信息”或包括某些个人隐私，而新加坡从立法以及司法层面上均未规定个人隐私权，**因此 PDPA 的保护范围也不涉及个人隐私**
3	个人信息出境的条件	26.-（1）组织不得将任何个人数据转移到新加坡以外的国家或地区，除非符合本法规定的要求，以确保组织为如此转移的个人数据提供与本法保护相当的保护标准。 （2） 委员会可根据任何组织的申请，以书面通知免除该组织根据第（1）款就该组织转移个人数据的任何规定。 （3） 根据第（2）款的豁免—— （a） 可准予，但须符合委员会书面规定的条件;和	《个人信息保护法》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：（一）依照本法第四十条的规定通过国家网信部门组织的安全评估；（二）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；（三）按照国家网信部门制定的标准合同与境外接收方订立	在 PDPA 下，一般情况数据不可以进行跨境传输，除非数据接受方可以通过 有法律效力的方式提供和 PDPA 下同等的数据保护。

		（b） 无须在宪报刊登，委员会可随时撤销。 （4） 委员会可随时增加、更改或撤销根据本条施加的任何条件。	合同，约定双方的权利和义务；（四）法律、行政法规或者国家网信部门规定的其他条件。	
4	同意的要件	PDPA 14.-（1） 个人未根据本法同意组织出于某种目的收集、使用或披露有关该个人的个人数据，除非 — （a） 已向该个人提供第 20 条所要求的信息; （b） 个人根据本法为此目的表示同意 （2） 组织不得 - （a） 作为提供产品或服务的条件，要求个人同意收集、使用或披露有关该个人的个人数据，超出向该个人提供产品或服务的合理范围;或 （b）通过提供有关收集、使用或披露个人数据的虚假或误导性信息，或使用欺骗性或误导性做法，获得或试图获得收集、使用或披露个人数据的同意。 提及个人就收集、使用或披露有关该个人的个人数据给予或被视为已给予的同意，包括代表该个人有效行事的任何人就收集、使用或披露此类个人数据给予或被视为已给予的同意。	第十四条 基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。 个人信息的处理目的、处理方式和处理的个人信息种类发生变更的，应当重新取得个人同意。	**低于中国境内保护水平。**两国的同意均将告知、知情作为同意生效的要件，也不得使用误导、欺诈等方式获取同意。但在特殊情况下，比如对外提供、处理敏感个人信息，境内要求单独同意，这一点会严格于新加坡。而且新加坡还有特殊的“视为同意“规则（见下文），境内均要求当事人明确做除同意。
5	视为同意	视为同意规则：15.-（1） 如果个人未经第 14 条所述的实际同意，自愿为此目的向组织提供个人数据，则被视	无	**低于中国境内保护水平。**中国境内的同意均

		为同意组织出于某种目的收集、使用或披露有关该个人的个人数据; （2） 如果个人同意或被视为已同意一个组织出于特定目的向另一个组织披露有关该个人的个人数据，则该个人被视为同意该其他组织为该特定目的收集、使用或披露个人数据。根据第（9）款，向组织（A）提供个人资料以使 P 与 A 签订合同的个人（P）被视为同意以下合理必要的事项，以订立 P 与 A 之间的合同： （a）A 向另一个组织披露该个人数据（B）; （b）B 收集和使用该个人数据; （c）披露 [40/2020]		要求是个人信息主体明确做出的。
		（4） 如果组织收集乙根据第（3）（c）款向其披露的个人数据，则第（3）（b）和（c）款适用于该组织，就好像 A 根据第（3）（a）款向该组织披露了个人数据一样。就个人而言，个人在 2021 年 2 月 1 日或之后与组织签订合同;或 （b）该合同在 2021 年 2 月 1 日之前订立，并于该日仍然有效， 好像第（3）和（4）款- （c）小节在提供个人数据时有效;	无	同上

		（d） 有效期至 2021 年 2 月 1 日 [40/2020] （6） 在不限制第 （2） 小节的情况下，根据第 （9） 小节的规定，与组织 （A） 签订合同并根据该合同或与该合同向 A 提供个人数据的个人 （P） 被视为同意以下内容： （a） A 向另一个组织披露该个人数据 （B）， 披露是合理必要的 — （i） 为履行原告与甲之间的合同;或 （ii）甲与乙订立或履行应原告要求订立的合约，或理智人士认为符合原告利益的合约; （b）乙收集和使用该个人资料，而收集和使用对于（a）段所述的任何目的而合理必要; （c）乙向另一组织披露该个人资料，[40/2020]		
		（7） 如果组织收集 B 根据第 （6）（c） 款向其披露的个人数据，则第 （6）（b） 和 （c） 款适用于该组织，就好像 A 根据第 （6）（a） 款向该组织披露了个人数据一样。与该组织在该日期之前签订的合同有关的个人，该合同在该日期仍然有效，就好像第（6）和（7）小节- （a）在提供个人数据时有效; [40/2020]	无	**同上**

		（9） 第（3）、（4）、（5）、（6）、（7）和（8）款不影响原告与甲之间订明或限制的任何义务 - （a） 甲方可能向另一组织披露的原告提供的个人资料;或 （b）甲可向另一机构披露原告提供的个人资料的目的 [40/2020]		
6	经由通知视为同意	经由通知视为同意：15A.-（1） 本节适用于组织在 2021 年 2 月 1 日或之后收集、使用或披露有关个人的个人数据。以及 （b）个人未在第（4）（b）（iii）款所述的期限届满之前通知组织，该个人不同意组织拟议收集，使用或披露个人数据。 第（2）款不适用于出于任何规定目的收集，使用或披露有关个人的个人数据 [40/2020] （4）就第（2）（a）款而言， 在收集、使用或披露有关个人的任何个人数据之前，组织必须 - （a） 进行评估以确定拟议的个人数据收集、使用或披露不太可能对个人产生不利影响; （b） 采取合理步骤提请个人注意以下信息： （i） 组织收集、使用或披露个人资料的意图; （ii） 收集、使用或披露个人资料的目的;	无	**同上**

		（iii）个人可以通知组织该个人不同意该组织建议收集的合理期限和合理方式， 个人数据的使用或披露; [40/2020]		
	经由通知视为同意	（5）就第（4）（a）款所述的评估而言，组织必须确定为有关目的而拟议收集、使用或披露个人数据可能对个人产生的任何不利影响; （b）确定并实施合理措施，以 （i）消除不利影响; （ii）降低不利影响的可能性发生;或 （iii）减轻不利影响;以及 （c）遵守任何其他规定的要求。	**无**	**同上**
7	撤回同意	16.-（1）在向组织发出合理通知后，个人可以随时撤回根据本法给予或被视为已给予的关于该组织出于任何目的收集，使用或披露有关个人的个人数据的任何同意。 （3） 组织不得禁止个人撤回其对收集、使用或披露有关该个人的个人数据的同意，但本节不影响因撤回而引起的任何法律后果。 根据第 25 条， 如果个人撤回同意组织出于任何目的收集、使用或披露有关个人的个人数据，该组织必须停止（并导致其数据中介和代理人停	第十五条 基于个人同意处理个人信息的，个人有权撤回其同意。个人信息处理者应当提供便捷的撤回同意的方式。 个人撤回同意，不影响撤回前基于个人同意已进行的个人信息处理活动的效力。 第十六条 个人信息处理者不得以个人不同意处理其个人信息或者撤回同意为由，拒绝提供产品或者服务；处理个人信息属于提供产品或者服务所必需的除外。	**低于中国境内保护水平。**PDPA 中并未明确禁止个人信息处理者在个人不同意处理其个人信息或撤回同意的情况下拒绝提供产品或服务。

		止）收集、使用或披露个人数据（视情况而定），除非根据本法或其他成文法要求或授权未经个人同意而收集、使用或披露（视情况而定）。		
8	“谢绝来电”条款(Do-Not-Call 或“DNC”)	在 PDPA 的第 9 部分，第 36-48 条规定了“谢绝来电”(Do-Not-Call 或“DNC”)登记系统，用来保护电话用户不受营销广告的骚扰。DNC 登记系统分为三个子系统，分别对应语音电话、文字信息以及传真信息。该登记系统由新加坡政府负责维护，任何个人或组织都可以通过登录官网 https://www.dnc.gov.sg 进行登记，也可以通过电话或者短信方式完成登记。 新加坡的电话号码都可以主动选择在一个或多个子系统中登记。任何组织机构都不得向已进行登记的电话号码以其登记的通讯方式向其拨打电话或传送信息。除非满足例外的条件，否则任何组织机构在向任何新加坡电话号码发送营销广告之前都有义务通过查询登记系统确认其目标号码不在登记系统内后，方可发送相关信息。同时，组织机构在发送营销广告信息或拨打营销电话时必须明示发送人或拨打人的身份，也不得通过隐蔽拨出电话号码、使用虚拟电话号码或者其他的手段达到隐匿自己身份的目的。	无	高于境内保护水平

	“谢绝来电”条款(Do-Not-Call 或“DNC”)	当然，任何一个新加坡电话号码也可以在加入登记之后，以书面方式同意接受特定的组织机构发出的营销广告信息。同时，并不是所有的信息都受 DNC 登记的限制。《PDPA》附录八中收录了若干不属于 DNC 监管的信息类型，例如因为发生人身伤害危险时的紧急通知，用来辅助、确认、提供、完成服务承诺的信息，发送质保、召回等与产品安全有关的信息等等。 同时，新加坡也禁止使用“字典式拨号”(dictionary attack)和“电话号码搜集软件”(address-harvesting software)。“字典式拨号”指的是使用软件或其他手段通过将数字通过排列组合而产生可能的电话号码的方式；而“电话号码搜集软件”指设计为可以通过搜索互联网搜集、汇总、抓取或以其他方式获得电话号码的软件。新加坡对通过以上两种手段获得他人电话号码的行为通过立法予以禁止。	无	同上

附录 B：国家以及行业数据安全分类分级标准

标准编号	标准名称	适用行业	标准类型
JR/T 0197-2020	《金融数据安全 数据安全分级指南》	银行	行业标准
暂无	《信息安全技术 网络数据分类分级要求》	通用	国家标准
DB11/T 1918-2021	《政务数据分级与安全保护规范》	地方政务	地方标准
JR/T 0158—2018	《证券期货业数据分类分级指引》	证券期货	行业标准
YD/T 3746-2020	《车联网信息服务 用户个人信息保护要求》	汽车/车联网	行业标准
暂无	《信息安全技术 重要数据识别指南》	通用	国家标准