

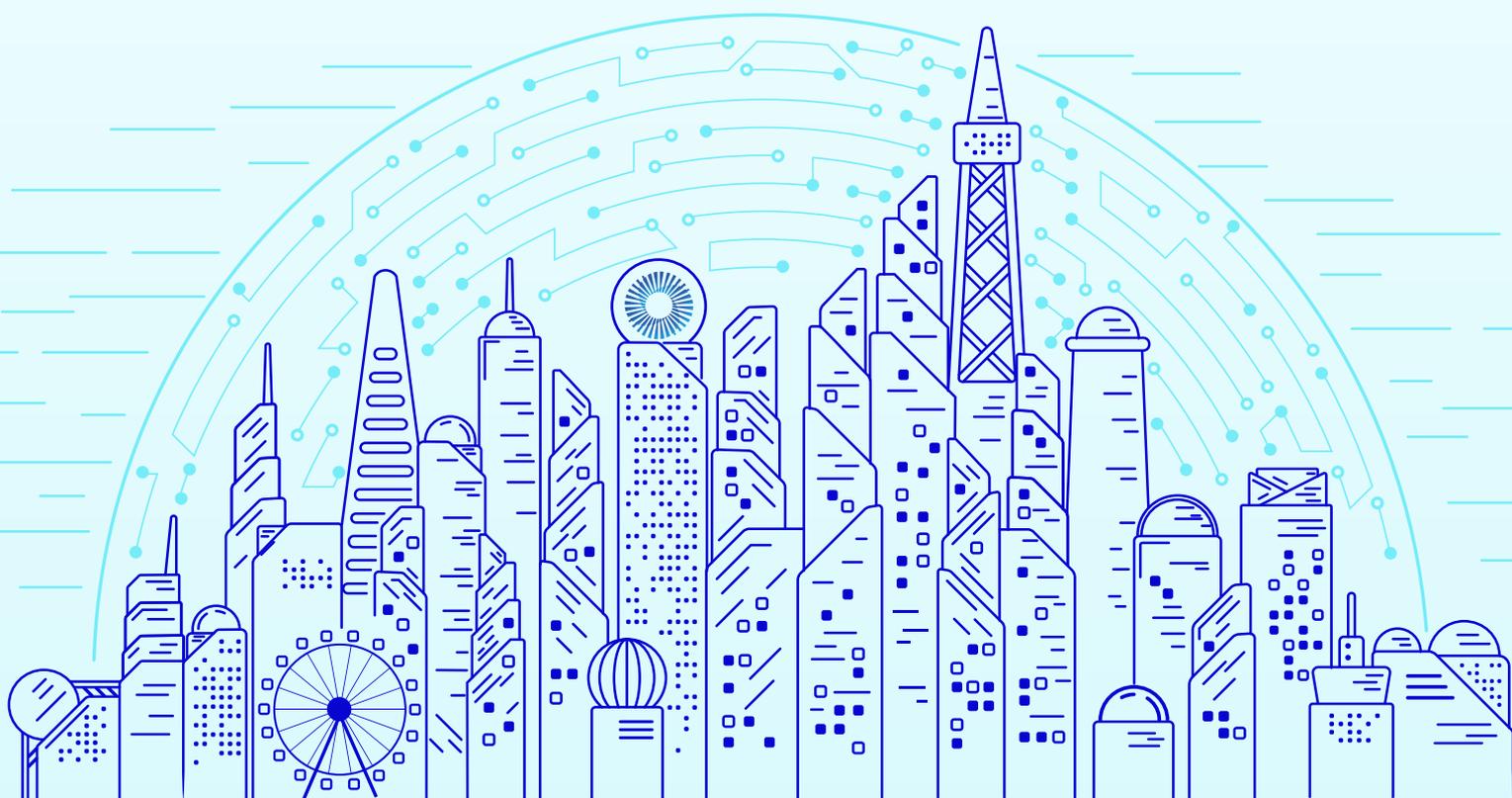


Open Islands

2023

跨境数据流通 合规与技术应用白皮书

The White Paper on Cross-border Data Transfer
Compliance and Technology Applications



开放群岛开源社区跨境数据流通小组
2023年12月



Open Islands

跨境数据流通 合规与技术应用白皮书 (2023 年)

开放群岛开源社区跨境数据流通小组
2023 年 12 月

版权声明

本白皮书版权属于开放群岛开源社区跨境数据流通小组所有，依据 CCBY-NC-SA4.0 (<http://creativecommons.org/licenses/by-nc-sa/4.0/>) 许可证进行授权，并受法律保护。转载、编撰或利用其他方式使用本白皮书文字或观点，应注明来源。

违反上述声明者，编者将追究其相关法律责任。

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联合国世界丝路论坛数字经济研究院院长、浙江大学网络空间安全学院王春晖教授。

❖ 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、深圳数据交易所、深圳市星创数字研究中心、广东卓建律师事务所、北京信联数安科技有限公司、勤达睿（中国）信息科技有限公司、北京植德（深圳）律师事务所、南方科技大学深圳国家应用数学中心、江苏无锡大数据交易有限公司、数交数据经纪（深圳）有限公司、深圳职业技术大学、深圳赛西信息技术有限公司、南昌大学、万商天勤（深圳）律师事务所、万商天勤（杭州）律师事务所、华东江苏大数据交易中心股份有限公司、深圳信息通信研究院、北京中企数安咨询有限公司、大数据协同安全技术国家工程研究中心、中国电信股份有限公司研究院、邓白氏中国、北京市汉坤（深圳）律师事务所、北京市京师（深圳）律师事务所、日本野村综合研究所、广东经天律师事务所、粤港澳大湾区大数据研究院、广东际唐律师事务所、福建旭丰律师事务所、北京万商天勤律师事务所、优刻得科技股份有限公司、中诚信征信有限公司、浙江九鑫智能科技有限公司、深圳市电子商务安全证书管理有限公司、厦门海峡链科技有限公司、四川久远银海软件股份有限公司、领禹智通数据科技（上海）有限公司、三六零数字安全科技集团有限公司、腾讯科技（深圳）有限公司、贵州财经大学、青岛国创智能家电研究院有限公司、南方科技大学智能管理与创新发展研究中心、奇安信科技集团股份有限公司、南财合规科技研究院、数库（上海）科技有限公司

❖ 编写组主要成员（排名不分先后）：

陈曦	李如先	王冠	丁振赣
周宏	张巍	宫仁海	李兰兰
刘媛	陈宁	王艺	郭巧真
王以玮	史亦言	于丹丽	张雅婷
王鑫	罗欣	劳国威	易海博
谭瑞琥	柴颖	戴志敏	吴朝阳
周阅	杨淋雨	尤磊	张昊
杨子安	王雪纯	何思婷	周钢
李东阳	陈璐	王雨薇	李清莲
宋杰	李丹	袁芸	夏彦
廖瞰曦	赵鹏飞	陈慧	曾铮
陈嘉琪	袁玥	成雨杨	杜瑜
莫斯航	王岩飞	樊思琪	李智慧
王孝冉	谢贤保	李昌旺	舒青云
王琼	彭晓燕	孙红	李和清
侯子博	刘沛	郭婷	程晶晶
彭文琪	魏倩	黄念念	王澜
吴一	吴昊	马兰	阮舟
王志辉	王超博	陈建宏	张长彬
吴治中	罗瑶	邓祥静	胡浩

魏安迪	崔如德	李 坤	贺志生
王永霞	代 威	丁红发	杨 楠
梁 娜	黄 伟	周谢军	蔡小芳
唐 鑫	蔡 欢	马纪园	肖苗苗
刘岭峰	蔡剑戈	王青兰	朱 琳
蒙雄发	李文塔	陈俊昌	陆忠明

前言

随着信息技术的飞速发展，数字贸易逐步成为国际贸易发展新趋势和贸易增长新引擎。跨境数据流通是开展数字贸易的前提条件，是世界经济流动新要素。全球数据流动对经济增长有明显的拉动效应。世界贸易组织数据显示，2022年，全球跨境数据流通规模增长120.6%，数字服务贸易规模增长36.9%，均高于同期的全球服务贸易和货物贸易的增速。跨境数据流通对贸易模式、贸易结构、全球贸易规则和世界贸易格局产生深刻影响。加强数据跨境流动探索，已成为打造我国在全球数字经济发展格局中优势的关键。

2022年12月，《中共中央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》提出，坚持开放发展，推动数据跨境双向有序流动。2023年9月28日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，该规定在个保法以及相关数据跨境传输规定的基础上，降低了相关主体在数据出境时的合规成本，加快了我国数据出境的效率，有利于促进国际机构跨境活动的高效运营。截至目前，全国已有北京、上海、广州、深圳等20余地出台“数据相关条例”，推进数据跨境流动工作。

在此背景下，联易融于2022年受邀牵头创建开放群岛跨境数据流通小组，以助力企业合法合规实现数据跨境流通，业务出海为目标；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。去年组织三十余家境内外机构编写了《跨境数据流通合规与技术应用白皮书（2022）》，收到广泛关注。据不完全统计，发布之初，就得到了超过30W次的阅读量，以及包括主流媒体在内的超过500家媒体等机构转载。

跨境数据流通对贸易模式、贸易结构、全球贸易规则和世界贸易格局产生深刻影响。加强数据跨境流动探索，已成为打造我国在全球数字经济发展格局中优势的关键。2023年联易融继续牵头并携深数所、信通院等40多家机构撰写《跨境数据流通合规与技术应用白皮书》（以下简称《白皮书（2023）》）。

《白皮书（2023）》进一步拓宽国际视野和跨境场景，聚焦粤港澳大湾区优势，具有以下特点：

第一，国际视野更加开阔，追踪欧美日韩最新跨境数据合规法律动态，增补我国重要贸易伙伴以及邻近国家和地区的法律环境分析，如东盟成员国、沙特阿拉伯、俄罗斯、中国台湾等地，并与中国大陆的数据跨境规则进行对比，为数据处理者与相关国家或地区开展数据跨境活动时提供参考。数据跨境的规范更需要不同国家间相互合作才能完成，《白皮书（2023）》对当今主要的数据跨境流通

国际条约也加以介绍，为探索跨国合作提供新的视角。

第二，数据跨境场景更加丰富，在关注跨境重点行业的基础上，发掘新场景和新应用。例如，从民生出发，关注大湾区居民异地银行或证券开户的个人数据跨境流动。从工业智造出发，关注关键工业数据合规跨境提升芯片制作工艺。从公共健康出发，关注跨境就医结算服务和医疗临床研究项目的数据合规出境规范。

第三，数据跨境区域更加聚焦，粤港澳大湾区具有独特的区位优势，是我国跨境数据流通的重要节点。作为一个重要的经济合作区域，涉及“一个国家、两种制度、三个关税区、三种货币”，这里具备强大的经济发展实力和跨境数据流通需求。《白皮书（2023）》重点关注粤港澳大湾区跨境数据流通发展现状，推进数据跨境流动安全规则研究、制定和落地的先行先试。

本次白皮书成功发布，离不开“开放群岛跨境数据流通小组”各位领导专家的支持和帮助。他们在跨境数据合规与流通实践方面，拥有成熟的经验与领先的优势。在编写过程中，各位专家不吝分享自己专业领域的真知灼见，每一次讨论都是思想的碰撞，每一次交流都是思维的提升。再次感谢各参编单位的团结贡献，让我们继续为推动数据跨境安全有序流动贡献力量！

目 录

版权声明	1
编制说明	2
前 言	1
目 录	1
图列表	1
第一章 背景介绍	1
1.1. 我国跨境数据流通的发展现状	1
1.2. 港澳大湾区跨境数据流通的发展现状	4
1.3. 全球跨境数据流通的发展趋势	4
1.4. 我国跨境数据流通发展面临的挑战	5
第二章 国际条约中的数据跨境规则	8
2.1. 总览	8
2.2. 具体条约中的数据跨境规则	9
2.2.1. 基于世界贸易组织（WTO）框架下的重要多边条约	9
2.2.2. 《区域全面经济伙伴关系协定》（RCEP）	12
2.2.3. 《全面与进步跨太平洋伙伴关系协定》（CPTPP）	14
2.2.4. 《数字经济伙伴关系协定》（DEPA）	15
2.3. 对中国数据跨境管理的启示	16
第三章 数据跨境域外法律环境分析	18
3.1. 中国香港	18
3.1.1. 推动数字经济发展，打造亚太地区数据中心设立首选地	18
3.1.2. 香港数据保护及数据跨境的要点简析	19
3.1.3. 香港与中国大陆个人信息保护法规之对比情况	21
3.2. 中国澳门	22
3.2.1. 完整的个人资料保护规范，但不完善的跨境规则	22
3.2.2. 澳门数据保护及数据跨境的要点解析	22
3.2.3. 注意敏感个人信息保护，避免行政处罚	23
3.3. 中国台湾	24
3.3.1. 台湾地区个人资料保护及跨境流通监管的法律环境	24
3.3.2. 我国台湾地区数据保护及数据跨境的要点简析	25
3.3.3. 我国台湾地区《个人资料保护法》与大陆《个人信息保护法》的衔接与差异	27

3.4 东盟	27
3.4.1. 出台系列指导性政策文件，统筹数字经济发展与数据保护	28
3.4.2. 《东盟个人数据保护框架》促各成员国国内数据保护政策一致化	28
3.4.3. 《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》为企业 提供数据管理和跨境数据流通的指引	29
3.5.新加坡	29
3.5.1. 寻求加强监管与数据开放流动直接平衡的监管体系	29
3.5.2. 新加坡数据保护监管框架概览及数据跨境的要点解析	30
3.5.3. 新加坡与中国个人信息保护之比较	33
3.6. 越南	33
3.6.1. 越南数据保护法律体系概况	33
3.6.2. 越南数据保护和数据跨境的要点简析	33
3.6.3. 越南与中国数据保护法律之对比	34
3.7. 沙特阿拉伯	35
3.7.1. 沙特阿拉伯数据保护法律框架概述	35
3.7.2. 沙特《个人数据保护法》要点简析	35
3.7.3. 沙特数据保护与中国的对比	37
3.8. 日本	37
3.8.1. 日本数据跨境流通战略举措	37
3.8.2. 日本数据跨境流通法律规制要点简析	39
3.8.3. 与我国数据跨境法律法规对比分析	41
3.9. 印度	42
3.9.1. 经历多次曲折，终接近出台数据保护专门立法	42
3.9.2. 印度数据保护及数据跨境的要点解析	42
3.9.3. 与中国法律的对比	45
3.10. 俄罗斯	46
3.10.1. 俄罗斯联邦个人信息及数据法律环境分析	46
3.10.2. 俄罗斯联邦数据跨境保护及审查要点分析	47
3.10.3. 中俄数据保护及数据跨境合规对比	49
3.11. 欧盟	49
3.11.1. 棱镜事件推动的数据跨境流动立法密集时代	49
3.11.2. 欧盟数据保护及数据跨境的要点简析	50
3.11.3. 中国对 GDPR 的借鉴与发展	51

3.12. 美国	53
3.12.1. 美国个人信息及数据法律环境分析	53
3.12.2. 美国数据保护及数据跨境的要点解析	54
3.12.3. 美国与中国数据保护法律之对比	56
3.13. 尊重区域差异，做好数据跨境合规	57
第四章 跨境数据流通技术解决与合规方案	58
4.1. 跨境消费：某知名大型港资消费品企业数据跨境方案	58
4.1.1. 案例背景	58
4.1.2. 技术方案	59
4.1.3. 方案创新点和亮点	59
4.1.4. 应用效果	60
4.2. 跨境金融：香港银行跨境电子签署	60
4.2.1. 案例背景	60
4.2.2. 技术方案	60
4.2.3. 方案创新点和亮点	62
4.2.4. 应用效果	62
4.3. 跨境芯片研发：M2&SKC 芯片数据跨境安全计算	62
4.3.1. 案例背景	62
4.3.2. 技术方案	63
4.3.3. 方案创新亮点	64
4.3.4. 应用成效	65
4.4. 跨境数据：中国首单场内跨境数据交易	65
4.4.1. 案例背景	65
4.4.2. 整体方案	65
4.4.3. 数据产品创新点和亮点	68
4.4.4. 应用成效	68
4.5. 数字贸易：基于数字贸易资产的融资解决方案	69
4.5.1. 案例背景	69
4.5.2. 技术方案	69
4.5.3. 方案创新点和亮点	71
4.5.4. 应用成效	72
4.6. 跨境金融：港股开户跨境可靠电子签署	72
4.6.1. 案例背景	72
4.6.2. 技术方案	72

4.6.3. 方案创新点和亮点	73
4.6.4. 应用效果	73
4.7. 卫生健康：跨境就医结算服务平台	74
4.7.1. 案例背景	74
4.7.2. 技术方案	74
4.7.3. 方案创新点和亮点	77
4.7.4. 应用效果	77
4.8. 跨境征信：海外用户信用风险评估报告	78
4.8.1. 案例背景	78
4.8.2. 技术方案	78
4.8.3. 方案创新点和亮点	80
4.8.4. 应用效果	80
4.9. 健康医疗：临床试验数据跨境合规	81
4.9.1. 案例背景	81
4.9.2. 合规方案	82
4.9.3. 方案创新点和亮点	83
4.9.4. 应用效果	84
4.10. 跨境贸易：基于区块链的两岸跨境贸易商品溯源系统	84
4.10.1. 案例背景	84
4.10.2. 技术方案	85
4.10.3. 方案创新点和亮点	88
4.10.4. 应用效果	88
4.11. 跨境电商：跨境数据推动电商企业 ESG 供应链改进	88
4.11.1. 案例背景	89
4.11.2. 技术方案	90
4.11.3. 方案创新点和亮点	91
4.11.4. 应用效果	91
4.12. 数据合规：企业数据出境风险评估	92
4.12.1. 案例背景	92
4.12.2. 合规评估	92
4.12.3. 方案创新点和亮点	94
4.12.4. 结语建议	94
第五章 数据跨境流通与技术应用发展建议	95
5.1. 数据跨境安全管理底线坚持与便利化探索	95

5.2. 企业全面建成数据跨境合规体系	96
5.2.1. 企业数据安全性与隐私保护	96
5.2.2. 企业供应链风险控制与管理	97
5.2.3. 企业跨境数据流通合规能力建设	98
5.3. 推动跨境数据流通合规技术产业发展	99
5.4. 重视合规人才培养与产业共生	101
5.5. 深化开放合作实现跨境合规应用多样化	102
参考文献	104
附录 A: 数据跨境流通域外法律解析	107
1. 香港	107
2. 澳门	113
3. 台湾	117
4. 新加坡	131
5. 越南	140
6. 日本	149
7. 印度	150
8. 欧盟	160
9. 美国	176
附录 B: 编写单位简介	193

图列表

图 1	跨境流程示意图	59
图 2	跨境电子签署服务平台总体架构图	61
图 3	跨境电子签署服务平台网络传输路径图	62
图 4	整体架构图	64
图 5	UCloud 安全屋业务流程图	64
图 6	数库 SmarTag 新闻分析数据产品架构图	66
图 7	跨境数据交易流程图	67
图 8	传统供应链中 DTA 的应用流程图	70
图 9	多级供应链中 DTA 在发行、转让、融资和兑现场景中的应用	71
图 10	深圳 CA 港股开户电子认证服务平台总体架构图	73
图 11	跨境就医结算服务平台框架结构图	76
图 12	平台业务流程图	76
图 13	跨境就医结算服务平台技术架构图	77
图 14	用户信用风险评估报告处理系统作业流程示意图	79
图 15	征信报告模板示意图	80
图 16	数据出境安全评估流程	82
图 17	自评估流程图	83
图 18	两岸跨境贸易商品溯源应用技术架构图	86
图 19	两岸跨境贸易商农产品溯源应用数据上链流程	86
图 20	两岸跨境贸易商品溯源应用数据采集示例	87
图 21	两岸跨境贸易商品溯源应用案例	87
图 22	方案功能展示图	89
图 23	企业跨境数据安全技术体系架构图	96

第一章 背景介绍

数据是国家重要的战略资源，跨境数据的积累、精炼、加工和管控是数字经济的重要组成部分，对于促进全球经济的可持续发展具有重要的推动作用。数据跨境流通对数字丝绸之路建设具有积极的推动作用，有助于促进全球数字经济的健康发展，实现各国在数字化时代的共同繁荣。在数字化转型背景下，跨境数据流通已愈发成为全球经济增长中的关键引擎。一是**跨境数据推动数字经济全球化**。跨境数字业务如跨境金融、跨境医疗、跨境零售等都需要大量的数据在全世界范围内快速传输和处理，实现全球化的服务和运营；如果无法跨境传输数据，这些基于网络的数字业务将难以实现全球发展，实现数字经济的全球布局。二是**跨境数据保障数字贸易一体化**。随着数字贸易规模不断扩大，跨境数据流通将成为促进数字贸易发展的重要基础，只有实现安全高效的跨境数据流通，数字贸易才能真正实现全球一体化，这将进一步推动全球数字经济的深入发展。三是**跨境数据流通支撑产业高质量**。企业通过跨境数据流通，整合全球各地区的数据资源实现资源最优化配置，这可以帮助企业缩短产品迭代周期，提高研发效率，优化全球运营决策，在全球竞争中获得先发优势，同时产业也可以利用数据优势，实现转型升级和高质量发展。四是**跨境数据流通助力企业高效益**。通过收集和分析来自不同国家和地区用户数据，企业可以更好地了解全球客户的需求和偏好，挖掘出新的商业机会，针对不同市场提供定制化的产品和服务，实现精准营销，拓宽全球销售渠道，这将有利于企业快速扩大市场规模。

1.1. 我国跨境数据流通的发展现状

(1) 跨境数据流通的快速发展导致新的商业模式不断涌现，产生更加紧密复杂的经济互动，从而促进数字经济外延形式上的持续扩张和内在逻辑上的持续延伸。在数字经济全球化的背景下，我国对于跨境数据流通的管理上也参考了国际先进经验，制定和实施了許多重要的管理措施。总体而言，我国跨境数据流通整体呈现管理框架更加完善、跨境数据流通行业应用更加丰富等特征。

(2) 数据跨境流通管理规范体系愈发完善

为顺应跨境数据流通，融入全球化发展，近年来我国出台并施行了《中华人民共和国民法典》《电子商务法》《网络安全法》《数据安全法》《个人信息保护法》《中华人民共和国密码法》《中华人民共和国外商投资法》《反垄断法》《出口管制法》等法律规范。随着《网络安全法》《数据安全法》《个人信息保

护法》等法律的发布，我国建立了以数据保护与跨境数据流通为框架的制度体系，同时法律框架机制的设计也采取了全球共识和本土经验相融合的创新模式，积极探索跨境数据流通规则体系多样性的建设。2022年9月国家互联网信息办公室发布实施《数据出境安全评估办法》，进一步规范了数据跨境的事前管理路径；2022年12月中共中央国务院发布《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称“数据二十条”），进一步有利于提高数据要素治理效能；2023年6月1日施行的《个人信息出境标准合同办法》及《个人信息出境标准合同》，是对《个人信息保护法》中国家层面的跨境数据流通管理制度体系的落实；2023年7月国务院印发《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》，进一步提出和倡议了“为符合条件的外商投资企业高效开展重要数据和个人信息出境安全评估，提供绿色通道”；2023年9月28日国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，进一步对数据跨境流动的禁止性行为、可行性行为进行了明确的界定，并针对允许的跨境数据流通的可行性行为给予了操作指引，并强调了企业数据出境安全责任和监管要求。总体而言，我国跨境数据流通相关管理体系愈发完善。

(3) 我国跨境数据流通行业应用愈发丰富

在我国，跨境数据流通已经渗透到众多行业中，其中以金融、制造业、医疗、物流、数字贸易和数字服务等行业为国内跨境数据流通的行业代表，跨境数据流通在其中发挥了积极重要的作用。

在金融行业，对客户全球范围的金融资产进行配置和管理的过程中，包含大量的跨境数据信息需求，如金融跨境结算，反洗钱及全球风控、客户金融资产管理实时跨境同步等业务场景，都涉及到国境间的个人数据传输。例如，在风控业务中，有的外资机构帮助中国客户在全球范围内进行投资，建设全球风控系统需要掌握较敏感的数据。

在制造业，全球化产业链发展格局下，制造业涉及大量数据协同过程，以实现优化配置和降本增效，如当前市场火热新能源领域汽车制造业，车企需要将海外数据存储在当地自有数据中心或公有云中，虽然不涉及到出口国当地个人信息跨境传输，但由于海外销售、研发等分支机构需要共用国内业务系统，会有研发、制造、销售、财务、运行等相关数据跨境流动的需求。

在物流行业，随着全球化贸易的增长和电子商务的兴起，跨境数据流通和整合为物流行业提供了高效便捷的信息管理和运营模式。通过数字化技术和跨境数据流通，全流程物流信息获取需求得以满足，物流公司可以实时获取全球运输、库存、订单等关键信息，实现供应链的可见性和精细化管理，更好地与海外供应商、制造商和客户进行合作和沟通，促进国际贸易的便捷性和可靠性。

在医疗行业，药物海外研发对于多样性的个人数据跨境需求显得更为迫切，药企需要收集、处理包括临床试验数据、试验样本中包含的人类遗传资源信息、患者的健康检测和管理数据等，这些数据部分属于重要数据和敏感个人信息。如我国药企向美国申请新药上市，需要向美国食品与药品管理局（FDA）提出新药临床试验审批申请（IND）和新药注册申请（NDA），并提交临床前研究、检测结果、药物组成、药物生产与质控程序数据。

在数字贸易，全球化产业的发展，对打通供应链、产业链、服务链从而实现三链贸易的整体打通，提出了“供应链可视化和跨境数据流通整合”的需求，其中跨境数据流通是实现供应链可视化的重要步骤。同时，伴随着数字技术的发展，通过数字技术延伸出来的数字人、元宇宙、NFT等相关数字服务和需求也相继产生，在数字服务和产品进行全球流通的背景下，跨境数据的流动是必然性的刚性需求，形成了一种跨境数据流通的新型生态系统。

(4) 跨境数据流通技术解决方案日趋成熟

当前跨境数据流通相关技术日趋成熟并广泛应用。依据我国现有法律法规要求及相关标准规范建议，强调企业应当建立数据跨境的技术能力体系，以规范和促进数据依法有序自由流动。主要从以下几个方面：

在数据资产梳理方面，数据分类分级技术将助力实现核心数据、重要数据、一般数据的高效识别以及与相应数据类别、数据安全等级的智能关联，从而大幅提升识别效率和安全性。

在数据分析处理方面，隐私计算技术将在助力企业实现“数据可用不可见，原始数据不出域”。已经有越来越多的企业将通过跨境部署隐私计算节点来完成重要数据或个人数据的处理分析。

在数据流动管理方面，区块链技术将有效助力实现跨境数据流通全生命周期的“防篡改、可追溯、可信任”，为国家及企业的个人信息保护合规审核和数据跨境流动安全监管审计工作提供有力的技术保障。

(5) 数据跨境措施持续促进外商投资和服务贸易发展

2020年8月，商务部在《全面深化服务贸易创新发展试点总体方案》中提出，要积极开展数据跨境传输安全管理试点，并选择了北京、天津、上海、广州、深圳等28个省市作为试点地区。2022年1月，国家发改委、商务部宣布将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。2023年7月，国务院公布《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》，其中首次提出建立数据出境的清单制度，回应了众多外商投资企业和国内企业的关注；同时在全国范围内统一适用数据出境安全评估、标准合同、认证认可的“三件套”监管措施中，另单设京津

沪粤四地“试点探索”形成“可自由流动”的“一般数据清单”，此举是国家发展大战略之一京津冀一体化的通盘考虑，覆盖环渤海、长三角、珠三角国内三个重要经济带。

1.2. 粤港澳大湾区跨境数据流通的发展现状

粤港澳大湾区是我国跨境数据流通的重要节点，作为一个重要的经济合作区域，涉及“一个国家、两种制度、三个关税区、三种货币”，具备强大的经济发展实力和跨境数据流通需求。大湾区以率先探索制定数据跨境流动规则，拥有庞大的数据跨境流动应用场景和基础设施，其在数据流动方面的地位与影响力日益凸显，成为了我国跨境数据流通的重要支撑，是进行跨境数据流通研究的先行试验田。粤港澳大湾区并结合行业需求，产生了一大批的经典应用案例。**在金融领域**，粤澳上线跨境数据验证平台，利用区块链技术，以金融信息为试行范畴，在个人资产信息、企业资产证明和核数证明等业务场景方面实现跨银行、跨机构间的数据验证服务。**在医疗领域**，粤港实现电子病历跨境互通，香港大学深圳医院通过电子健康纪录互通系统（简称“医健通”）实现电子病历跨境互通。**在政务领域**，粤港澳实现政务“跨境通办”，江门市在香港和澳门设立“跨境通办政务服务专区”，推出“湾区政务通”可视化智慧服务柜台，通过引入线上身份核验、远程视频、数字空间、区块链等新技术促进跨境政务数据可信共享，实现涵盖商事登记、不动产登记、公积金、社保等多项高频服务的跨境办理。**在科研领域**，中国澳门与欧盟实现科研数据共享，澳门与欧盟合作构建“中国澳门—欧盟数据跨境流动通道”，以科研数据为突破点，探索出包括规则、技术和管理的治理机制，采用 IPV6、隐私增强、区块链等技术确保数据流动的可追溯和可管控，实现了科研数据安全有序跨境双向传输。**在教育领域**，粤港澳大湾区已成为我国科研创新中心，数十家境外高校陆续在广东办学或成立实验室，其中包括香港中文大学、香港科技大学、香港浸会大学、澳门科技大学等，通过合作办学的推动，进一步推动了校区之间包括人员身份信息、实验室科研数据、管理规则技术体系的跨境数据流通共享。

总体而言，粤港澳大湾区在促进数据跨境流动方面先行先试，成效显著，但当前仍面临数据跨境难以同时实现数据安全、隐私保护和自由流动三大目标的“三元悖论”，数字基础设施互联互通仍存在一定障碍。

1.3. 全球跨境数据流通的发展趋势

伴随着产业全球协同化发展和数字经济的全面到来，在全球范围内进行的跨

境数据流通愈发变得频繁，成为全球经济发展过程中的刚性需求。通过对全球跨境数据流通的现状进行深入分析，全球跨境数据流通具有以下发展趋势：**一是数据跨境治理政策愈发明确。**一方面，全球数据跨境流动的政策、规则 and 标准存在越来越多的共同点、互补性和趋同因素，都聚焦数据跨境安全保护和自由流动双重目标。另一方面，数据跨境流动全球的监管力度、约束规则、惩戒措施，虽总体趋向严格和出现相关处罚案例，但相关的跨境数据流通的政策已愈发清晰具体。**二是数据主权之争愈演愈烈。**数据是基础性、战略性资源，数据主权之争成为国家冲突的新形态，许多国家和国际组织积极推动数据主权战略部署和政策规制；迄今，全球近 60 个国家和地区出台了数据主权相关法律或战略；特别是美欧滥用长臂管辖进一步导致数据主权冲突加剧。**三是数据跨境安全面临新技术冲击。**生成式人工智能等新技术的发展促进数据应用场景和主体日益多样化，同时也给数据安全带来新的威胁，导致隐秘在新技术外衣下的数据泄露、数据贩卖、数据侵权等数据跨境安全事件频发；如用户在使用 ChatGPT 的过程中若使用不当，将对个人隐私、商业秘密、国家安全造成严重威胁。**四是数据本地化趋势上升。**出于国家主权、数据安全、个人信息保护等多种因素的考虑，越来越多的国家和地区采取数据本地化措施，限制部分相关重要数据跨境流动；同时，这些措施的限制性越来越强，许多措施涉及禁止数据流动的存储要求。

1.4. 我国跨境数据流通发展面临的挑战

我国跨境数据流通发展整体呈现出蓬勃发展之势，但综合分析现状和未来趋势，当前仍存在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、跨境数据流通安全评估成本高和耗时长、境外直接面向境内收集数据主体的申报难、大模型训练数据来源广泛导致监管难度加大等五个方面的问题和挑战。

(1) 跨境数据流通实施标准和落地措施不足

国家发布的《数据出境安全评估办法》《工业和信息化领域数据安全管理办法（试行）》《汽车数据安全若干规定（试行）》《重要数据识别指南（征求意见稿）》和《规范和促进数据跨境流动规定（征求意见稿）》已对数据和重要数据的范围进行了定义，明确了告知原则和解决了范围模糊的问题，并有效降低了数据处理者的合规成本；但在目前构建的数据跨境底座之上，我们仍然缺乏更加清晰的跨境数据相关标准、落地措施，以作为数据跨境流动的发展底层设施；如《数据出境安全评估申报指南》中对属于“数据出境”的行为做出了描述，但在具体业务中，企业仍缺乏更加细致统一多方互认的数据跨境标准和共通的落地执行措施。

(2) 境外主体数据安全保障能力评估受限

《数据出境安全评估办法》《个人信息出境标准合同办法》等法规对境外接收方的数据安全保障能力、个人向境外接收方主张权利的途径有效性评估进行了规定，但在具体核查评估过程中，仍然存在能够进行有效评估的企业数量有限、评估事项评估标准理解不清晰、人工梳理出境活动协调难还原不准确等问题，大多数企业仍主要是靠“在合同中进行约定的方式”来完成判定境外主体履行责任义务的管理和技术措施、能力等保障出境数据的安全，也只有零星几家企业有能力“派遣公司内部人员进行实地考察判断其管理和安全防护能力”。同时，在具体开展技术检测过程中，仅通过书面材料审核还是需要到境外对相应接收方进行审核的不确定性导致很难对另外主体的数据安全保障能力进行一个精确性的评估。

(3) 跨境数据流通安全评估成本高和耗时长

数据出境安全评估过程中，需对境内外双方数据出境场景规模必要性、境外接收方数据法律环境、数据安全保障能力、数据出境风险等进行评估，内容庞杂且复杂，评估内容涉及多层面、多维度，单一能力团队无法支撑。就所需要评估的内容，企业需要聘请内外部多方团队，如聘请外部律师事务所、咨询机构、技术单位进行评估申报、履行评估、整改和申报义务，总体花费的经济成本较高。同时，由于涉及的层面内容的多样性和多维度，处理评估、整改和申报相关手续及流程的时间周期较长，甚至可能经过多轮修改补充仍无法通过，在境内企业难以评估数据跨境风险和控制措施的有效性的情况下，评估周期有可能进一步拉长。

(4) 境外直接面向境内收集数据主体的申报难

根据《个人信息保护法》五十三条规定，本法第三条第二款（分析、评估境内自然人的行为）规定的中华人民共和国境外的个人信息处理者，应当在中华人民共和国境内设立专门机构或者指定代表，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。同时，《个人信息保护法》明确对于数据跨境业务和场景，应当依照个保法相关规定履行数据出境安全义务，强调对于满足数据出境安全评估条件的境外个人信息处理者，应当申报数据出境安全评估，并满足制度要求：仅具有独立法人资格的主体可以进行认证并持有认证证书。如境外主体或其境内不具有独立法人资格的分支机构需要进行认证，需由境外总部进行认证。现阶段而言对于境外数据处理者主体，面向境内收集数据也成为实务中难点。

(5) 大模型训练数据来源广泛导致监管难度加大

大模型训练数据中数据类型及数据来源多元复杂，包括他人隐私、个人信息、

智力成果等，使用这些数据训练模型存在侵犯他人个人隐私、个人信息等风险。在使用过程中，境内主体通过 API 接口形式接入境外大模型，还可能会伴随数据跨境传输及数据泄露风险。如众多个人用户跨境调用大模型服务，或导致数据积累违规跨境，业内多家大模型服务科技企业由于跨境调用大模型服务而致使企业陷入合规危机。在企业内部，企业在多场景应用训练时无法使用同一个模型，需采购或研发大模型（必要场景下国内外大模型都采用），这将使得企业面临中国境内一套模型，境外一套模型的境况，无法实现系统的整体统一监控，导致跨境数据传输的风险进一步加大，同样增加了跨境数据流通监管难度。

第二章 国际条约中的数据跨境规则

2.1. 总览

数据的跨境自由流动是当今世界经济发展必备的常态，应当在保障国家安全、经济安全和社会公共利益等少数必要情况下，尽可能促进和鼓励数据跨境流动，以便创造出更大的经济和社会价值。鉴此，产业界、学术界、社会公众对于简化和便利数据跨境流动监管手续的呼声持续高涨，国际组织、区域机构、各国政府也在积极探索和不懈推动。主要经济体基于自身立场、产业要求分别形成了两种不同的管理路径：一是倡导数据自由流动的全球化主义；二是以本地化存储、数据跨境审查为主要特征的本地主义。在此情况下，条约作为国家之间、政府间国际组织之间、国家与政府间国际组织之间缔结的国际协议，便发挥了最主要的契约型约束和造法性指引。

必须承认，目前数据跨境活动并未形成全球性规制体系。换言之，全球范围内暂不存在数据跨境流动监管中统一适用的“国际规则”，导致无专项性国际条约、无国际统一适用标准、无国际专业仲裁机构、无国际专项争端解决。“条约是确立国际法主体之前权利义务的书面的协定，是国际法渊源最主要体现。”目前国际法按照缔约方数量的划分，针对数据跨境这一特定问题构建权利和义务的国际条约：分为双边条约、诸边条约和多边条约。由于体例和篇幅的限制，本节简要分析涉及中国出境业务或对中国国内立法具有重要影响或参与国际规则谈判发挥范例效应的主要国际条约。

(1) 缺有效强制但顽强推进的多边条约

目前，多边条约主要中涉及部分数据跨境内容的国际组织成员签署的条约或主要国际治理机发布的宣言，由于成员间的立场和利益分歧、经济发展水平差异、执法水平经验和机构无法对齐，导致普遍缺乏强制力保障，主要有三类：一是经济合作与发展组织（OECD）于1980年确立的首部关于全球数据跨境流动执法原则立法--《隐私保护和个人数据跨境流动指南》、2013年制定的《OECD隐私框架》，中国为观察员身份未加入；二是二十国集团积极倡导于2019年签署的《数字经济大阪宣言》，中国加入；三是世界贸易组织（WTO）于1995年生效的《服务贸易总协定》、于1997年生效的《信息技术产品协议》、于2019年生效的《关于电子商务的联合声明》，中国均已加入。

值得关注的是，尽管存在数据主权、隐私安全、管辖权的政策议题争议诸多困难，国际多边组织始终在不懈努力积极推进。特别是不断有学者和产业人士呼

吁成立世界数据组织（WDO）并缔结管辖数据跨境并具备强制约束力的条约，虽目前看此提议遥遥无期，但无容置疑：统一适用的国际多边条约必是最终目标。

(2) 重区域适用但蓬勃发展的诸边条约

由于达成多边组织的广泛一致和签署具有约束效力的协商共识，近二十年来区域经贸协定和近年来的区域数字协定成为各经济体开展对外合作的主流，涉及数据跨境移动便利化规制的诸边条约主要有三类：一是中国已加入的具有相对广泛代表性的，比如亚太经合组织（APEC）各成员于 2005 年签署的《隐私保护框架》、2007 年签署的《数据隐私探路者协议》、2011 年开发的“跨境隐私规则体系”；二是针对中国正积极申请加入且具备较高水平的，包括 2018 年生效的《全面与进步跨太平洋伙伴关系协定》，特别是其中的数字贸易规则；2020 年新加坡、新西兰和智利（亦是 CPTPP 签署方）线上签署的《数字经济伙伴关系协定》，特别是其中应对数字经济对传统商业贸易治理产生的巨大挑战规定；三是国际上一体化程度十分紧密且为各成员广泛关注的，如 2020 年，美国、墨西哥、加拿大之间新的贸易协议——《美墨加协议》正式生效，该协议不仅正式承认了“APEC 跨境隐私规则体系”的有效性，而且要求确保数据跨境自由传输、最大限度减少数据存储与处理地点的限制以促进全球化的数字生态系统。

(3) 高标准雄心但数量有限的双边条约

基于美欧密切的经济联系和高科技的深度合作，2022 年《欧美数据隐私框架》达成。欧盟委员会不仅扩大数据跨境移动方面的规则解释，更是更新了标准合同条款，明确确保数据进口提供同等保护的责任主体在于将个人数据提供数据跨境的数据出口方。美国也提出了修补隐私盾协议的实质性承诺。

2.2. 具体条约中的数据跨境规则

本节将从具体的条约着手，简析其中的数据跨境规则。由于体例和篇幅的限制，我们挑选部分条约进行分析，供参考。

2.2.1. 基于世界贸易组织（WTO）框架下的重要多边条约

在全球发展数字经济的背景下，世界贸易组织（World Trade Organization, WTO）作为全球范围内的多边贸易组织拥有 164 个经济体成员，主要通过减免数字产品关税、推动跨境数据自由流动促进全球范围内信息技术产品贸易涉及数字服务贸易的统一化、便利化、自由化。

在不断涌现新兴技术的有力加持下，多种形式的国际贸易均可能涉及到相应的国际间数据跨境传输，相关成员关于数据跨境传输的法律和政策确实会影响贸

易开展。鉴于 WTO 框架目前主要针对基于贸易关切的数据跨境进行专项规制，在 WTO 体系下讨论数据跨境问题应从相关成员的国（境）内法律政策对贸易本身的影响考虑，从而援引相关贸易协定进行分析，本节侧重中国数据安全和个人信息保护开展例证。后续一节将重点讨论三个重要多边条约：《服务贸易总协定》（General Agreement on Trade in Services，以下简称 GATS）、《信息技术产品协议》（Information Technology Agreement，以下简称 ITA）、《关于电子商务的联合声明》（Joint Statement on Electronic Commerce，以下简称 JSEC）。

（1）《服务贸易总协定》（GATS）

GATS 是关贸总协定（GATT）乌拉圭回合谈判达成的第一套规范国际跨境服务贸易的具有法律效力的多边条约，于 1995 年 1 月正式生效，包括美国、欧盟、日本、澳大利亚、中国等 140 多个成员，其宗旨是在透明度和逐步自由化的条件下扩大服务贸易。GATS 规定国际服务贸易具体分为四种方式：跨境交付（cross-border supply）、境外消费（consumption abroad）、商业存在（commercial presence）、自然人流动（movement of natural persons），其核心是市场准入及具体承诺表（schedules of specific commitments）。GATS 中与数据流动有关的内容，缔约时放在计算机和相关服务（computer and related services）类别，其中包括数据处理服务（data processing services）。

如前所述，目前上没有一部专门管辖数据跨境的国际条约，WTO 规则中关于数据跨境传输的规制散见于各协定、备忘录、宣言中。WTO 各项协议中都存在少量例外条款，如果符合例外条款，则有关限制数据跨境流动的国（境）内监管措施将不构成违反 WTO 规则。这些例外规则暂时替代性地构成数据跨境流动的国际法基础，其中最为重要的是，GATS 的例外包括了第 14 条的“隐私例外”和“安全例外”，第 14 条之二的“基本安全例外”，具体为：

“隐私例外”系指第 14 条第 1 款的“为保护公共道德或维护公共秩序所必须的措施”；第 14 条第 3 款“为遵守法律或法规所必需的措施”及其第 2 项的“保护与个人信息（personal data）处理与传播有关的个人隐私及保护个人记录和账户的机密性”。

“安全例外”系指第 14 条第 3 款第 3 项的“安全（safety）”。

“基本安全例外”系指第 14 条之二第 1 款第 1 项的“（不得）要求任何成员提供其认为如披露则违背其基本安全利益（essential security interests）的任何信息（any information）”。

世界各国在国内立法以及开诸边经贸谈判、区域规则谈判过程中涉及数据跨境流动章节的规则设置时，包括紧接本节讨论的 CPTTP、DEPA、RECP 等诸边条约时，总体上均未超越 GATS 中限制跨境服务贸易的上述例外。

(2) 《信息技术产品协议》 (ITA)

ITA 是世界贸易组织于 1996 年 12 月 9 日至 13 日达成的协议，于 1997 年 4 月 1 日生效。它由世界贸易组织成员和申请加入国或单独关税区自愿参加，作为 WTO 框架下“次多边贸易协定”的新类型，ITA 的成果在最惠国待遇原则的基础上适用于所有成员，每个成员都可以从 ITA 缔约方的市场准入承诺中受益。

ITA 在 2015 年完成了扩围谈判，达成了《关于扩大信息技术产品贸易的部长宣言》，新增了 201 项产品。扩围谈判的成功使 ITA 适应了技术发展的现实，扩围后的 ITA 涵盖了尖端技术产品，例如自动数据处理设备、计算机、网络设备、医疗磁共振成像机、高端半导体、激光技术等。ITA 扩大了作为数字贸易基础的技术产品贸易，但 ITA 的规制局限于信息技术产品的关税削减机制，不包含任何形式的非关税壁垒的有约束力的承诺。数字贸易壁垒更多涉及边境后的非关税措施，尽管存在一定谈判深入中的举步维艰，ITA 为与信息技术相关的硬件贸易提供了非常自由的体制保障，极大地推动了信息技术在全球的普及和运用，从而促进了跨境数据流通。

(3) 《关于电子商务的联合声明》 (JSEC)

2019 年 1 月 25 日，在瑞士达沃斯举行的 WTO 电子商务非正式部长级会议上，中国、澳大利亚、日本、新加坡、美国、欧盟、俄罗斯、巴西、尼日利亚、缅甸等共计 76 个世贸成员签署 JCEC。

从多边拓展层面分析，JCEC 所积极倡导的 WTO 电子商务谈判已扩大到 90 个成员参与，形成覆盖数字相关 7 个领域 16 项议题；**从双边区域层面分析**，至 2023 年上半年，全球已签署超 130 个数字协定，其中多为双边、区域自贸协定 (FTA) 以及数字经济专门协定。**从历史演进层面分析**，JCEC 最早可以追溯至 WTO 于 1998 年成立的“电子商务工作计划”，强调将充分认识并考虑世贸组织成员在电子商务领域面临的独特机遇和挑战，鼓励所有成员参加谈判，以便使电子商务为企业、消费者和全球经济带来更大利益。**从发展理念层面分析**，WTO 成员形成三排意见：一是以美国为代表的发达经济体，主张跨境数据自由流动，对电子传输永久免证关税，并禁止数据本地化；二是以中国为代表的发展中经济体，呼吁建立以货物流动为主的跨境电子商务规则；三是以非洲、加勒比和太平洋岛国等相关成员，反对将数字贸易及跨境电子商务议题纳入多边贸易框架下讨论。

但近期出现重大的事件却将改变 ICEC 后续谈判的走向，2023 年 10 月 25 日，在瑞士日内瓦举行的 WTO 电子商务联合声明倡议会议期间，美国贸易代表凯瑟琳-戴办公室声明，美国在 WTO 电子商务规则谈判中放弃该国长期以来坚持的部分数字贸易主张，其中包括关于跨境数据自由流动的要求，并且美国正在审

查其在数据和源代码等敏感领域的贸易规则现行举措.....事态最终走向值得进一步关注。

(4) WTO 涉及数据跨境规则与中国立法的联系

我国制定的《网络安全法》、《数据安全法》、《个人信息保护法》等法律,《关键信息基础设施管理条例》、《网络数据安全条例(征求意见稿)》等行政法规,《网络安全审查办法》、《数据出境安全评估办法》等部门规章,对于重要数据跨境流动的限制、对于达到规定数量的个人信息出境从而会触发安全影响的评估,对于关基运营者在境内运营中收集和产生的个人信息和重要数据应在境内存储,这些措施都是援引 GATS 的“基本安全例外”来适度限制,其中对个人信息跨境流动的限制还会增加援引 GATS 的“隐私例外”和“安全例外”。特别指出的是,国家核心数据禁止出境、数据安全审查等事项可以援引“基本安全例外”,这两种限制措施都着眼于保障国家安全和重大公共利益,属于“基本安全”范畴。

另一方面, WTO 例外条款的适用旨在协调多边贸易自由化与国内公共政策目标之间的冲突,既保障成员方善意行使例外条款的权利,又保持多边贸易规则的包容性和灵活性。例外条款毕竟是在限缩明确条件和特定少数情况下适用,从既往涉及 GATS 例外条款的争端来看,无论是美国博彩案还是中国出版物及音像产品案,争端解决机构裁决中均采取了严格解释,认为例外条款的要件没有得到充分满足。遵循这一法律逻辑, GATS 例外条款似乎也难以支持成员方限制跨境数据流通,即便是欧盟 GDPR 似乎亦未满足 GATS 例外条款的适用条件。我国在数据出境安全评估的后续地方法规和细化的部门规章出台和具体执法实践中,也应秉持审慎的原则。

GATS 创设的隐私例外和安全例外存在共同的适用条件以及适用限制,即“为遵守国内法律法规所必需的措施”(称为“必要性测试”)、“实施措施不得构成任意或不合理的手段或者构成变相限制的前提下”(称为“非歧视性测试”)。目前,暂不确定主要国家和地区限制数据跨境流动的规则能够通过 GATS 第 14 条的“必要性测试”和“非歧视性测试”。同时, GATS 第 6.4 条规定服务贸易理事会应制定国内管制纪律,以“保证有关资格要求和程序、技术标准和许可要求的各项措施不致构成不必要的服务贸易壁垒”。这些多边规定和纪律要求在我国深入开展数据安全和隐私保护立法及其落地实践中必须得遵守。

2.2.2. 《区域全面经济伙伴关系协定》(RCEP)

《区域全面经济伙伴关系协定》(Regional Comprehensive Economic Partnership, RCEP) 由东盟于 2012 年发起,东盟十国和中国、日本、韩国、澳大利亚、新西兰等 15 个亚太国家共同制定的协定。2020 年 11 月 15 日,前述 15

个国家正式签署了 RCEP。2022 年 1 月 1 日，RCEP 正式生效，目前，该条约已在 15 个签约国中生效，中国是首批生效的国家之一。RCEP 的签署对我国扩大对外开放，形成国内国际双循环新发展格局，促进亚太地区区域协调均衡发展，提升区域经济一体化水平有重要意义。

RCEP 由序言、20 个章节和 4 部分市场准入附件共 56 个承诺表组成，是一个现代、全面、高质量、互惠的大型区域自贸协定。其中，关于数据跨境的规定主要集中在第十二章“电子商务”。RCEP 在原则上倡导和鼓励跨境数据的自由流动，但考虑到各国在数字经济和数据治理水平方面的差异，相应的也做出了例外规定，如允许各缔约国基于“实现合法的公共政策目标”及“保护基本安全利益”采取必要措施。RCEP 关于数据跨境的具体规定如下：

(1) 个人信息保护的要求

对于个人信息保护，RCEP 要求各缔约国应制定法律保护电子商务用户的个人信息，且在制定相应法律时应考虑相关国际组织或机构的国际标准、原则、指南和准则，并应向电子商务用户提供“个人如何需求救济、企业如何遵守法律要求”等关于个人信息保护的信息。同时，鼓励法人公布其与个人信息保护相关的政策和程序。

(2) 推动各缔约国间数据跨境自由流通

围绕着“促进缔约方之间的电子商务，以及全球范围内电子商务的更广泛使用”的目标，RCEP 在第十二章第十一条规定缔约方不对电子传输征收关税；第十四条第二款规定了不得强制将数据“本地化”作为在该缔约方领土内进行商业行为的条件；第十五条第二款规定“一缔约方不得阻止涵盖的人为进行商业行为而通过电子方式跨境传输信息。”即使在监管较重的金融领域及电信领域，RCEP 在其第八章服务贸易的附件一及附件二中也作出了相应规定，原则上应允许相应领域的数据自由跨境流通。

(3) 以“合法的公共政策目标”及“基本安全利益”为例外的流通限制规定

RCEP 以促进数据跨境自由流通为原则，但也为各缔约国作出了例外规定，构建一套“原则+例外”的数据跨境流通规则体系。例外情形主要有两种情形，一是基于合法的公共政策目标采取的必要措施，在 RCEP 序言中即已表明“每一缔约方为实现合法的公共福利目标而进行监管的权利”，在第十二章第十四条第三款第（一）项，第十五条第三款第（一）项做出了相应规定。在金融领域，也对数据本地化做出了例外规定，在不作为规避 RCEP 项下承诺或义务手段的前提下，可以要求金融服务提供者将数据在本地进行存储。二是基于安全采取的必要

措施。该例外主要规定于第二章第十四条第三款第（二）项，第十五条第三款第（三）项。电信领域也有类似规定，在不够成“任意的或不合理歧视或变相限制”的前提下，可以采取保护措施保证信息的安全性和机密性，并且保护公共电信网络或服务终端用户的个人信息。

（4）灵活的争端解决方案

RCEP 第十九章是专门的争端解决条款，但第十二章第十七条对此作出了限制规定。根据该条的规定，缔约国如果对第十二章的解释和适用存在分歧的，首先应善意的进行磋商，尽最大努力达成共同满意的解决方案。如磋商未能解决分歧的，可将分歧提交至 RCEP 联合委员会，第十二章电子商务的争议不适用第十九章关于争端解决的规定，但未来可对该条款进行一般性审议，在审议完成后，就电子商务分歧，可以在同意适用的缔约国间适用争端解决机制。

2.2.3. 《全面与进步跨太平洋伙伴关系协定》（CPTPP）

全面与进步跨太平洋伙伴关系协定（Comprehensive and Progressive Agreement for Trans-Pacific Partnership, CPTPP）《跨太平洋伙伴关系协定》（Trans-Pacific Partnership Agreement, TPP），在美国退出后，原 11 个 TPP 成员国于 2018 年 3 月在智利首都圣地亚哥共同发表声明，宣布新的协议已经达成并正式更名为 CPTPP。2021 年 9 月 16 日，中国商务部部长王文涛向 CPTPP 保存方新西兰贸易与出口增长部长奥康纳提交了中国正式申请加入 CPTPP 的书面信函。同 RCEP，CPTPP 并非专门的关于数字经济，数据贸易的协定，而是一个全面的区域贸易协定，但其中关于数字经济、数据贸易的规定是协定的重要组成部分。

CPTPP 由全面与进步跨太平洋伙伴关系协定、序言、30 个章节及附件全面与《进步跨太平洋伙伴关系协定委员会关于 CPTPP 加入程序的决定》组成，其中关于数据跨境的规定集中于第十四章电子商务一章。与 RCEP 相同，CPTPP 也采取了“原则+例外”的模式对数据跨境进行规定，两者原则上都鼓励跨境数据的自由流动，但在数据流通的自由度上有所差异，具体分析如下：

（1）建立促进不同个人信息保护体制间的兼容性的机制

CPTPP 在个人信息保护方面的规定与 RCEP 相似，但较 RCEP 更进一步的是，考虑到缔约方可能采取不同法律方式保护个人信息，CPTPP 提出每一缔约方应鼓励建立促进这些不同体制之间兼容性的机制。这些机制可包括对监管结果的承认，无论是自主给予还是通过共同安排，或通过更广泛的国际框架。为此，缔约方应努力就其管辖范围内适用的此类机制交流信息，并探索扩大此类安排或其他适当 安排的途径以促进各机制之间的兼容性。

(2) 促进各缔约国间的数据自由流通

CPTPP 通过不对缔约方间的电子传输征收关税，数字产品的非歧视待遇，允许通过电子方式跨境传输信息，不强制将数据本地化作为在其领土内开展业务的条件，不强制开放源代码等进行规定，促进数据在各缔约国间自由流通。

(3) 更为自由的数据跨境自由流通规则

相较于 RCEP，CPTPP 关于数据跨境流通的规则更加自由，除了前述提到的 RCEP 未做规定的数字产品的非歧视待遇，不强制开放源代码等外，在海关关税上两者也存在差异，RCEP 的关税规定属于“临时性”规定，而 CPTPP 的要求则较为严格，不仅“永久性”免征电子传输关税，还明确要求涵盖电子传输的内容，即数字产品。此外，CPTPP 在例外规定方面有更严格的限制。关于“实现合法公共政策目标”的必要措施，CPTPP 在不构成任意或不合理歧视或对贸易构成变相限制之外规定了不对信息传输施加超出实现目标所需限度的限制。CPTPP 并未将“保护基本安全利益”作为例外情况进行规定。

2.2.4. 《数字经济伙伴关系协定》（DEPA）

《数字经济伙伴关系协定》（DIGITAL ECONOMY PARTNERSHIP AGREEMENT, DEPA）由新西兰、智利和新加坡三国于 2020 年 6 月 12 日在线上签署，于同年 12 月 28 日生效。与 RCEP、CPTPP 不同，DEPA 是全球第一个关于数字经济的专项协定，因此，尽管该协定由三个经济体量较小的国家提出，但在一定程度上为全球数字经济制度提供了模板。中国目前正积极推动加入 DEPA，已正式于 2021 年 11 月 1 日向 DEPA 保存方新西兰提交了加入申请。2022 年 8 月 18 日，根据 DEPA 联合委员会的决定，中国加入 DEPA 工作组正式成立，将全面推进中国加入 DEPA 的谈判进程。2022 年 12 月 5 日、4 月 25 日，中国已就加入 DEPA 进行了两次首席谈判代表会议，并于 2023 年 3 月 28 日举行第一次技术磋商。

DEPA 深度借鉴了 CPTPP 中的数字贸易条款并对其进行细化归类，将文本分为了十六章，涵盖了商业和贸易便利化、数字产品待遇、数据问题、数字身份、新兴趋势和技术、创新和数字经济、数字包容性等内容。可以说，DEPA 非常全面的就数字贸易问题做出了详细规定，但限于篇幅和体例，我们主要就数据跨境的规则进行简析。

(1) 个人信息保护

DEPA 第 4.2 条用了十个条款对个人信息进行了规定，除与 RCEP、CPTPP 相同的地方外，主要在以下几点做出了不同的规定：

首先是对个人信息保护法律框架应包含的原则做出了规定。主要包含了八大原则，分别是收集限制、数据质量、用途说明、使用限制、安全保障、透明度、个人参与及责任。

其次是不对电子商务用户违反个人信息保护规定的行为采取歧视性做法。

再次，在促进不同个人信息保护体制的兼容和交互方面，相较 CPTPP，规定了在可行时，对各自法律框架下的可信任标志或认证框架所提供的相当水平的保护给予适当承认，或建立缔约方之间个人信息转移的其他途径。

最后，应鼓励企业采用数据保护可信任标志，以帮助验证其符合个人数据保护标准和最佳做法，并推动各缔约国间对他国数据可信任标志的承认。

(2) 与 CPTPP 相似的例外限制

在通过电子方式跨境传输信息、数据本地化要求方面，DEPA 第 4.3 条和第 4.4 条的规定与 CPTPP 相似，对于相关规定的限制均要求不得构成任意或不合理歧视或对贸易构成变相限制且不对信息传输施加超出实现目标所需限度的限制。

(3) 推动数据开放，实现数据驱动开放

DEPA 关于数据开放主要分为两部分。一是企业数据的开放，通过数据监管沙盒机制，可信数据共享框架和开放许可协议等推动跨境数据流通和数据共享，从而实现数据驱动的创新。其次是政府公共数据的开放，DEPA 鼓励各缔约方就政府公共数据开放开展合作，从而扩大获取和使用公共数据的方式。合作方式包括共同确定可利用开放数据集、鼓励开发以开放数据集为基础的新产品和服务及推动使用和开发通过可在线获得的以标准化公共许可证为形式的开放数据许可模式。

2.3. 对中国数据跨境管理的启示

推动数据的跨境有序自由流动绝非一国之力可以完成，各国间数字经济发展水平不一，利益诉求不一，法律体系不一，很难通过一国立法或标准来实现数据跨境标准和规则的统一。因此，才需诉诸于双边、诸边或多边协议来实现各国、各地区间的利益协商和标准统一，从而促进数据跨境的有序自由流动。无论是我国已经加入的 WTO，RCEP，还是正在推动加入的 CPTPP、DEPA，均是我国在这方面的尝试和探索。这条路并非一条容易的道路，相关条约的规定与我国现行法律之间存在一定的差异，对于加入相关协定，势必会对我国现有法律体系造成冲击，如何平衡好国家数据主权与数据跨境流动在未来一段时间需要重点探索。但无论如何，积极对接国际标准，促进数据跨境有序自由流动已是正在推进也应积极推进的事业。在全球范围内暂不存在数据跨境流动监管中统一适用的“国际

规则”的当下，探索并推广中国模式，发出中国声音的绝佳机会。

第三章 数据跨境域外法律环境分析

本章将以“一带一路”为线索，按地理顺序对具体国家或地区的数据跨境规则进行介绍。国际条约的落地依赖于各缔约方立法的转化，相关条约也允许缔约方对条约进行例外规定，了解不同国家或地区间的数据跨境规则，对于实际开展数据跨境活动十分必要。更为重要的是，跨境数据流通双方对跨境数据具有相对一致的保护水平是当前数据跨境流动风险管控的共识。对于中国境内的数据处理者，对境外接收方所在地法律对数据跨境的影响进行评估是履行《数据出境安全评估办法》等规章的规定的义务。

3.1. 中国香港

3.1.1. 推动数字经济发展，打造亚太地区数据中心设立首选地

香港是国际金融、贸易及物流的重要枢纽，众多跨国企业及国际机构将地区办事处或地区总部设立于此。随着数字经济发展以及网络数据体量与日俱增，有关企业及机构对高效能和安全可靠的数据中心设施和服务的需求越来越殷切。为此，香港特别行政区政府近年来积极推广香港的电讯基础设施、有利营商环境、资讯自由、人才体系、土地供应优惠政策等优势，并推出了包括设立数据中心促进组及专题网站、将工业大厦改装作数据中心用途、预留数据中心等多项促进措施，致力促进香港成为在亚太地区内设立数据中心的首选地点。为进一步促进香港的数字化经济发展，香港特别行政区政府于2022年6月成立了数字化经济发展委员会，负责制定有关鼓励不同行业采用数字化的策略和措施及推进数据服务的产业和数字化政府的发展等。该委员会特别成立了跨境数据协作小组、数码基建工作小组、数码转型工作小组及人才发展工作小组，以分析确定数据流通、数字化基建、数字化转型及人才培养方面的具体促进措施。

此外，香港也抓住了国家推动建设“一带一路”数字丝绸之路和粤港澳大湾区数据中心的机遇谋求自身发展，2023年，香港特区政府在促进大湾区数据跨境流动方面更是向前迈进了重要一步，其专门负责香港创新科技政策的创新科技及工业局携手与中国国家互联网信息办公室于2023年6月29日签署了《促进粤港澳大湾区数据跨境流动的合作备忘录》，以期会同中国国家互联网信息办公室采取有效管理措施，推动建立粤港澳大湾区数据跨境流动安全规则，共同促进粤港澳大湾区数据跨境安全有序流动。

3.1.2. 香港数据保护及数据跨境的要点简析

(1) 亚洲最早全面保障个人资料的法域之一

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》《香港特别行政区基本法》《个人资料（私隐）条例》，其中涉及个人资料保护的相关规定内容概述如下：

《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。”

《香港特别行政区基本法》

1997 年，《香港特别行政区基本法》正式实施（后其附件经数次修订）。《香港特别行政区基本法》第三十九条确认了《公民权利和政治权利国际公约》中“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”。《香港特别行政区基本法》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》（以下简称“《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），是亚洲最早出台的全面保障个人资料（私隐）的法例之一。《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。

(2) 个人资料私隐专员

根据《私隐条例》第 5 条之规定，为监察《私隐条例》的施行，设立“个人资料私隐专员”（以下简称“私隐专员”）职位。该职位由香港特别行政区行政长官委任一人，任期为 5 年，至多连任一次。

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

(3) 推行港股实名制：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（以下简称“香港证监会”）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。此后香港证监会发布了一系列公告为该制度的落地做准备，并于 2023 年 3 月 31 日的通告中公布，该制度已于 2023 年 3 月 20 日成功推出。在该制度实施后，相关受规管的中介人须在取得其客户的明示同意后向香港联合交易所有限公司（以下简称“香港联交所”）提交有关识别信息（即客户的名称及身份证明文件资料），以符合香港证监会及相关的私隐法例规定的要求。如投资者不提供所需同意，则只能出售、转出或提取已持有的证券，而不得在香港联交所买入证券。因此如果境内用户需要在香港进行证券交易，需要提供相关的身份证明文件，涉及数据的跨境流动。

(4) 构建以《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

在香港，跨境个人数据保护的监管职责主要由公署承担，该公署与境外相关机构协同处理跨境个人数据的保障事宜。《私隐条例》的第 33 条对个人资料转移至香港以外的地方作出严谨和全面的规管，除在条例指明的情况下，明确禁止把个人资料转移到香港以外的地方，以确保该条例对个人资料被转移后所提供的保障不会被削弱。虽然该第 33 条至今尚未施行，但为了更好指引资料使用者保障个人资料跨境转移并为企业提供最可行方式的建议，公署于 2014 年 12 月 29 日发布了《保障个人资料：跨境资料转移指引》（以下简称“《2014 指引》”），并特别拟备了一份建议范本条文，协助资料使用者制定与境外资料接收者订立的跨境资料转移协议。《2014 指引》明确指出，《私隐条例》第 33 条的适用范围：“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资料使用者所控制；但如果一个位于香港的个人或实体经互联网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（在传输中资料没有被查阅或储存），则不属于第 33 条调整的范畴”。2022 年 5 月，公署发布了更新的《跨境资料转移指引：建议合约条文范本》（以下简称“《指引》”）与《建议合约条文范本》（以下简称“《范本》”）（详见附件 1.1），该等《指引》和《范本》均非强制性规范，属于自愿遵守性质。

3.1.3. 香港与中国大陆个人信息保护法规之对比情况

(1) 两地保护思路较为一致

香港地区《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。

(2) 保护强度存在一定差异

在个人信息保护范围、保护义务、法律责任等方面，香港地区《私隐条例》与大陆《个保法》的保护强度存在一定差异。具体而言，对于个人信息的保护范围，香港对“个人资料”的定义强调“确定性”，即强调能够确定具体个人身份的资料才属于“个人资料”，而大陆《个保法》则遵循了“可识别性”的定义思路，对“个人信息”的定义包含了“已识别”和“可识别”两个层面，既涵盖了具体个人身份信息，也涵盖了与个人关联的信息。此外，《个保法》还对敏感个人信息作出了专门的定义和明确的处理规定。相较而言，大陆对个人信息的保护范围更广。对于个人信息的保护义务，香港并无本地化存储、个人信息保护影响评估、指定个人信息保护负责人、自动化决策等相关要求，而大陆对该等方面明确地作出了规制。行政罚款权限和惩处力度方面，香港的个人信息监管机构没有罚款的权力，香港《私隐条例》规定的最高罚款额度仅100万港元，实务中，罚款额度普遍在5万港元以下，而根据大陆《个保法》规定，履行个人保护职责的有关机构最高可处违法者以五千万元以下或者上一年度营业额百分之五的罚款，对企业具有明显的震慑力。

(3) 个人信息跨境转移的管理规则不同

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，可跨境传输个人信息。香港《私隐条例》第33条关于个人资料跨境转移的规定尚未正式实施，目前仅有《指引》作为参考。由于存在上述差异，加上两地对个人信息的保护强度不同，在大陆与香港数据跨境流通合作中，存在着制度衔接的问题。不过，从大陆与香港地区的个人信息保护思路、保护强度来看，一般情况下，中国大陆主体向香港地区传输数据时，香港地区数据接收方的合规程度通常能够满足要求。结合粤港澳大湾区建设及数据互联互通机制深化的总体背景，香港与内地两地的数据跨境主要有赖于数据跨境流动双方的安全保障能力和个人信息权益保障的响应。

3.2. 中国澳门

3.2.1. 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》。截至2023年9月，澳门并未制定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），该机构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款及《个资法》所指之公共当局，行使法律赋予的职权，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，澳门《个资法》的制定早于中国大陆《个人信息保护法》（以下简称“《个保法》”）16年。由于历史的渊源，澳门较早地制定了完整的个人资料保护法律规范，但从实践层面上来看，澳门对公民个人资料跨境的规定并不完善，没有形成类似于欧盟白名单这样的具体标准，而主要是依据个人资料保护办公室的意见判断决定。根据个人资料保护办公室的公开信息，自2019年起，截至2023年9月尚未有个人资料保护相关的意见书发布。

3.2.2. 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。

(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。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，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) 转移是保护重要的公共利益，或是在司法诉讼中宣告、行使或维护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申请许可。

3.2.3. 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。

3.3. 中国台湾

3.3.1. 台湾地区个人资料保护及跨境流通监管的法律环境

(1) 逐步完善的个人资料保护立法

20 世纪 90 年代起，受欧美国家的影响，我国台湾地区开始重视个人资料保护问题。为满足当地民众对于个人资料保护的主观诉求并促进对外贸易，台湾地区的政府成立了专门小组研究个人资料保护相关法律问题，并于 1990 年开启了个人资料保护立法。1991 年 9 月，台湾地区法务部成立了专门小组负责起草相关法律法规，并于 1995 年 8 月公布施行了《电脑处理个人资料保护法》（以下简称“《电资法》”），于 1996 年 6 月公布了《电脑处理个人资料保护法施行细则》。由于面临诸多质疑，法务部于 2012 年颁布了修正后的《个人资料保护法》（以下简称“《个资法》”）及《个人资料保护法施行细则》（以下简称“《个资法施行细则》”），其于 2012 年 10 月 1 日正式实施。自此，《个资法》及《个资法施行细则》经历多次修正，至今为我国台湾地区个人资料保护的基本规范。

(2) 加入 CBPRs，促进数据跨境流通

为了促进数据跨境流通，我国台湾地区于 2018 年 12 月加入了亚太经济合作

组织 (Asia-Pacific Economic Cooperation, 以下简称“APEC”) 框架下的跨境信息传输区域安排“跨境隐私规则体制” (Cross-Border Privacy Rules System, 以下简称“CBPRs”)。CBPRs 的基本逻辑是, 如果位于不同经济体的不同公司, 统一承诺并遵循“APEC 隐私框架”提出的九大个人数据保护原则, 则个人数据在这些公司之间的传输就不应受到阻碍, 获批准加入CBPRs 的成员国家或地区的政府会指定一个或多个法人担任“问责代理机构” (Accountability Agents), 经 CBPRs 认可的问责机构通过认证成员国家或地区内其他企业或组织使这些“认证企业”最终成为 CBPRs 的真正参与者。此后, 我国台湾地区资讯工业策进会于 2021 年 6 月 3 日经审查认证成为问责代理机构。截至目前, 美国、日本、墨西哥、加拿大、新加坡、韩国、澳大利亚、我国台湾地区及菲律宾已加入CBPRs。

(3) 以临床试验及海关检验为代表的数据库互通探索

海峡两岸在数据库互通问题上进行了很多探索。例如在临床试验方面, 海峡两岸关系协会与台湾海峡交流基金会签署的《海峡两岸医药卫生合作协议》于 2011 年 6 月 26 日正式生效后, 两岸展开了一系列合作。2014 年台湾“食品药物管理署”委托台北荣民总医院启动了《建立两岸临床试验中心合作计划》。在此框架协议下, 两岸 8 家临床试验中心签署了合作意向书, 承认对方所做的符合 ICH 的临床试验数据。2016 年 4 月 25 日国家食品药品监督管理总局发文《两岸开展药物临床试验机构的共同认定》, 其中明确了大陆药品注册申请人可以委托 4 家台湾医院 (台北荣民总医院、三军总医院、台湾大学医学院附属医院、林口长庚纪念医院), 按照两岸有关监管要求, 开展药物临床试验, 符合要求的临床试验数据可用于在大陆申报药品注册。

在海关检验方面, 福建检验检疫局于 2015 年组织两岸检验建议数据交换测试工作, 通过两岸检验检疫数据交换中心实现了与台湾关贸网的双向数据互通, 双方均成功接收到了来自对方的电子通讯报文, 这标志着两岸检验检疫数据的“电子跨海大桥”已经成功“对接合拢”。近期, 中国工业合作协会、北京海峡两岸民间交流促进会和台湾工业合作协会于 2023 年 9 月共同举办海峡两岸数字经济交流研讨会, 来自海峡两岸相关协会、科研院校、金融、制造业、互联网、文旅、数字技术等领域的 60 多位专家、学者和企业家在会上针对“海峡两岸数字经济协同发展的机遇与挑战”共同探讨了两岸数字经济发展方面的交流与合作。

3.3.2. 我国台湾地区数据保护及数据跨境的要点简析

(1) 《个资法》的适用主体及适用范围

在台湾发生的所有个人资料的收集、处理和使用活动 (不论信息当事人是否是台湾籍、实施该活动的主体是否为台湾境内主体) 均必须遵守《个资法》。另

外，该法区分了公务机关和非公务机关，并对它们在收集、处理和使用个人资料方面设置了不同的规定，其中非公务机关包括不属于台湾地区公务机关的任何个人或实体。

根据《个资法》，个人资料指自然人的姓名、出生日期、身份证号码、护照号码、特征、指纹、婚姻状况、家庭信息、教育背景、职业、医疗记录、医疗保健资料、遗传资料、性生活资料、体检记录、犯罪记录、联系方式、经济状况、有关个人社会活动的资料及其他可以直接或间接用于确定自然人的资料。其中，收集、处理或使用有关自然人的医疗记录、医疗保健资料、遗传资料、性生活资料、体检记录、犯罪记录须符合更高的标准。

(2) 对数据跨境传输采取“原则允许，例外禁止”的立法思路

我国台湾地区在立法上对于数据传输采取“原则允许，例外禁止”的态度。在《个资法》中，仅对非公务机关设置了跨境传输个人资料的限制：根据《个资法》第 21 条规定，有以下情形之一的，监管机关可以对其进行限制：（1）“涉及国家重大利益”；（2）“国际条约或协定有特别规定”；（3）“接受国对个人资料的保护没有完善之法规，致有损当事人权益之虞”；（4）“以迂回方式向第三国（地区）传输个人资料以规避《个资法》的情形”。因此，依据《个资法》规定，在监管机关未限制国际传输个人资料前，非公务机关基于合法收集、处理及利用要件，即可将个人资料进行跨境传输。

此外，我国台湾地区的行业主管部门可以发布适用于相关行业的个人资料跨境传输的规则和规定，对行业内的主体进行跨境资料传输方面的限制。台湾地区行政院于 2021 年 8 月进一步制定了实行个人资料保护的合作规范指引，规定各部委应修订针对受其监督的特定行业部门的现行个人资料保护法规，要求各部委应定期认真研究是否有必要制定针对受其监督的特定行业部门的新的数据保护法规，且应考虑相关行业非公务机关的规模、所保留的个人资料的数量或性质、数据泄露对数据主体的潜在影响及跨境数据传输的频率等因素。

(3) 数据跨境传输的监管部门

在 2018 年 7 月以前，我国台湾地区法务部负责解释《个人资料保护法》，在我国台湾地区发展委员会下属机构个人资料保护专案办公室于 2018 年 7 月 4 日成立以后，《个人资料保护法》的解释权于 2018 年 7 月 25 日正式移交给发展委员会。2023 年 5 月，台湾地区立法院通过了《个资法》的修正草案，补充了《个资法》第 1 条之 1 规定，规定由个人资料保护委员会担任《个资法》主管机构。未来个人资料保护委员会将作为专责机关，整体规划对于公务机关及非公务机关个人资料保护的监管机制，解决目前《个资法》分散式管理下的实务监管问题。

3.3.3. 我国台湾地区《个人资料保护法》与大陆《个人信息保护法》的衔接与差异

《个资法》施行早于大陆《个保法》，两者均吸收了 GDPR 相关思路和经验，因此在保护模式上大致相同。但整体而言《个资法》的侧重点在敏感个人信息及弱势群体的保护，比如对敏感个人信息具体规定了特殊保护，并鼓励公益诉讼、规定团队诉讼减免诉讼费等。该法对于个人信息跨境传输原则上允许，没有设置过多的限制，对信息本地化也没有明确要求，而是通过台湾当局在《个资法》的基础上通过颁布行政指令的方式规定信息本地化储存的规则，以及对特定传输进行限制。《个保法》虽然也规定了敏感个人信息的保护以及公益诉讼，但较为笼统，将更多的重点放在了跨境信息流动规制上，注重国家层面的信息和数据安全。

此外，我国台湾地区的《个资法》不仅规定了民事责任，还区分主体规定了详细的行政责任和刑事责任。如第四十一条规定了违反本法收集处理个人信息导致损害他人利益的将会被判处有期徒刑或罚金的刑事责任，第五十条规定了有关主体在非公务机关受到罚款的行政处罚时，若不能证明自己尽到防止义务，也要承担与非公务机关一样数额的罚款，第二十八条规定了公务机关违反本法导致个人信息泄露或者是有其他侵害信息主体权利行为且无免责事由的，要承担损害赔偿赔偿责任。《个资法》甚至对特殊情况的量刑也做出了统一规定，比如第四十四条规定“公务员假借职务上之权力、机会或方法，犯本章之罪者，加重其刑至二分之一”。我国大陆境内的制度框架则结合《个保法》《民法典》《行政法》和《刑法》等多部门法进行规制，没在《个保法》中进行详细的统一规定。

3.4 东盟

东南亚国家联盟（Association of Southeast Asian Nations，简称“东盟”）成立于 1967 年，截至 2023 年 10 月，成员国包括印度尼西亚、泰国、新加坡、菲律宾、文莱、马来西亚、越南、老挝、柬埔寨和缅甸 10 国。东帝汶是东盟候选成员国，巴布亚新几内亚是东盟观察员国。

东盟稳步推进东盟共同体建设，目前已发展成为东南亚地区以经济合作为基础的政治安全、经济和社会文化一体化的合作组织，并建立起一系列的合作机制。东盟与中国、日本、韩国、印度、澳大利亚、新西兰、美国、俄罗斯、加拿大、欧盟、英国等 11 个国家和国际组织建立了对话伙伴关系。在经贸合作方面，东盟已经与中国、中国香港、日本、韩国、印度、澳大利亚及新西兰分别达成自由贸易协定或经济伙伴协定。2022 年 1 月 1 日，由东盟主导发起的《区域全面经济伙伴关系协定》（RCEP）正式生效实施。2023 年 6 月 2 日，RCEP 对东盟十国

和中国、日本、韩国、澳大利亚、新西兰 15 个成员全面生效，全球最大经济规模的自由贸易区进入全面实施新阶段。

东盟目前是亚洲第三大经济体，世界第五大经济体，也是中国第一大贸易合作伙伴。因此，促进数据跨境流动对中国和东盟的双边贸易有及其重要的意义。

3.4.1. 出台系列指导性政策文件，统筹数字经济发展与数据保护

东盟作为一个重要的区域性组织，基于对外经贸的需要，一方面在数据治理和数据跨境流动领域亟需建立协调统一的合规路径和机制；而另一方面，因东盟各成员国国内法针对数据保护机制的成熟度和数据治理水平差异较大，除了新加坡、泰国、马来西亚、菲律宾、印尼、越南出台数据保护的相关法律法规外，柬埔寨、老挝、缅甸和文莱等其他国家尚未出台数据保护的相关法律。因此，东盟陆续出台了一系列具有灵活性、包容性和指导性的政策文件，以帮助东盟各成员国内的企业和组织根据自身的业务情况，自愿参考适用。

为此，东盟于 2016 年出台《东盟个人数据保护框架》，提出保护数据、支持数字贸易和创新。2018 年制定《东盟数字信息治理框架》，促进东盟跨境数据流通认证，推动东盟地区的数字信息互联互通。2019 年 11 月，东盟颁布《东盟跨境数据流动机制的关键方法》，明确将重点建立东盟示范合同条款和东盟跨境数据流动认证两个机制。2021 年出台《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》，促进各成员国国内数据保护政策一致化，推进数据管理指标考核、建立跨境数据传输评估标准。

3.4.2. 《东盟个人数据保护框架》促各成员国国内数据保护政策一致化

《东盟个人数据保护框架》确立了一系列的原则，包括同意、通知和目的，个人数据的准确性、安全保障、访问和更正、跨境数据传输、存留以及问责等 7 个方面。在同意、通知和目的方面，该框架规定企业在未获同意情况下不得收集、使用和披露个人数据。在跨境数据传输方面，该框架规定在将个人数据转移到另一个国家或地区之前，企业应获得个人有关向境外传输的同意，或采取合理措施确保数据接收方将按照框架中确定的原则保护个人数据。

《东盟个人数据保护框架》虽然是东盟出台的首个专门针对个人数据保护的区域层面的规制，但该框架对各成员国并不具有国际和国内的法律约束力，仅作为指导性文件为各成员国提供数据治理合作的框架基础，旨在灵活适应各成员国在数据保护监管方面的不同的成熟度。各成员国适用该框架可采取符合本国国情的例外措施。

3.4.3. 《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》为企业提供数据管理和跨境数据流通的指引

《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》是东盟落实跨境数据流动机制的具体举措，目的是要促进数据相关的业务运营，减少谈判和合规成本，同时确保跨境数据传输过程中的个人数据保护。

《东盟数据管理框架》为东盟企业提供指南，说明建立数据管理系统的每个步骤，包括建议的数据治理架构、防护措施及适当的风险管理。整个过程可以分为6个重点环节，包括治理与监督、政策与程序、数据清单、风险影响评估、数据保护控制、以及监测与持续改进。

《东盟跨境数据流动示范合同条款》为企业之间跨境传输个人数据提供了合同条款模板，具体分为从控制者到处理者的数据传输、从控制者到控制者的数据传输两个合同模板。企业可以采纳或修改这些条文，就跨境传输个人数据拟订自己的法律协议。

不过《东盟数据管理框架》和《东盟跨境数据流动示范合同条款》属于自愿性条款，并不对东盟企业具有强制的约束力，这也是考虑到东盟各成员国间数据治理水平的差异。

2023年5月，东盟和欧盟联合发布了《东盟跨境数据流动示范合同条款（MCCs）和欧盟标准合同条款（SCCs）联合指引》（“联合指引”），以利两个经济体内成员国的企业参考适用。联合指引将分为《参考指引》和《实施指引》两个部分。此次颁布的是《参考指引》，该指引对MCCs和SCCs条款的共性和差异性进行比较和详解，帮助企业理解相关的合同义务和数据保护要求。之后将颁布的《实施指引》将提供企业遵守合同条款要求的最佳实践，以供企业参考如何更便利的履行MCCs和SCCs合同义务。

除了《东盟跨境数据流动示范合同条款》以外，东盟也承认其他的跨境数据流动机制，例如同等保护水平机制、个人信息主体的同意、行为规范（Codes of Conduct）、具有约束力的企业规则（BCR）、认证机制，如ISO体系或APEC跨境隐私规则（CBPR）和处理者隐私识别体系（PRP）等。

3.5.新加坡

3.5.1. 寻求加强监管与数据开放流动直接平衡的监管体系

作为全球贸易自由化程度最高的经济体之一，新加坡在严格保护个人隐私的前提下，对数据跨境流动秉持开放的态度。整体来看，新加坡的数字跨境流动政策比欧盟宽松，对国内数据的保护比美国更为严格。新加坡通过运用双边协议或

多边协议中关于数据跨境流动的条款、在局部区域范围内试点数据跨境流动、探索沙盒监管模式等阻力更小、可行性更高的方式，积极参与区域合作机制建设和寻求区域内数据自由流动。

3.5.2. 新加坡数据保护监管框架概览及数据跨境的要点解析

(1) 新加坡数据保护监管框架概览

2012年10月，新加坡颁布《个人数据保护法》(Personal Data Protection Act, “PDPA”)，该法确立了新加坡个人数据保护的基本制度。2021年12月1日，新加坡对PDPA进行了修订，修订版本于2021年12月31日生效，系当前适用版本。《个人数据保护条例》(Personal Data Protection Regulations, “PDPR”)作为PDPA规定的实施细则，进一步细化个人数据保护的合规要求。

新加坡在2013年设立个人数据保护委员会(Personal Data Protection Commission, “PDPC”)。PDPC隶属新加坡信息通信媒体发展局(Info-communications Media Development Authority, “IMDA”)，负责制定PDPA合规指引、监督PDPA履行。

在合规指引制定方面，PDPC当前已颁布《关于PDPA关键概念的咨询指南》(Advisory Guidelines on Key Concepts in the PDPA, “PDPA Guidelines”)、《关于特定合规话题的PDPA咨询指南》(Advisory Guidelines on the Personal Data Protection Act for Selected Topics)、《拒绝来电条款咨询指南》(Advisory Guidelines on the Do Not Call Provisions)等。另外，对于特定专业领域的的数据流动，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。

在监督PDPA履行方面，PDPA赋予PDPC较大的执法权，PDPC有权对于违反PDPA的行为开展执法调查、作出处罚决定，采取的处罚措施包括但不限于：a.要求处罚对象停止收集、使用或披露违反PDPA的相关个人数据；b.要求处罚对象销毁违反PDPA的相关个人数据；c.对处罚对象最高处以其在新加坡年度营业额的10%或100万新加坡元(以较高者为准)的罚款等。

在违反PDPA的责任后果方面，除前述提到行政责任外，PDPA还规定民事责任和刑事责任。PDPA第480条赋予个人向法院起诉的民事救济权利。在刑事责任方面，对于未经授权故意使用、披露个人数据构成刑事犯罪的，行为人可能面临最高2年监禁如PDPA以及最高5,000新加坡元的罚款。企业通过故意更改、伪造、隐瞒个人数据收集、使用或披露的相关信息以逃避个人访问或更正个人数据的请求，可能面临最高50,000新加坡元的罚款，而行为人可能面临最高12个

月监禁以及最高 5,000 新加坡元的罚款。

(2) 数据跨境流通：不限制数据入境，但对数据出境要求“同等保护”

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 不设限制；对于以新加坡作为出海各国数据集中存储地，在数据跨境合规义务方面，新加坡规定数据中转行为 (intransit)，即来自新加坡境外的数据通过新加坡进一步转移至第三方国家或地区过程中的个人数据，该个人数据在新加坡境内未被任何组织访问、使用或披露（传输方或传输方员工访问和使用除外），该类情形被视为已履行数据传输限制义务（PDPR 第 9-10 条）；对于由新加坡境内流向境外的数据，PDPA 第 26 条等条款规定除非根据 PDPA 相关要求确保接收方对传输的个人数据提供至少与 PDPA 同等的保护，不得将任何个人数据传输到新加坡以外的国家或地区。

需注意的是，上述义务仅适用于“数据传输方”。对于数据接收方，新加坡则通过要求数据传输方确保数据接收方提供“同等保护”，通过数据传输方向数据接收方传导 PDPA 规定的的数据保护义务。

(3) 持续传输及集团内部传输场景常见跨境传输方式

从实践及 PDPA Guidelines 建议看，对于持续或集团内部传输场景，企业通常采用与接收方签订数据处理协议、集团内签订具有约束力的公司规则 (Binding Corporate Rules, “BCRs”) 的方式进行跨境传输。如传输方通过与接收方签订数据处理协议履行数据跨境传输义务，除要求接收方提供与 PDPA 相当水平的保护外，还需注意：

a. 协议内容：1) 数据传输目的地国/地区；2) 如接收方为数据中介（数据处理者）时，该合同还应包括：安全措施、留存期限限制、数据泄露通知相关内容；以及 3) 如接收方为数据中介外的其他主体（数据控制者）时，该协议还应包括：收集、使用和披露的目的、数据准确性要求、安全措施、留存期限限制、数据保护政策、访问权、更正权以及数据泄露通知相关内容 (PDPR 第 11 (2) (b) 条及 PDPA Guidelines) 。

b. 协议生效条件：该等协议经双方缔约即生效，无需再经新加坡政府审批或备案。新加坡主管部门也尚未像中国这样预先制定数据出境标准合同，因此数据传输方和接收方可自行起草该等数据处理协议。但新加坡作为东盟成员，PDPC 明确承认《东盟跨境数据流动示范合同条款》(ASEAN MCCs) 可满足协议要求。因此出海企业在起草数据处理协议时可参考 ASEAN MCCs。

如传输方通过签订 BCRs 履行上述义务，除要求接收方提供与 PDPA 相当水平的保护外，须注意下述事项：

a. 适用范围限制：接收方与传输方须存在关联关系，包括传输方与接受方之

间存在控制关系或为同一主体所控制 (PDPR 第 11 (3) (a) 条及 PDPA Guidelines)。因此, BCRs 更适合用于集团内数据传输情况;

b. CRs 内容应包含: 1) 适用 BCRs 的接收方; 2) 适用 BCRs 的数据传输接收国; 以及 3) 数据保护权利及义务 (PDPR 第 11 (3) (b) 条)。

如传输方未能与接收方签订数据处理协议或 BCRs, PDPC 在 PDPA Guidelines 中建议, 企业可通过取得用户的同意或视为同意的方式履行数据跨境传输的义务。其中, “视为同意”情形包括: 1) 跨境传输为履行合同所必需: 如基于该事由跨境传输数据, 接收方可基于履行合同所必需向第三方再传输数据; 2) 用户主动提供个人数据或虽未主动提供但允许个人数据被收集使用。无论是取得同意或“视为同意”情形, 传输方均须履行以下义务:

a. 告知义务: 在请求个人同意前, 传输方应向数据主体提供书面概要说明, 告知其数据接收国对数据的保护措施, 以及该保护水平不低于 PDPA (PDPR 第 10 (3) (a) 条);

b. 手段正当性: 传输方不得以任何欺骗性或诱导性方式获得该同意 (PDPR 第 10 (3) (c) 条);

(4) 积极参与区域合作机制建设和寻求区域内数据自由流动

2018 年, 新加坡加入了亚太经济合作组织 (Asia-Pacific Economic Cooperation, APEC) 主导的亚太经合组织跨境隐私规则体系 (Cross-Border Privacy Rules System, 以下简称“CBPRs”) 和亚太经合组织数据处理者隐私识别体系 (Privacy Recognition for Processors System, 以下简称“PRPs”)。根据 CBPRs 的文件, 想要通过 CBPRs 认证的企业需要通过 CBPRs 对于企业所在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、隐私法的评估。

新加坡个人数据保护委员会 (Personal Data Protection Commission, 以下简称“PDPC”) 因此建立了一项与 CBPRs 对接的认证机制, 如果在新加坡获得这一认证的企业, 即可以在其他 CBPRs 成员内与其他认证企业自由传输个人数据。当接收方为数据中介方 (Data Intermediary)¹时, 接收方应取得 APEC Privacy Recognition for Processors System (APEC PRP) 或 APEC Cross Border Privacy Rules System (APEC CBPR) 认证; 当接收方为数据中介外的其他组织 (如数据控制者) 时, 该接收方应取得 APEC CBPR 认证 (PDPR 第 12 条)²。

¹ 根据 PDPA 及 PDPA Guidelines 的定义, “数据中介”为代表数据传输方并为其目的处理个人数据的主体。

² 对此, 数据出传输方可以登录 APEC 网站 (www.cbprs.org) 查询数据接收方是否已通过认证。

3.5.3. 新加坡与中国个人信息保护之比较

新加坡与中国在个人信息保护方面存在诸多的异同（详见附件4），例如不适用个人信息保护法律的规定，新加坡相较中国做出更为宽泛的规定；关于同意的规定，中国的法律要求同意必须是个人信息主体自愿、明确做出的，但新加坡规定了可以视为同意的情形。在个人信息跨境传输方面，新加坡相较于中国而言，有更为清晰的个人信息跨境规则，如前文所述的数据中转、持续跨境个人信息及跨国集团内部数据传输等情形，新加坡均做出了清晰的规定，为数据处理者提供了很好的指引。

3.6. 越南

3.6.1. 越南数据保护法律体系概况

(1) 数据保护相关法律法规

越南《个人数据保护法令》于2023年7月1日起施行，是越南首部个人数据保护综合性立法，对个人数据保护原则、数据主体权利以及数据控制者和数据处理者义务、数据跨境传输等方面作出了规定。该法令同越南《刑法》《网络安全法》《网络信息安全法》《消费者权益保护法》《信息技术法》《电子交易法》《关于网络安全法若干条款的详细规定法令》《关于信息系统安全分类法令》《关于互联网服务及在线信息的管理、提供与使用法令》《电子商务管理法令》《关于邮政服务、电信、无线电频率、信息技术和电子转账的若干行政处罚规定法令》等法律法规构成了越南现行的数据保护法律体系。

(2) 主要监管部门

越南与个人数据保护相关的主要监管机构包括公安部、信息和通信部、国防部和科技部等。其中公安部负责指导和实施个人数据保护工作，保护数据主体的权利免受侵害，提出出台数据保护标准、个人数据保护和适用建议，并开展依法检查、审查、处理投诉和控告等工作，是最主要的监管机构。

(3) 特殊主体的克减义务

《个人数据保护法令》明确规定，微型、小型、中型和初创企业在建立企业时，有权选择在注册的前两年内免于遵守相关要求。

3.6.2. 越南数据保护和数据跨境的要点简析

(1) 数据跨境传输机制

根据越南《个人数据保护法令》，“个人数据跨境传输”是指通过网络空间、

电子设备、电子手段或其他形式将越南公民的个人数据传输到越南境外地点或在越南境外的地点处理越南公民个人数据的任何活动。

要将越南公民的个人数据转移到境外，跨境数据传输者必须进行个人数据跨境传输影响评估并持续更新和维护跨境传输影响评估档案，以供越南公安部检查和评估。跨境数据传输者应在处理数据之日起 60 天内将个人数据跨境传输影响评估档案提交给越南公安部；数据传输完成后应将相关数据传输的信息及负责组织或个人的联系方式以书面形式通知越南公安部。

除特殊情况外，越南公安部将每年对个人数据跨境传输影响评估档案进行一次检查。如出现违反国家安全、提交的个人数据跨境传输影响评估档案不完整不符合要求或未根据新的变化及时更新、泄露或丢失越南公民个人数据等的情况，越南公安部可要求停止数据的跨境传输。

(2) 数据本地化及存储要求

为了加强数据安全，越南《网络安全法》中纳入了数据本地化储存条款，规定“在越南提供电信网络、互联网和网络增值服务的国内外企业，其收集、挖掘、分析和处理有关个人信息的数据、服务用户关系数据、服务用户生成的数据必须在政府规定的时间内储存在越南。本款规定的外国企业必须在越南设有分支机构或代表处。”

2022 年 10 月 1 日生效的《关于网络安全法若干条款的详细规定法令》对上述数据本地化条款进行了细化规定，特别强调对于在越南开展特定行业的外国企业，必须将上述三大类型的数据储存在本地，并在企业提供的服务被使用的情况下在越南设置分支机构或代表处。这些行业包括：电信服务；在网络空间存储和共享数据；为越南服务用户提供国内或国际域名；电子商务；在线支付；支付中介；通过网络空间传输连接服务；社交网络和社交媒体；网络视频游戏；以短信、语音通话、视频通话、电子邮件、在线聊天等形式在网络空间提供、管理或运营其他信息的服务。另外，该法令规定的数据储存期限最低为 24 个月，用于调查和处理违反网络安全法的系统日志至少保存 12 个月。

3.6.3. 越南与中国数据保护法律之对比

中国和越南的数据保护法律法规既有相似的内容，又有基于各自国情形成的差异。中越均高度重视国家网络安全和网络空间主权，两国的《网络安全法》对部分数据的本地化存储都作了要求。此外，中越均高度重视保护公民个人信息安全，但因基本国情和发展状况等的不同，中越两国的个人信息保护法律法规也有诸多差异之处。如在个人信息跨境传输方面，中国《个人信息保护法》规定了数据出境安全评估、个人信息保护认证和个人信息出境标准合同等三条个人信息跨

境合规路径。越南的个人信息跨境合规机制则较为独特，仅要求跨境数据传输者在规定时限内向监管部门提交个人数据跨境传输影响评估档案。该影响评估档案应随时备存且依据变化情况及时更新，以供监管部门进行事后监管。在告知同意机制方面，越南《个人数据保护法令》对于同意的认定作了更加细致的要求：数据主体的沉默或不回应不应被视为其同意；数据主体可以给予部分或有条件的同意；如果发生争议，个人数据控制者和/或个人数据控制者和处理者应负责证明数据主体的同意。另外，越南在将个人数据用于广告营销服务和违规后的通知义务等方面也提出了更为严格的规定（详见附件 5.1）。

3.7. 沙特阿拉伯

3.7.1. 沙特阿拉伯数据保护法律框架概述

目前，沙特阿拉伯规范数据治理的法律框架主要由《个人数据保护法》（The Saudi Arabia Personal Data Protection Law (PDPL)）和配套的《个人数据保护法实施条例》《沙特阿拉伯境外个人数据传输规定》以及适用于某些行业或部门的特定法规组成。

2021 年 9 月，沙特阿拉伯部长理事会批准了沙特阿拉伯《个人数据保护法》。这是沙特阿拉伯第一部全面的个人数据保护法案，旨在规范该国个人数据的收集、使用和传输等个人数据处理活动。PDPL 在 2023 年 3 月进行了修订，并于 2023 年 9 月 14 日正式生效。根据修订后的 PDPL 序言，自 PDPL 生效起有一年的过渡期，各实体应在过渡期内完成整改以使其个人数据处理活动符合 PDPL 的要求。

2023 年 9 月 7 日，沙特数据与人工智能管理局 (SDAIA) 发布了《沙特个人数据保护法实施条例》及《沙特阿拉伯境外个人数据传输规定》。两部法规扩展了 PDPL（于 2023 年 3 月修订）中概述的一般原则和义务，并对数据控制者提出了新的合规要求。

PDPL 适用于沙特境内以任何方式处理个人数据的实体。同时，PDPL 具有域外效力，如果外国组织处理与沙特居民有关的个人数据，则 PDPL 也将适用。

3.7.2. 沙特《个人数据保护法》要点简析

(1) 同意

PDPL 立法体例参照了欧盟的《通用数据保护条例》(GDPR) 的体例。它包括常见的关键原则和要求，如目的限制、最小必要、数据控制者责任、数据主体权利和违规处罚等。与许多国家的个人信息法案一样，对于个人数据收集和使用，PDPL 需要事先征得同意。

根据 PDPL 第 5 条，控制者必须在处理之前或处理时应“明确无误”获得个人同意。个人数据主体的同意可以以多种形式做出，包括书面、口头或电子方式等，但必须是在个人未被误导的前提下自愿做出。

数据主体可以随时撤回对个人数据处理活动的同意，控制者不得要求以拒绝提供服务或福利为条件获得数据主体同意（除非服务或福利与所获同意的处理活动特别相关）。

此外，如果存在多个个人数据处理活动，且分别具有不同的目的，则必须针对每个目的单独获得同意。

(2) 隐私政策

数据控制者必须制定隐私政策，PDPL 列明了隐私政策中必须包含的必要信息。数据控制者在收集个人数据前应当向个人数据主体提供隐私政策进行告知。

(3) 目的限制原则和最小必要原则

控制者必须明确收集和使用个人数据的目的，收集和使用的个人数据必须与收集和使用的目的具有相关性。另外，数据控制者必须在能实现预期目的的最小范围内收集个人数据。

(4) 影响评估

控制者必须对处理个人数据的影响进行评估，如果预期目的不再需要某类个人数据，则数据控制者必须停止收集该类数据。

(5) 违规通知

当发生数据泄露、未经授权访问个人数据等情况时，数据处理者必须通知监管机构；对个人数据主体造成损害的事件必须通知数据主体。

(6) 沙特《个人数据保护法》下的数据跨境传输

PDPL 要求数据控制者必须在沙特王国的地理边界内存储和处理个人数据。在某些情况下，如果不构成安全风险，数据可以在王国境外存储或处理。在向沙特境外提供个人数据之前，数据控制者必须进行影响评估，并获得监管机构的书面批准。监管机构将根据具体情况联系审批事宜。

根据 PDPL 修订后的第 29 条，数据控制者可以将个人数据转移到王国之外或向王国之外的实体披露个人数据的前提是：

- 1) 为保护公共利益、公共卫生、公共安全或保护特定个人的生命或健康安全以防止、测试或治疗病理性感染而进行的转移；
- 2) 根据王国作为当事方的国际条约进行的转移；
- 3) 为服务于王国的利益而进行的转移；
- 4) 为履行数据主体的义务；

5) 根据与 PDPL 配套的个人数据跨境传输法规的允许的目的进行的数据转移。

对于上述条件，PDPL 及其执行条例的草案也设置了具体的豁免情形：

如果主管部门本身与其他机构合作，并经评估个人数据在沙特王国境外可以得到足够的保障，且不包括敏感个人数据的传输时，主管部门可以根据具体情况，免除控制者遵守第 29 条规定的任何其他条件。

在不满足上述例外情况时，数据控制者必须向主管部门申请批准，方可将个人数据传输到沙特王国之外。批准申请必须在传输前至少 30 天提出，数据保护部门将有 30 天时间审查申请，并可酌情延长这一期限。如果这些例外都不适用，企业需创建本地的数据中心，并使用在沙特王国内处理数据的服务提供商，以满足沙特的数据本地化要求。

3.7.3. 沙特数据保护与中国的对比

沙特《个人数据保护法》对个人数据跨境传输规定了严格的限制，其批准要求比 GDPR 数据转移限制更进一步，更类似于中国的《个人信息保护法》（以下简称《个保法》）。

在个人数据权利方面，沙特 PDPL 与《个保法》一样，PDPL 赋予个人对自己的个人数据的权利，包括访问、更正和销毁/删除的权利。此外，PDPL 还授予个人知情权，要求处理者告知个人收集其个人数据的法律或实际理由和目的。

违反《个保法》和沙特王国的 PDPL 都会引发行政或刑事处罚。沙特对违规行为的处罚相对严厉，包括对实施非法数据转移的行为的主体处以最高一年的监禁和/或 100 万里亚尔（约 25 万美元）的罚款，对实施违法披露敏感个人数据的行为处以最高两年的监禁和/或 300 万里亚尔（约 80 万美元）的罚款，以及 SDAIA 能够施加最高 500 万里亚尔（约 130 万美元）的罚款。

可以看到，沙特阿拉伯正在逐步对其境内的个人数据使用进行国家监管，并为法律的实施提供了宽限期，使监管对象符合 PDPL 的规定。同时需要注意的是，沙特目前关于数据合规、隐私保护的法律法规尚未完善，争议性的网络行为可能被禁止，中国企业在沙特运营应严格遵守当地法律并评估风险。

3.8. 日本

3.8.1. 日本数据跨境流通战略举措

出于振兴本国经济、提高网络空间软实力、提升国际社会话语权等多重因素的考虑，日本通过修订国内立法、签订双多边国际协议、推广全球理念等战略举

措，不断推进跨境数据流通治理，倡导参与全球数据跨境流动合作。

(1) 通过修订和完善立法，构建与数据自由流动相匹配的数据安全机制

日本多次修订《个人信息保护法》，对个人信息跨境制度规则进行动态调整。2015年，日本修订《个人信息保护法》，增加了关于跨境数据流通的规定，包括设立个人信息保护委员会（PIPC）作为独立监管机构，制定向境外传输数据的规则和指南，增加数据出境须获得数据主体同意的一般性规定及例外情形。2020年、2021年，日本分别再次修订《个人信息保护法》，旨在促进大数据利用的同时解决数据的跨境流动中面临的风险。新《个人信息保护法》要求，在取得个人信息主体同意之前，应披露信息接收方所在国家及该国的个人信息保护体系、信息接收方采取的个人信息保护措施，同时采取必要措施确保接收方所在国家或地区持续实施了与日本《个人信息保护法》对个人信息保护要求相当的保护措施。总体而言，日本多次修订《个人信息保护法》，强化对个人信息出境行为的监管，对个人信息出境提出了更为严格的要求，体现了日本通过构建数据安全机制来保障数据自由流动的战略考量。

(2) 积极参与双边、多边贸易协定，寻求数据跨境流动规则的广泛合作

在双边贸易协定方面，日本积极与欧美英等发达经济体签订贸易协定，对接协调数据治理规则，构建“数据流动圈”。例如，《日本与欧盟经济伙伴关系协定（EPA）》《日美数字贸易协定》，《日英全面经济伙伴关系协定》等双边协定均提到了促进数据自由流动的合作倡议。以日本与欧盟在数据跨境方面的合作为例，2018年7月，日本与欧盟正式签署EPA，约定建立数据流通安全区，相互将对方的数据保护体系视为同等有效；2019年1月，日本与欧盟正式施行以互认为基础的个人信息跨境传输充分性框架，实现了日欧之间个人数据的双边自由传输；2022年10月，日本与欧盟同意就将数据跨境流动规则纳入EPA进行谈判。在多边贸易协定方面，日本参与或加入《亚太经合组织跨境隐私规则体系（CBPR）》《全面与进步跨太平洋伙伴关系协定（CPTPP）》、《区域全面经济伙伴关系协定（RCEP）》等双多边规则体系和贸易协议，积极寻求和推动跨境数据流通规则的多边合作。以CPTPP为例，2017年美国退出TPP后，日本接替美国开启了CPTPP的多边谈判，沿袭了美国在TPP中设置的一系列跨境数据流通规则。面对国际格局的深刻变革，日本积极参与双边、多边贸易协定，寻求数据跨境流动规则的广泛合作，不断提升其建立在高标准基础上的数据跨境国际协作水平。

(3) 构建和推行“基于信任的数据自由流通（DFFT）”机制，积极参与全球数据规则制定

2019年1月，日本时任首相安倍晋三首次提出 DFET 概念。同年5月，安倍在第25届国际交流会议演讲中指出，将在G20峰会上启动名为“大阪轨道”的国际数据流动倡议。随后，在G20大阪峰会期间，“大阪轨道”正式启动，并签署《大阪数字经济宣言》，标志着 DFET 从概念提出阶段进入实践阶段。从2021年至今，日本通过七国集团（G7）、二十国集团（G20）等国际平台，不断推进 DFET 的制度化、机制化落地。2021年4月，在英国举行的G7数字和技术部长级会议通过了《G7 DFET 合作路线图》。同年8月，在意大利举行的G20数字经济部长级会议发布《部长宣言》，重申了 DFET 的重要性和挑战。2022年5月，在德国举行的G7数字部长会议通过了《促进 DFET 行动计划》，同年8月，在印度尼西亚举行的G20数字经济部长会议发布《主席宣言》，也重申了 DFET 的重要性。今年3月，在日本举行的G7数字与技术部长会议发布了《G7数字和技术部长级宣言》，提出建立新机制和通过新的伙伴关系制度安排来运作 DFET。在全球数字贸易治理碎片化的情况下，日本通过构建和推进 DFET 机制，倡导基于信任的数据自由流动，积极参与全球数据规则制定，不断提升全球的数字治理影响力和话语权。

3.8.2. 日本数据跨境流通法律规制要点简析

日本数据跨境流通法律规制主要包括个人信息出境法律法规体系和多边贸易协定数据流通规则体系。其中，前者致力于规范和强化对个人信息出境行为的监管，后者致力于在高标准的基础上推进协定国之间的数据自由流通。

(1) 个人信息出境法律法规体系分析

日本于2003年制定了《日本个人信息保护法》，并先后颁布了与个人信息保护法有关的施行令、施行规则，进一步细化个人信息保护规则。此外，日本政府专门设置个人信息保护委员会作为个人信息保护的主管部门，该委员会相继制定、更新了关于个人信息保护法的指南，为企业个人信息合规提供具体指导。日本个人信息保护法律法规体系如表1所示。

表1 日本个人信息保护法律法规体系

项目	法规名称
基本法	《日本个人信息保护法》
实施法规及细则	《日本个人信息保护法施行令》《日本个人信息保护法施行规则》
实务指南	《日本个人信息保护法指南》（其中，“外国第三方提供

根据新修订的《日本个人信息保护法》及其配套制度规则，日本个人信息出境需满足以下条件：一是以事先取得个人信息主体的同意为原则，以不需要取得同意为例外。获得个人信息主体关于跨境传输个人信息的同意时，应当履行告知义务，事先向个人信息主体提供数据接收方所在国家或地区的个人信息保护的度、数据接收方采取的个人信息保护措施以及应供个人信息主体参考的其他信息，以便个人信息主体判断是否同意。此外，日本规定了无需取得个人信息主体同意的例外情形，包括向白名单国家跨境传输个人信息（如欧盟、日本），以及向已经建立了符合日本法规定的保护标准的个人信息保护机制的接收方跨境传输个人信息。二是判断接收方所在国家或地区是否拥有与日本具有同等水准的个人信息保护制度。日本个人数据跨境传输规则借鉴了欧盟 GDPR 的白名单机制，根据 GDPR 的相关规定，对于与欧盟具有同等水准的个人信息保护制度的国家，从欧盟向其跨境转移个人数据时无需另外取得个人信息主体的同意。目前，日本与欧盟、英国已建立白名单机制，认定对方的个人信息保护水平及安全措施具有同等水准，在不需要事先取得个人信息主体同意的情况下，允许个人信息在日本和欧盟、英国之间自由流动。三是判断接收方所在国家或地区是否建立了符合日本法律法规标准的制度且可持续采取同等保护措施。满足下列条件之一的可被认定为符合日本法律法规标准：1) 个人信息运营商和第三方，应当以适当和合理的方法，确保第三方在处理个人资料时，实施符合《日本个人信息保护法》第四章个人信息运营商义务的措施；2) 通过第三方获得国际体系认证，例如经合组织的隐私准则和 APEC 的跨境隐私规则（CBPR）系统的认证。

(2) 多边贸易协定数据流通规则分析

如前所述，日本参与或加入了 CBPR、CPTPP、RCEP 等双多边规则体系和贸易协议，致力于在高标准的基础上推进协定国之间的数据自由流通。一是 CBPR 体系关于数据跨境流动的规则要求。CBPR 规则体系包含自评估、合规审查、承认或接受跨境规则、争端解决和执行四部分内容。在 CBPR 体系下，APEC 建立了数据处理者隐私识别（PRP）体系，并且还建立了跨境隐私执法安排（CPEA）。接受方获得 CBPR 体系的认证，是日本允许个人数据跨境传输的合法路径之一。二是 CPTPP 关于数据跨境流动规则要求。CPTPP 规定缔约方不得对数据跨境流动征收关税，要求缔约方允许包括个人信息在内的跨境数据自由流动，同时给予缔约方在不构成对其他缔约方贸易歧视和变相限制的情况下基于“合法公共政策”的豁免；允许缔约方对计算机设施的使用根据安全保障和机密保护设有不同监管要求，同时不得将数据本地化存储作为市场准入条件的强制性要求。三是 RCEP

关于数据跨境流动的规则要求。RCEP 要求缔约方不能阻止金融服务提供者进行其金融服务活动必需的相关信息传输；不得将计算机设施必须置于境内的规定，作为进入该缔约方内部市场的前提条件，不得阻止正常经营活动中的信息跨境传输活动，同时为以上约束提供了实施“合法公共政策”和保护“基本安全利益”两种豁免情形。

3.8.3. 与我国数据跨境法律法规对比分析

在数据安全方面，我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”三个条件。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。

在个人信息保护方面，中国主要遵循的上位法为《个人信息保护法》，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》，确立对个人信息权利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；我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（JIPDE）

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。

3.9. 印度

3.9.1. 经历多次曲折，终接近出台数据保护专门立法

印度作为人口大国，超过 14 亿人口中拥有超过一半的互联网用户，且印度是全球科技巨头的重要发展市场，此前依赖的 2011 年的《信息技术（合理的安全实践和程序以及敏感个人数据或信息）规则》已无法解决互联网时代用户数据隐私保护和数据处理市场的平衡问题，因此制定一部专门的个人数据保护立法成为印度各界共同的呼声。

然而，由于印度特殊的国情和庞大的人口基数，印度个人数据保护立法工作十分曲折，从 2018 年 7 月印度高级别专门委员会提出首版法案《2018 年个人数据保护法案》开始，经历了 2019 年印度电子和信息技术部提交的《2019 年个人数据保护法案》版本，2021 年印度议会联合委员会经历 78 次会议提交审议报告包括 81 项修正案和 12 项建议，2022 年印度政府则以议会联合委员会对法案修改过多为由，撤回了 2019 年版本，而后 2022 年 11 月，印度电子和信息技术部发布了《2022 年数字个人数据保护法案草案》，最终于 2023 年 8 月 9 日由电子和信息技术部长发布了印度《2023 年数字个人数据保护法案》（DPDP）。该法案将在印度总统批准后正式成为法律，使印度接近出台第一部数据保护专门立法。关于 2018 年、2019 年、2021 年印度议会联合委员会的建议及 2023 年法案主要内容的对比可参见附件 10.1。

《2023 年数字个人数据保护法案》限缩了该法的适用范围，将此前采用的更为广泛的个人数据保护，替换为了更为明确、具体的“数字个人数据”（digital personal data），后者使用范围更为广泛，研究规制也较为充分。同时，在境外适用方面，《2023 法案》相较于《2022 法案》删除了“特征分析”（profiling）这一情形，只保留了向印度境内数据委托人提供商品或服务相关的境外数据处理应适用法案的规定。

3.9.2. 印度数据保护及数据跨境的要点解析

（1）确定了“特定合法使用”的数字个人数据处理的合法性基础

一般而言，亚太地区的数据保护立法皆采用了“视为同意”（deemed to have given her consent）作为个人数据处理的合法性基础。印度《2022 年法案》同样采取了“视为同意”的立法技术，但是其引入了过多的“视为同意”情形引发了较大的

争议。因此,《2023 法案》则创新性地采取了“特定合法使用”(certain legitimate uses)作为数字个人数据处理的合法性基础,但是保留了大部分《2022 年法案》中“视为同意”的情形,包括个人资源提供数据的特定目的、政府提供福利或服务、医疗紧急情况、就业等。此外,《2023 年法案》还特别赋予了国家处理个人数据的多项豁免,包括预防和调查范围行为、执行合法权利或索赔等,此处的国家包括中央政府、州政府、地方机构、政府设立的机关和公司等。由于国家的豁免允许国家将处理的数据用于其他目的,并允许国家将已有的个人数据用于任何目的,即消除了目的限制这一隐私保护的关键原则,因此关于国家豁免是否可能对隐私保护产生不利影响,目前仍在广泛讨论之中。

(2) 数据出境情形的规定更为宽松,从“必要因素评估”转为“通知限制”的方式

印度政府监管境外个人数据传输的目的是保护印度公民的隐私,因此若其他国家或地区缺乏健全的数据保护法,则存储在该国家或地区的数据可能更容易遭到泄露或未经授权与外国政府共享。因此,印度政府尝试对数据对外传输进行限制,四部法案(或建议)皆对数据跨境传输进行了规定,参见下表。

法案名称	具体内容
2018 年《个人数据保护法案草案》	<ul style="list-style-type: none"> ● 每个受托人在印度至少存储一份个人数据副本 ● 如果获得同意,可以转移到印度境外的某些允许的国家或根据管理局批准的合同 ● 某些关键数据只能在印度处理
2019 年《个人数据保护法案》	<ul style="list-style-type: none"> ● 敏感个人数据的副本应保留在印度 ● 仅在获得明确同意的情况下才能传输某些敏感个人数据,对其他个人数据没有限制 ● 关于关键个人数据,与 2018 年法案相同
2021 年议会联合委员会的建议	补充说明,未经中央政府事先批准,敏感个人数据不会与外国机构或政府共享
2023 年《数字个人数据保护法案》	<ul style="list-style-type: none"> ● 删除敏感和关键的个人数据分类 ● 中央政府可能会通过通知将个人数据限制在某些国家/地区

目前由于《2023 年法案》极有可能成为印度个人数据保护的正式立法,因此

未来在印度的数据跨境流通中特别需要关注《2023 年法案》的规定。其中明确，印度中央政府可以通过通知的方式限制向某些国家传输个人数据。这也意味着个人数据传输到所有其他国家在一般情况下没有任何明确的限制，除非中央政府以通知的方式予以限制，一般体现在将这些国家列入限制的清单之中。该措施相当于前三个法案（或建议）放宽了对数据跨境传输和流通的限制，此前的法案都要求对数据可能传输到的每个国家的标准进行逐案评估，而《2023 年法案》下则可以有针对性地选择进行评估，可能导致传输国家评估的不充分，引发了印度业界关于该机制能否为印度公民的数据和隐私提供足够的保护的担忧。

(3) 业务流程外包提供商处理不在印度境内个人数据等特殊情形可不落入适用范围

《2023 年法案》规定，业务流程外包提供商在处理不在印度境内的数据主体的个人数据时，如果是根据印度境内的任何人员与印度境外的任何人员签订的任何合同进行的，则不受该法的约束。然而，《2023 年法案》的某些规定仍然适用，如实施 "合理的安全保障措施以防止个人数据泄露 " 的义务。

(4) 对本地化存储的特殊规定

对于特定行业，印度通过行业法规，对该行业的数据做出了本地化存储的要求。例如银行业，印度储备银行 (RBI) 依据 2007 年《支付和结算系统法》(the Payment and Settlement Systems Act, 2007) 于 2018 年 4 月 6 日发布的关于支付系统数据存储的通知，RBI 指示所有系统提供商须确保与其运营的支付系统相关的全部数据存储在印度法律管辖范围内的系统中；再比如 2020 年《外国直接投资综合政策》(the Consolidated Foreign Direct Investment Policy) 中规定的条件之一是广播公司不得将用户数据库转移到印度法律管辖范围以外的任何实体或地方，除非得到相关法律的允许；再比如 2014 年《公司 (账目) 规则》[the Companies (Accounts) Rules] 第 3 (5) 条中的但书规定，以电子方式保存的账簿、公司其他账簿和文件的备份 (包括在印度境外的) 应存储在物理上位于印度法律管辖范围内的服务器中。

(5) 特别法庭

印度建立了一套专业审理信息技术相关案件的专业法庭，并在较低审级的阶段排除了普通法院体系的管辖权。为了行使印度 IT 法下的权利，个人必须向印度政府任命的、具有相关专业知识的裁决官 (Adjudicating Officer) 提出投诉并由裁决官审理：对裁决官的决定不服的，则应向电信争端解决和上诉法庭 (Telecom Disputes Settlement and Appellate Tribunal, TDSAT) 上诉；对于 TDSAT 的裁决结果，可再次上诉至相应州的高等法院。

(6) 印度数据保护机构

在现行立法下，印度的数据保护机构是电子和信息技术部（Ministry of Electronics and Information Technology, MeitY）。电子和信息技术部有权就电子和信息技术领域的问题提供指导。为应对数据安全事件，电子和信息技术部成立了印度计算机应急小组（CERT），作为接收和回应所有违规通知的节点机构。

根据《2023 年法案》，中央政府将成立印度数据保护委员会。该委员会的主要职能包括（i）监督合规情况并实施处罚，（ii）指导数据受托人在发生数据泄露时采取必要措施，（iii）听取受影响者的申诉。委员会成员的任期为两年，并可连任。中央政府将规定委员会成员人数和遴选程序等细节。对委员会决定的上诉将由 TDSAT 受理。

3.9.3. 与中国法律的对比

印度《2023 年法案》对标的是我国的《个保法》，皆是针对个人信息或个人数据做出的综合性立法。由于国情和法域的巨大差异性，两部法律存在较多的不同之处，具体可见附表。下文将展开重点需要关注的四点不同。

(1) 适用范围方面，印度法案适用于“数字个人数据”，相比中国“个人信息”的范围更为狭窄

印度在《2023 年法案》中将该法的适用范围确定为“数字个人数据”（digital personal data），而将以线下方式或是非数字化形式收集的个人信息排除在规制范围外。中国《个人信息保护法》的适用对象为“个人信息”，并不排除如纸质收集的非数字化形式收集的个人信息，保护范围更为广泛。

(2) 在主体名称方面，印度法案使用了“数据持有者”和“数据受托人”两个概念，中国《个保法》则使用了“个人信息处理者”和“受托人”的表述

印度《2023 年法案》在主体名称使用上与欧盟的“数据控制者”“数据处理者”结构较为类似，其使用“数据持有者”一词去概括“合法持有并且有一定保护义务的人”，英文翻译为 Data Fiduciary，而不同于欧盟“数据控制者”（Data Controller）；而对于接受委托处理数据的人，则使用“数据处理者”的概念予以概括。我国《个保法》则使用了“个人信息处理者”和“受托人”的表述，“个人信息处理者”是我国《个保法》规则的核心对象，《个保法》明确了个人信息处理者对受托人的个人信息处理活动的监督职责。这与印度《2023 年法案》确定了“数据持有者”首要和唯一的责任地位具有类似性。即，印度《2023 年法案》明确，数据处理者仅是代表数据持有者并按其指示或约定进行数据处理，数据持有者对数据处理者获取、使用、开发乃至删除数据的整个过程都在程序和实质上掌握着控制权和主动权。

(3) 处理个人数据的合法性基础方面，印度法案采取“合法目的+同意 or 特定合法使用”的模式，特定合法使用的范围较中国《个保法》合法理由的范围更为广泛

印度《2023 年法案》规定处理个人数据的合法性基础是在根据本法规定并出于合法目的下处理个人数据，在此情形上满足数据委托人已同意或属于特定合法使用两个条件其一。中国的《个保法》则并列规定了七点处理个人数据的合法理由，除了取得个人的同意之外，其余六种情形可以视为在同意以外处理个人数据的合法事由。在具体的合法事由中，中国的《个保法》额外包括“处理已合法公开的个人信息”，印度《2023 年法案》则包括“为国家机构提供补贴、福利、服务、认证、执照或者许可目的使用”“主权和国家安全”“为履行判决等理由”等中国《个保法》处理个人数据合法理由中没有涵盖的情形。同时，印度特定合法使用的情形之一是“自愿提供数据并且未向数据受托人表示不同意使用其个人数据的”，该条款可以理解成个人自愿同意相当于默示同意，只要个人未明确反对，即可处理。因此，印度处理个人数据的合法性事由是宽泛于我国《个保法》的。

(4) 在向境外传输个人信息方面，印度《2023 年法案》调整成了“不限制向境外传输个人数据”的模式，但赋予了中央政府确定能否数据出境的权力，我国法律则对数据出境进行了较为严格的限制

在此前版本的印度法案中，对于印度的数据出境予以了较为严格的限制，即必须进行中央政府的“必要因素评估”后通知数据受托人方可出境。同时，印度 2022 年版本的法案还提出了满足条件的强制数据本地化的要求，对于个人敏感数据，必须存储在印度境内，但其副本可以按照跨境转移的要求进行传输到印度境外。而印度《2023 年法案》极大地放宽了对于数据出境的限制，没有了数据本地化的强制性要求，更加鼓励数据流动，然而也为中央政府赋予了较大的权力，即数据能否出境将依赖于中央政府的通知或者其他法律的另行规定，这也为印度数据出境的宽严程度附加了更多的不确定性。我国法律则对数据出境提出了较为严格的限制，规定了数据出境应当经过安全评估、认证、签署标准合同等流程。

3.10. 俄罗斯

3.10.1. 俄罗斯联邦个人信息及数据法律环境分析

(1) 俄罗斯联邦数据与信息安全法律体系

根据俄罗斯国家杜马发布的《关于网络与数据信息保护立法与政策发展报告》（以下简称《网络与数据报告》），俄罗斯关于网络主权与数据保护的规范性文

件主要呈现“两大类、双层次”的分布特征，“两大类”是指传统部门法和新颁布的政策性文件；“双层次”是指对国内、国外两个层次的监管，该特征在传统部门法和政策性文件中也均有体现。《网络与数据报告》指出，俄罗斯已发布了近 50 部国家层面的法律法规与政策性文件，就网络主权问题给予国家立法支持与保护，呈现出立法数量多、颁发部门层级高、涉及范围广的特征；形成了以《俄罗斯联邦宪法》及已经缔结的国际条约为基础，以《俄罗斯联邦关于信息、信息技术和信息保护法》《俄罗斯联邦个人数据法》和《俄罗斯联邦主权互联网法案》为准则，以其他联邦法律与规范性文件为补充的数据与信息安全法律体系。

(2) 强本地化的规定

目前，全球对于数据流动监管尚未形成统一的规则和方案，新兴经济体与发达国家采取了截然相反的数据监管制度。各国在选择数据流动监管制度上受地缘政治、国家安全、隐私保护、产业发展水平等因素的影响，形成了数据自由流动与数据本地化两大基本监管制度。俄罗斯作为全球化进程中重要的经济体，基于数据主权的安全需求与立场，制定了数据本地化的监管措施，表现为跨境与境内限制性措施相结合，既要求跨国企业在俄开展业务或提供服务时须在俄境内建立数据中心，也对数据存储和服务器地址提出本地化要求。

3.10.2. 俄罗斯联邦数据跨境保护及审查要点分析

(1) 信息安全要点

俄罗斯联邦法律对信息安全的要求主要有以下几点：

- 1) 未经本人同意，禁止收集和传播有关其生活的信息。
- 2) 所有信息技术都是平等的——不能强迫公司使用任何特定的技术来创建信息系统。
- 3) 对特定类型的信息传播不做限制，例如有关环境状态的信息。
- 4) 对特定类型的信息禁止传播，如宣扬暴力的信息。
- 5) 存储信息的人有责任保护信息安全。
- 6) 被禁网站的登记册。俄罗斯联邦通信、信息技术和大众传媒监督局 (Роскомнадзор) 可以禁止在俄罗斯联邦境内传播非法信息的网站。
- 7) 被封禁网站的所有者可以通过删除非法信息并将其报告给俄罗斯联邦通信、信息技术和大众传媒监督局 (Роскомнадзор) 解禁网站。

(2) 个人数据保护要点

《个人数据保护法》是俄罗斯联邦关于“个人数据”保护的主要法律。该法律规范了个人数据的处理活动，对个人数据的保护主要有以下几点：

- 1) 在收集和处理个人数据之前，需征得个人的同意；

- 2) 为了保护个人数据, 仅可基于特定目的收集个人数据;
- 3) 有义务保障收集的个人的数据的安全;
- 4) 个人数据的主体要求删除其个人数据的, 需按要求删除其个人数据;
- 5) 在俄罗斯处理个人数据, 需在俄罗斯联邦境内的数据库中存储和处理这些数据。

(3) 公司数据保护要点

- 1) 公司可以决定某一数据是否是商业秘密并形成公司商业秘密的数据清单。
- 2) 特定类型的数据不能归类为商业秘密, 例如, 有关公司创始人或员工人数的数据。
- 3) 俄罗斯联邦基于充分的理由可以要求公司提供商业秘密, 例如, 对公司涉嫌违法的情况进行调查。
- 4) 公司有义务保护其商业秘密, 并保留有权访问此数据的人员的记录。
- 5) 公司员工泄露商业秘密, 可能会被解雇、罚款或起诉。

(4) 数据跨境监管要点

1) 数据共享或转让

如果个人数据不是从数据主体处直接取得, 接收人(处理人)应在开始处理个人数据前向个人数据主体履行告知义务, 但以下情况除外:

处理人已对数据主体进行告知;个人数据是由处理人履行法定义务或数据主体作为一方当事人的合同而取得;该等个人数据是由该数据主体自行公开或由处理人从公开来源取得的;为统计或其他研究目的、或处理是由新闻记者或大众传媒作为其专业活动的一部分或为科学、文学或其他创造性活动的目的而进行的, 但处理行为会损害数据主体的权利和自由的除外; 若向其告知会侵犯第三者的权利和合法权益。

2) 数据跨境转移: 提供同等保护

在将个人数据转移出俄罗斯之前, 处理人必须确保接收国对个人数据提供足够的保护。比如接收人所在国加入并批准了《个人数据自动化处理中的保护公约》。2013年, 俄罗斯列出了被官方认可为“确保充分保护”的国家名单。除了公约成员国外, 截至目前还有 26 个国家被认可为“确保充分保护”的国家名单。

如果处理人向无法提供同等保护的境外主体转移个人数据, 必须满足以下条件之一: 取得数据主体的书面同意; 俄罗斯联邦参加的国际条约中关于签证事宜另有规定的, 以及国际条约中涉及提供民事、家庭和刑事案件司法协助事宜另有规定的; 基于保护俄罗斯联邦宪法制度、保障国家安全目的所需; 履行数据主体作为一方当事人的合同要求; 在不能取得个人数据主体的书面形式同意时为保护个人数据主体或者他人的生命、健康、其他重大生存利益。

3.10.3. 中俄数据保护及数据跨境合规对比

在个人数据层面，俄罗斯注重保护个人数据权利。在保障个人数据权利的同时，注重保障个人数据不被窃取、破坏和滥用，以及确保整体数据系统的安全可靠运行。由于个人数据隐私的属性很难界定，俄罗斯所采取的措施与美国等国家有所不同，俄罗斯在加强对科技公司使用本国用户数据的监管与限制使用搜索引擎的同时，正研究制定向数字企业征收数字税的规范。

在跨境数据流通层面，俄罗斯实行严格的管控制度，对不同国家的数据主体实行差异化的法律监管。例如，对于美国等主动型数据流动国家，俄罗斯以《俄罗斯联邦主权互联网法案》为基础，在全球首次立法，实施“主动断网”，以识别网络主权威胁；在保护数据主权的同时，孤岛维权式地反对网络霸权成为保护性特征的重要表现形式。面对新兴经济体保守型数据流动国家，俄罗斯采取较为柔和的监管态度，在实施数据本地化存储的同时，兼顾数据流动的对等性。

俄罗斯联邦信息数据安全保护的监管特点最明显的就是数据存留本地化，数据存留本地化是专门限制数据跨境传输的措施，包括禁止信息出境、跨境传输信息必须征得数据主体的同意、要求在境内留存信息副本、对数据输出征税等形式。“棱镜事件”后，俄罗斯加快了数据流动法律的修改，旨在全面限制数据流动，加强数据流动监管，从法律层面确立了数据处理本地化的基本规则。

总体来看，俄罗斯的立法规定十分严格，通过对企业施加法定义务，实现了政府对数据处理、存储和跨境传输等环节的全面控制，牢牢掌握了本国数据跨境流动的主动权。

我国个保法正式确立了我国个人信息跨境流动的规则体系，规定个人信息以在境内存储为原则，并确定了需要在满足法律规定的条件下可以向境外提供个人信息的规则。我国的数据治理模式和方法仍在逐步探索和完善中，鉴于我国数字经济蓬勃发展、数据要素丰裕，在借鉴他国经验的同时，更要积极寻求符合国内数据要素保护方式和跨境数据流通的规则，逐步探索出一条符合中国特色的数据治理之路。

3.11. 欧盟

3.11.1. 棱镜事件推动的数据跨境流动立法密集时代

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-US Privacy Shield，以下简称“隐私盾协议”）。2016年，欧盟议会通过了2016/679号条例《通用数据保护条例》（GDPR），建立了基于充分性认定的白名单制度、约束性公司规则、标准合同条款和行为准则四项数据跨境流动体系。2020年7月16日，欧盟法院对施雷姆斯案数据保护专员诉 Facebook 爱尔兰和 Maximilian Schrems 案，C-311/18,“Schrems II”作出裁决，认定欧美数据跨境传输机制的隐私盾协议无效。2021年6月4日，欧盟委员会公布了《将个人数据从欧盟传输到第三国的新标准合同条款》并于2021年6月27日生效。同时，欧洲数据保护委员会于2021年6月18日更新了《关于为确保遵守欧盟个人数据保护水平而采用的对数据跨境传输工具补充措施的建议》。欧盟委员会和美国于2022年3月25日宣布，双方原则上已就新的跨大西洋数据隐私框架达成一致，该框架将促进跨大西洋数据流动，并解决欧盟法院在2020年7月 Schrems II 裁决中提出的问题。美国总统拜登于2022年10月7日签署一项行政命令，指示美国将采取措施，履行跨大西洋数据隐私框架下的美国承诺。2023年7月10日，欧盟委员会通过了欧盟-美国数据隐私框架（EU-US Data Privacy Framework, DPF）的充分性决定。DPF规定了将个人数据从欧盟的控制者或处理者转移到第三国和国际组织的规则，包括明确了欧盟的数据控制者及处理者可以在无需获得任何进一步授权的情况下将个人数据转移到经认证的美国主体。（详见附件8.1）

3.11.2. 欧盟数据保护及数据跨境的要点简析

欧盟 GDPR 将个人数据作为基本人权进行保护，其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%。GDPR 及其对违反 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8.3），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) 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 of Conduct, 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。

3.11.3. 中国对 GDPR 的借鉴与发展

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、韩国、瑞士和乌拉圭、英国、美国（参与 DPF 的商业组织）。另外，2022 年 10 月 10 日，EDPB 公布了对 Europrivacy 认证标准的批准意见，使得该认证标准成为欧盟通用标准，经评估后符合这一标准的认证对象，证书中可以获颁欧盟数据保护印章（European Data Protection Seal）。Europrivacy 认证成为目前所有欧盟成员国唯一正式认可的 GDPR 认证机制。

有看法认为，GDPR 在相当程度上扮演了贸易壁垒角色，提高了他国互联网企业进入欧洲市场的成本。同时，欧盟试图通过对外输出占据道德高地的欧盟标准，以获取与美国等数字经济领先国家在全球数字贸易谈判中的优势，扭转自身在全球数字竞争中的不利局势。在《通用数据保护条例》施行一周年之际，美国信息技术和创新基金会下属的数据创新中心发布的《GDPR 实施一年以来的影响》报告指出，《通用数据保护条例》并未产生欧盟立法者预期的积极效果，反而存在对欧盟经济的消极影响。其在增加企业数据合规成本、损害科技公司创新和竞争力的同时，也增加了消费者获取在线服务的成本和不信任感。

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前提下，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《个人信息保护法》《数据安全法》提供了借鉴意义，同时，中国的《个人信息保护法》《数据安全法》和《网络安全法》也设置了知情同意制度、原则上本地化、黑名单制度和反歧视措施，在全球数字经济发展的背景下更全面地规范了数据处理活动和数据跨境流动，以促进个人信息的自由安全的流动与合理有效的利用，推动数字经济的健康发展。

2023 年 2 月 3 日，中国《个人信息出境标准合同办法》由国家互联网信息办公室 2023 年第 2 次室务会议审议通过并公布，自 2023 年 6 月 1 日起施行。《个人信息出境标准合同办法》对欧盟《将个人数据从欧盟传输到第三国的新标准合同条款》在一定程度上进行了借鉴，并结合中国个人信息保护与监管的特色有所创新，是中国跨境数据流通制度的又一里程碑。中国的《个人信息出境标准合同办法》对个人信息设置了更高级别的保护，要求境内提供方在标准合同生效之日起 10 个工作日内向所在地省级网信部门备案，提交标准合同（包含个案具体的保护措施及出境情况说明）和个人信息保护影响评估报告。欧盟虽然在 Schrems II 案后对标准合同条款提出了更高要求，即境内提供方须证明个人数据出境后在实质上可以达到欧盟同等保护水平，而非形式签署标准合同即可，但并没有要求对标准合同进行备案。

然而，和欧盟历史悠久且在 GDPR 实施后通过大量实践案例而不断丰富发展

的制度相比，中国《个人信息出境标准合同办法》仍存在需要完善的方面。比如，GDPR 中标准合同条款对于特定服务商来说并不是唯一的选择，还有公司准则、行为准则的承诺、第三方认证机制的承诺。但是根据中国《个人信息出境评估办法》，标准合同并不具有可选择性和任意性。其次，欧盟《将个人数据从欧盟传输到第三国的新标准合同条款》区分了四种可能的传输场景，包括控制器到控制器、控制器到处理器、处理器到控制器和处理器到处理器，分别规定相关义务。中国《个人信息出境标准合同办法》则并没有区分接收者的角色，仅规定从中国实体转移到“海外接收者”，更加强调各方数据处理者的责任义务，同等严格的要求。

3.12. 美国

3.12.1. 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

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。

美国数据保护立法体系由联邦级立法、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。

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。美国在特定政府部门、电信及网络、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，限制州政府的机动车辆部门的《1994年驾驶员隐私保护法》（Driver’s Privacy Protection Act of 1994, DPPA）、电信及网络领域的《视频隐私保护法案》（Video Privacy Protection Act, VPPA）及《1984年有线通信政策法》（Cable Communications Policy Act of 1984）等。同时，2023年3月，拜登-哈里斯政府发布了国家网络安全战略（National Cybersecurity Strategy）。

从州立法来看，各州均在积极进行数据保护领域立法。其中，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，该法案于2020年1月1日正式生效。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》（General Data Protection Regulation, 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。

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（Federal Trade Commission, FTC）、消费者金融保护局（Consumer Financial Protection Bureau, CFPB）、美国货币监理署（Office of the Comptroller of the Currency, OCC）、证券交易委员会（Securities and Exchange Commission, SEC）、联邦通信委员会（Federal Communications Commission, FCC）、卫生与公众服务部（Department of Health and Human Services, HHS）和商务部等。

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《格雷姆一里奇一比利雷法》（GLBA）负责金融隐私的执法。

3.12.2. 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 9.1）。

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 9.2）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。

(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”的跨境数据流通政策体系。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《2023 年保护美国人的数据免受外国监视法》（Protecting Americans' Data From Foreign Surveillance Act of 2023, PADFFSA）。目前，CLOUD Act 和 EAR 均已生效，但 PADFFSA 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。

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的数据出口。EAR 严格限制部分关键技术与特定领域的的数据出口，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。

PADFFSA 则针对敏感个人数据的跨境传输制定了严格的规则。虽尚未生效，但仍须引起中国企业注意。根据 PADFFSA，由美国商务部长联合其他联邦机构负责对数据进行分类，确定哪些数据类型可能会被外国势力利用，以及传输的数据的数量级高于特定的阈值从而损害美国的利益。对于适用范围内的数据将受到 EAR 项下的相应管制。

3.12.3. 美国与中国数据保护法律之对比

(1) 中美跨境数据流通存在政策限制

在两国的立法中，对于数据跨境流动都有所限制。以《美国数据隐私和保护法案》（以下简称“《法案》”）为例，该《法案》明确要求，数据处理企业应向消费者说明，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。中国的《个人信息保护法》要求，个人信息处理者需要向境外提供个人信息的，需要进行个人信息保护影响评估，取得当事人的单独同意，具备法定条件，并确保境外接收方的处理活动符合规定。

(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 9.1）。虽然美国尚无联邦层面的数据保护立法，但是，针对美国议院拟议的《美国数据隐私保护法》进展以及可能对我国企业境外合规工作的影响，我们亦加以整理（详见附件 9.2）。

(3) 中美数据保护立法取向不同

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，例如，中国的个人信息保护立法趋于欧盟的 GDPR 与美国之间，在重视保护个人信息的前提寻求与数字经济发展的平衡，美国则致力于加强美国在数字经济中的领先优势。例如，就个人对数据处理的“同意”而言，中国采取须取得信息主体同意（opt-in）的模式，要求个人数据处理活动应具有合法基础，而美国 CCPA/CPRA 选择退出模式（opt-out）为主要机制，仅要求特定的数据处理活动取得个人同意，其他情况下则可以不经个人事先同意而处理数据，但个人可以选择退出。

3.13. 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，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。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，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。

第四章 跨境数据流通技术解决与合规方案

数字经济的发展源自与技术的进步，跨境数据流通既是法律问题，也是技术问题。如何使数据依法有序安全跨境流通，不仅需要法律在数据跨境合规中发挥积极作用，还需要新技术在新场景应用上找解决方案。

4.1. 跨境消费：某知名大型港资消费品企业数据跨境方案

某公司，作为一家知名大型港资消费品企业，在境内与境外均有业务布局，境内境外会员相关业务相对独立。鉴于两地社会联系紧密且顾客群体中相当一部分存在交叉，为了服务好这一部分群体以及将来可能发生的跨地区经营活动。公司需要建立数据跨境通道，以实现两地会员业务数据互通并激发会员消费潜力。

4.1.1. 案例背景

该公司在境内境外两地均维护着 CRM 系统，并建立了两套独立的会员体系。在这两地，会员的消费积分、会员等级、会员信息等均未进行同步。随着两地游客往来频繁，线下门店接待的境外客户数量逐渐增多。然而，许多顾客对于两地会员体系不互通的问题产生困惑。

(1) 业务挑战

由于同一品牌下不同地区的会员体系不同，会员在一个地区的消费积分、会员权益在另一地区无法查看和使用。而且，由于会员权益带来的附加值较高，无法享受会员应有的会员权益会引起客户不满情绪。

线下门店的店员不能便捷地查询顾客的会员账户信息，这限制了他们及时识别客户类型并提供定制化服务。若客户若在两地接受不同水平的服务，可能会产生心理落差，影响其消费意愿。后端业务分析人员由于缺少此部分交叉客户群体的消费数据，难以分析和预测消费热点和消费人群等关键业务指标，这限制了业务活力，并为供应链、生产、销售等环节增加了不确定性。

(2) 应用场景与需求

在用户层面上，改方案能满足客户在两地同步累计消费积分享受会员权益的需求；在业务层面上：前线员工应能够及时得知客户的会员账号信息，以便提供定制化服务。同时，后台业务分析人员将能获取更多关于交叉用户地消费数据，从而促使经营分析更加全面可靠，支撑业务发展。

4.1.2. 技术方案

考虑到问题紧迫性、技术建设的时间周期、业务改造的难度、合规要求等，本跨境解决方案流程示意图如 4.1-1 所示，具体分为如下两个步骤：

(1) 短期补救方案实施：通过简单而高效的方法解决两地会员体系信息不互通的问题。将在原境内会员平台中增加一个新的功能区域，会员可以进入此区域来开通和绑定境外会员帐户，并同步其基础信息至境外会员系统数据库。一旦会员完成绑定和同步操作，境外线下门店地店员就能通过会员手机号识别出会员在境内的消费情况，识别是否高价值客户，或者是新客户。并为客户提供定制化的服务。

(2) 长期完善方案规划：通过系统搭建和业务同步等措施，目标是使境内外的会员体系最终融合为一个高度统一的整体。在未来的计划中，更多的境内会员账户信息将被传输至境外的会员系统数据库，会员在境内消费与境外消费的积分按照一定比例统一积累至唯一会员账户。同时在线下门店终端，可以根据会员手机号或会员码，识别出完整的会员在境内与境外的消费情况，以及其他相关会员信息。用于判断会员的消费习惯、兴趣，同时便利业务部门分析产品销售情况，优化业务布局与决策。

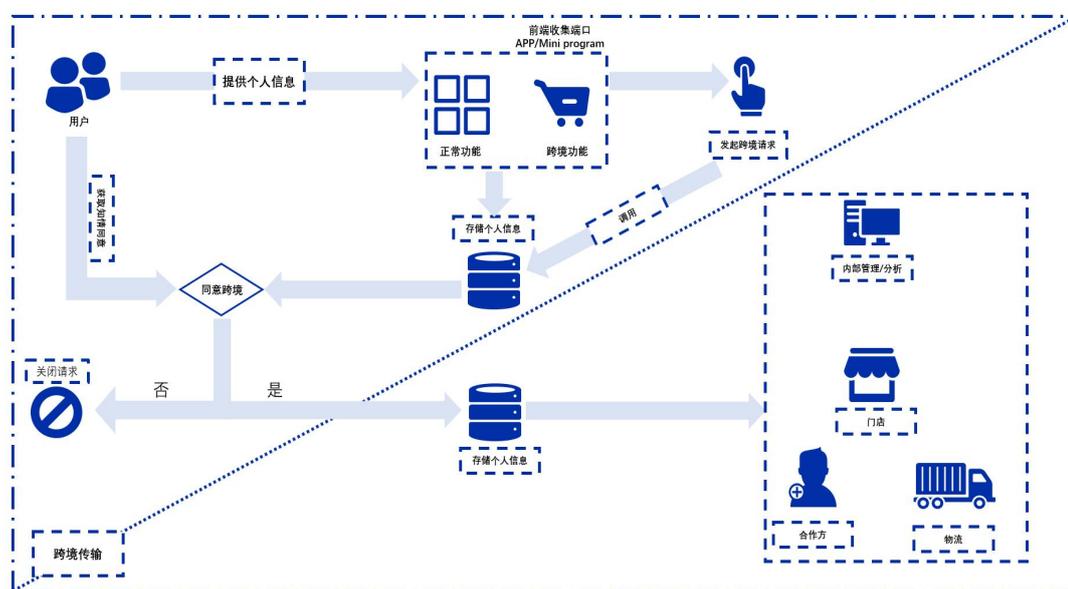


图 1 跨境流程示意图

4.1.3. 方案创新点和亮点

为缓和数据字段最小必要性所存在的矛盾，并在合规的红线内开展高效的数据跨境活动。在跨境方案设计之初，合规团队已与业务团队、数据分析团队展开深度沟通与合作，探索数据传输最小必要可能性。

第一期数据跨境方案当中仅传输七项个人信息字段，其中两项是由消费者在注册会员账号时自行提供、与其个人强相关的个人信息字段，其余五项是会员在该品牌消费后产生的消费记录相关字段。考虑到不同字段的敏感程度以及在业务当中的重要性。对于消费者个人强相关字段，在跨境传输前进行了脱敏处理。而基于消费后产生的数据字段也剔除了个人属性而使用会员编号替代。

4.1.4. 应用效果

采用此种方案成效是在最大程度上不影响业务正常开展的前提下，保证境外前线门店工作人员无法定位至具体的消费者，但可以了解会员的大致消费习惯以及会员等级，工作人员可以基于前述信息为消费者提供定制化的服务。后端数据分析人员开展分析工作同样基于无法定位至具体消费者的字段，同时也可以得出完整的数据分析结果，以支持业务决策。

4.2. 跨境金融：香港银行跨境电子签署

为了实现大陆居民、香港居民在线开立香港地区商业银行账户，深圳 CA 在项目中对持不同身份证件的两地居民提供统一标准的身份核验服务、数字证书服务和电子签署服务。且本项目在大陆和香港两地电子签名互认的司法框架下合法开展，深圳 CA 依据《中华人民共和国电子签名法》《粤港电子签名互认策略》等法律法规签发的数字证书签署的文件，在中国大陆和香港具有法律效力。

4.2.1. 案例背景

内地与香港居民在银行开户的跨境开户的需求确实受到一些监管限制，通常需要他们在银行所在地区进行面审和签署协议，以确保开户人的合规性。这种做法不仅效率低下，而且给客户带来了不便。为了解决这一痛点，在《粤港两地电子签名证书互认办法》的框架下，深圳 CA 结合自身产品能力，提出一套在内地和香港均合规的银行跨境电子签署方案。

4.2.2. 技术方案

(1) 方案思路

为满足银行的业务需求，深圳 CA 将项目中多个标准产品进行组合，并结合银行业务系统特点进行定制化改造。主要涉及如下产品和服务：大陆居民、香港居民身份核验、跨境数字证书、嵌入客户方 APP 的身份核验 SDK、嵌入客户方 web 端的电子签署页面、支持简体中文/繁体中文/英文的显示界面和短信服务等。

(2) 方案实现流程

深圳 CA 根据银行远程在线开户业务中对申请用户身份认证需求，以及跨境电子认证服务的业务规范，以 PKI/PMI (PKI: 公钥基础设施; PMI: 授权管理基础设施) 技术为基础，依托深圳 CA 作为第三方 CA 机构所提供的电子认证服务为核心，为银行建一个完整的电子认证服务平台。通过银行在线开户系统集成深圳 CA 的相关 SDK 控件和接口，在银行部署业务签署平台并与深圳 CA 的身份认证服务平台、证书签发系统、证书管理系统实现无缝对接，为远程开户业务提供完善的身份鉴证、在线签署、粤港互认等服务。本项目总体架构如图 2 所示：

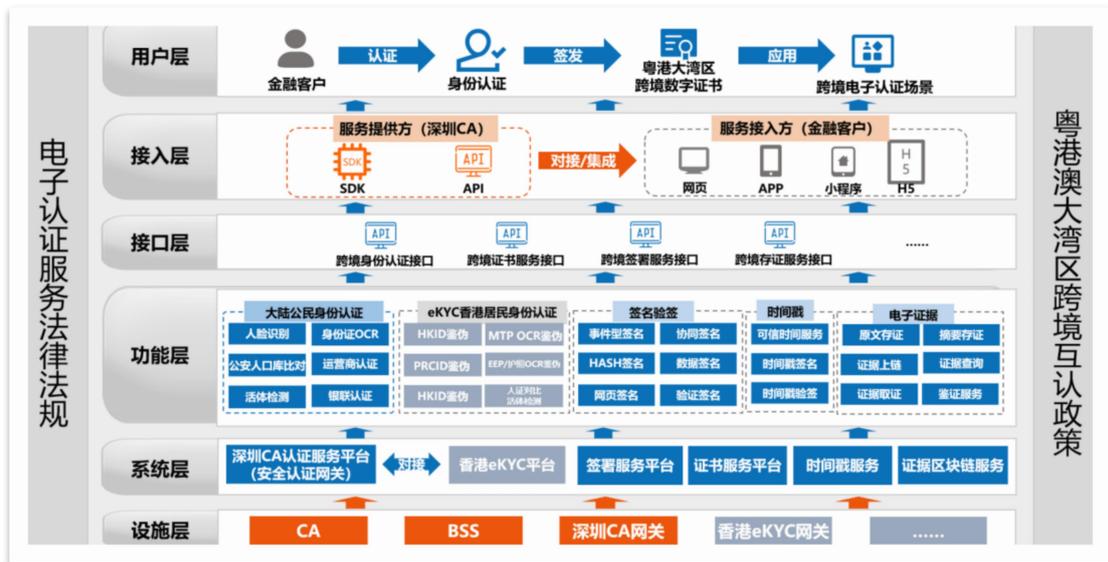


图 2 跨境电子签署服务平台总体架构图

4.2.3. 方案创新点和亮点

本项目将大陆居民身份核验 SDK 及香港居民身份核验 SDK 同时集成在银行的 APP 上，大陆香港两地客户通过同一银行 APP 办理所需的银行业务，客户通过选择不同身份证进入不同核验流程。采用 H5 签署的方式，将深圳 CA 的电子签署集成到银行的网页端，产品体轻量，实施效率高，客户体验感好。

4.2.4. 应用效果

通过此项目，推进了大陆客户在香港银行开设商业银行账户的进程，为日后吸引更多大陆客户打下了基础。香港市场采用了香港居民身份核验平安方案，摆脱了该行只有一家供应商的局面。在电子签署方面，首次采用基于数字证书+密

码学的更安全的电子签署方案。在整个香港银行业，大陆居民线上开户仍处于一个早期发展的时期，客户借此项目，走在整个行业前面，为促进两地金融科技合作提供了范本。

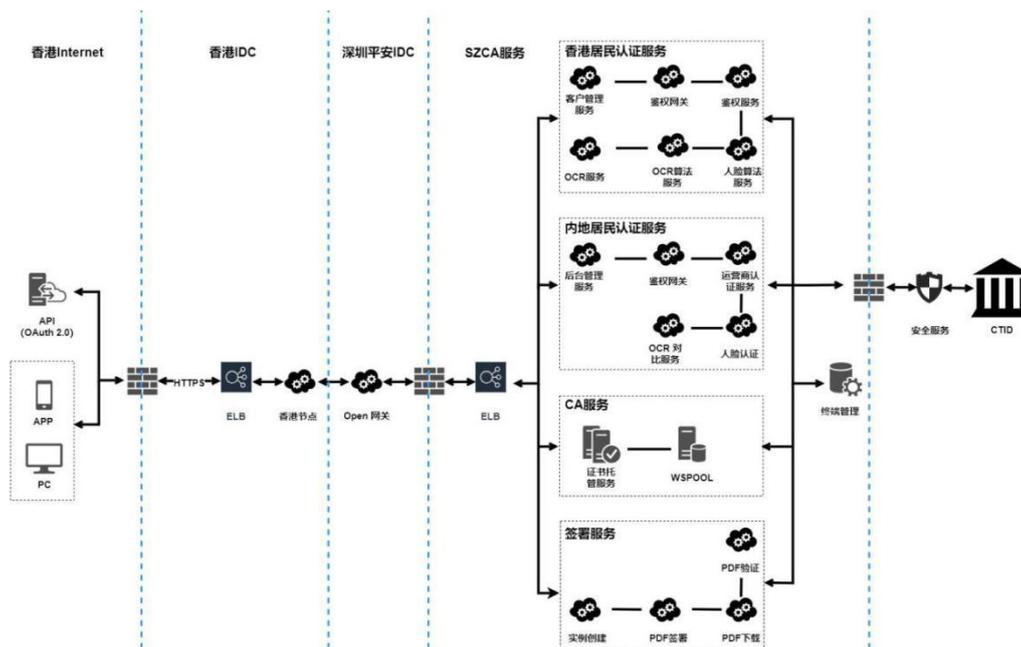


图 3 跨境电子签署服务平台网络传输路径图

4.3. 跨境芯片研发：M2&SKC 芯片数据跨境安全计算

为了降低 HBM IP 流片失败的成本，国内芯片设计公司 M2 需要更专业的境外芯片设计公司 SKC 帮助其进行设计调优和制造测试。因此，两家公司需要使用对方的数据进行加密隐私计算，以获取最直接的提高流片成功率的设计方案。由于项目涉及跨境数据流通，为了保证监管合规并尽量降低数据泄露风险，两家公司需要第三方中立 IT 服务商 UCloud 安全屋数据沙箱托管数据，并提供隐私计算、算力、存储、网络和安全服务。

4.3.1. 案例背景

(1) 业务挑战

首先，由于芯片设计制造行业算法成本及隐私加密难度高，全部为定制化流程，没有任何可参考经验。隐私计算部分涉及核心数据，且不能绕过 EDA 算法层。

其次，由于合规及数据风险评估需求，漫长的 POC 测试过程导致前期推进

几度停滞，商务及技术侧的对接失位导致项目受限于商务谈判能力效率滞后；合同谈判过程亦受技术侧进度和国内外数据安全政策变化影响。

最后，跨境合规要求及隐私计算性需要能跟上用户交付时效性要求。

(2) 技术挑战

首先，由于存在数据泄露风险，芯片数据部分明文规定，需要用合同条款约束使用方行为。

其次，由于数据的类型是非常规的，数据包量级基本 3T 以上，且由专业程序应用打开，相当于流通的加密数据包，EDA 算法嵌入对于安全检测有非常规要求，标准 MPC 产品难以实现。

最后，隐私安全与可用性难平衡。作为巨量算力项目且有时效性要求，对于隐私计算部分的加密程度需要做出部分牺牲，且需要客户允许 MPC 介入核心算法层进行改造，对业务效率进行妥协，通过其他技术手段和流程限制来同步规避数据安全风险。

4.3.2. 技术方案

UCloud 安全屋以成熟产品为基础核心输出第三方数据流通服务能力及 MPC 服务价值，在关键数据层完成价值保护及防窃取工作。UCloud 安全屋采用私有化集群部署，物理上是分布式部署，逻辑上是去中心化协作。

此项目中，国内芯片设计公司 M2 作为甲方，国外芯片设计公司 SK2 作为乙方，第三方中立 IT 服务商优得 UCloud 作为丙方，提供隐私计算、算力、存储、网络和安全服务。第三方服务商与另外两方之间不存在业务竞争性，不存在关联控股竞争性，且在原始能力上能够帮助甲乙双方完成软硬件及实时过程的整体安全合规和组织管理。芯片数据跨境安全计算应用场景的整体框架图如图 4 所示。

此项目中，国内芯片设计公司 M2 作为甲方，国外芯片设计公司 SK2 作为乙方，第三方中立 IT 服务商优得 UCloud 作为丙方，提供隐私计算、算力、存储、网络和安全服务。第三方服务商与另外两方之间不存在业务竞争性，不存在关联控股竞争性，且在原始能力上能够帮助甲乙双方完成软硬件及实时过程的整体安全合规和组织管理。芯片数据跨境安全计算应用场景的整体框架图如 5 所示。

安全屋应用场景：隐私保护计算_私有化+分布式部署_去中心化协作

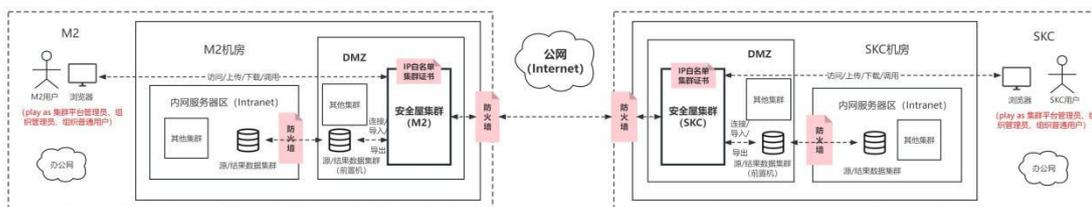


图 4 整体架构图

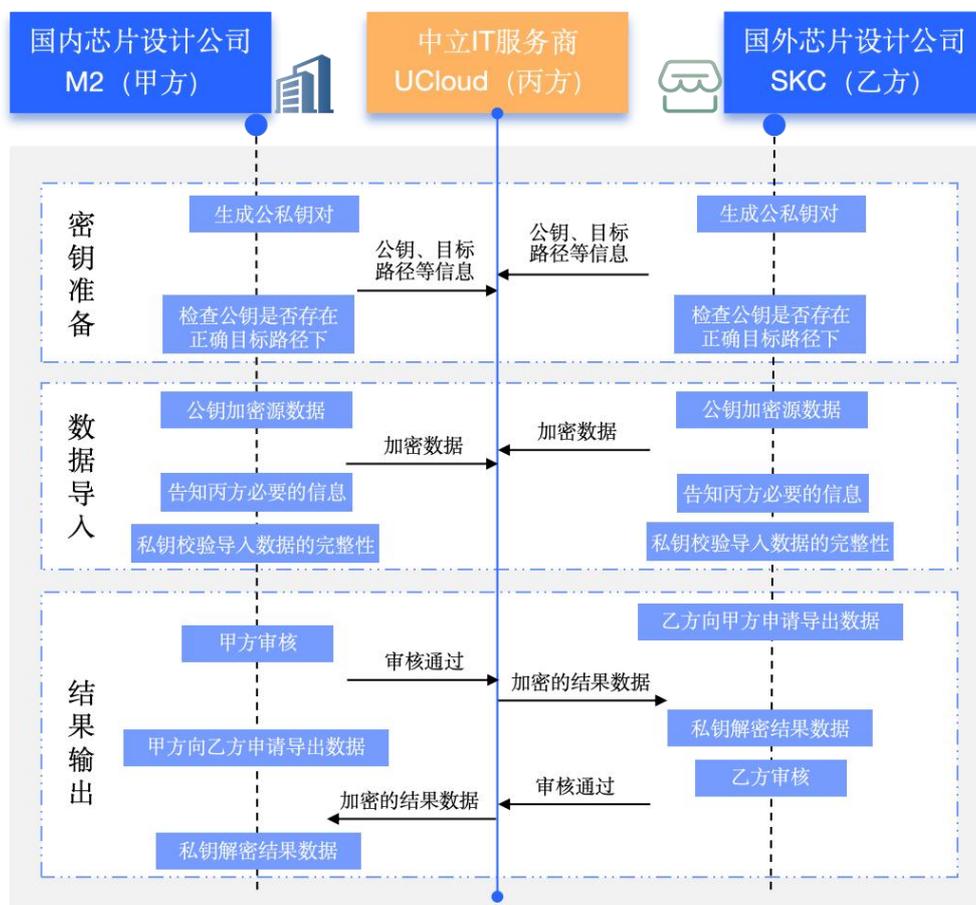


图 5 UCloud 安全屋业务流程图

4.3.3. 方案创新亮点

在技术升级上，超长前置调试 MPC 嵌入芯片 EDA 编译，直接对原算法进行拆分编译，使数据加密本身对业务影响降到最低，使用方无感应用。

在技术创新上，对原有算法进行最小程度拆分，一层 SMPC 隐私计算，叠加一层数据沙箱，将隐私加密计算与数据安全流通拆分进行，并尽量降低性能损耗，保证业务流畅及项目成果交付时效性。

4.3.4. 应用成效

甲方收益及目前成果有，按业务约定，甲方仅获得最终 PDK 文件，用于其项目的最终流片量产对接，过程文件及数据归乙方所有，不可被取出。项目截止时，甲方可获取应用于实际生产的 PDK 文件。甲方商业侧对于目前的成果进展表示满意，从时间效率进度及流片成本层面上极大的降低了无效损耗，提高芯片设计验证能力。

乙方收益有，SKC 侧的专家人力价值输出及知识产权被保护，在这个合作模式下可稳定长期收取费用，并且降低了差旅成本及人员投入数量。与此同时，在双方合作的中间过程中完整保留数据及工程经验，帮助其持续保持行业领先的工程经验值。

4.4. 跨境数据：中国首单场内跨境数据交易

2022 年 11 月 15 日，深圳数据交易所（以下简称：深数所），与数库（上海）科技有限公司（以下简称：数库科技）实现了国内首单场内跨境数据交易，为探索跨境数据流通交易迈出了坚实的第一步，也为推进跨境数据交易制度和规则衔接提供了实践经验。这不仅意味着数库科技的整体实力再次受到权威认可，更标志着数据跨境时代的正式起航。同时，该笔交易也经过了第三方律所合规评估及深数所的交易风险评估及见证。

4.4.1. 案例背景

2022 年 2 月 12 日，《深圳市探索开展数据交易工作方案》正式通过深圳市委全面深化改革委员会第二十四次会议。其中提及，到 2022 年底初步形成新型数据交易体系框架，到“十四五”期末初步形成全球数据交易市场枢纽，打造 5 家左右知名跨境数据商，培育 100 家以上具有技术优势及特色应用的中小型数据商。

深数所自成立以来，广泛对接央地各级部门以及跨行业多种类市场主体，开展调研与业务对接，积极探索跨境数据交易，已经与香港生产力促进局签订“跨境数据流通试点合作框架协议”，正在推进首批跨境数据交易，场景覆盖金融、电商、互联网、医疗行业。

4.4.2. 整体方案

(1) 数据产品介绍

此次数库科技与知名境外头部对冲基金交易的标的为“数库 SmarTag 新闻分析数据”。该数据产品属于原创数据集，是深数所重点推进首批跨境数据交易之

一，通过公司在自然语言处理领域的旗舰级新闻标签解析引擎 SmarTag 生产。SmarTag 主要通过自主研发的 NLP 算法将市场中的高频非结构化新闻资讯转化为机器可读的结构化元数据。

这一产品主要通过自然语言处理算法对国内主流网站的财经及行业新闻资讯进行提取加工，形成标签化数据，在剔除个人信息、新闻标题及新闻内容后，向境外客户提供。

在技术层面，SmarTag 以多种深度学习和机器学习技术为基础，将对新闻的分析转化为多种自然语言处理任务的组合。由于各任务存在一定的重合，分析过程采用有向无环图的形式调度各项算法。产品架构图如图 6 所示。



图 6 数库 SmarTag 新闻分析数据产品架构图

(2) 数据出境目的与方式

境及境外数据接收方的数据处理在金融行业投融资领域的应用，包括为资产管理机构的量化分析、优化二级市场的策略决策提供支持等。

交易数据以数据表及字段说明的形式，上传至 SFTP 服务器，供境外接收方访问、下载及存储。相关协议中约定了数据接收方的处理方式，并且均对数据接收方的转售或对外提供限制、数据安全保护及责任承担进行了约定。

(3) 数据出境涉流程

数库科技数据交付过程包含数据文件生产、数据文件授权、数据文件推送、

数据文件入库的环节。如图 7 所示：

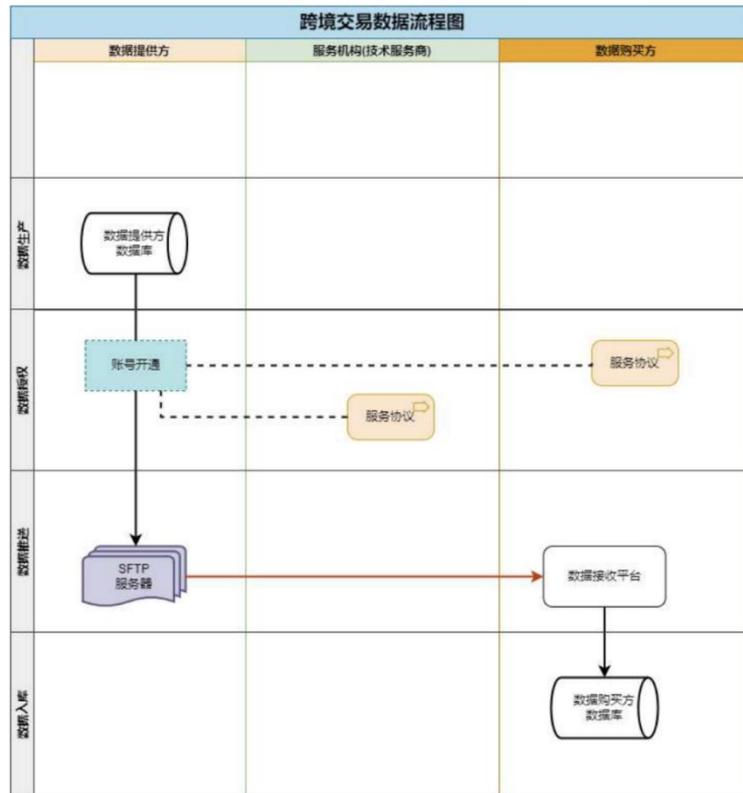


图 7 跨境数据交易流程图

在数据存储安全方面，数库科技数据库系统使用主备模式，从库用来进行数据的备份。另外，数库科技对数据库数据进行日度备份并使用多台机器存储。对于本地的数据 NAS 服务器，硬件磁盘通过定义 raid 的不同级别来增加磁盘可靠性。此外，还通过为对象存储提供 SSE-KMS 默认加密、为数据库使用 AES-256 进行数据加密来保障数据存储的安全性。

在数据传输安全方面，针对数据传输过程可能面临的被中断、截获、篡改、伪造等风险，数库科技采取以下措施控制风险：

- 1) 采用负载均衡技术，通过服务冗余的方式，将相同的应用部署到多台机器上，解决访问统一入口问题，实现流量分发。这样，即使面对大量用户访问、高并发请求或非法请求/攻击时，也能保障数据传输服务的可用性。
- 2) 采取防火墙技术有效隔绝外网非法入侵内网的风险，同时使 IP 白名单策略进行身份验证，有效拒绝非授权的访问请求。
- 3) 通过 SSL、HTTPS 和 SSH 等网络加密协议，保障数据传输通道的保密性，避免数据被截获。
- 4) 通过基于 SHA256 的 Hash 校验算法，保障数据传输的完整性。
- 5) 使用基于 RSA2048 的非对称加密算法，及私钥加签、公钥验签的数字签名

方式，保障数据传输不被篡改、伪造。

(4) 数据出境法律法规要求

数库科技委托广东北源律师事务所开展合规评估，广东北源律师事务所针对交易主体、交易标的、交易流程三大维度进行客观独立地评估并出具法律意见书。同时，深数所对该交易的交易主体基本情况、交易数据情况、交易合同及风险评估情况等多项事宜进行审查并留存了相关记录。基于相关材料，深数所尚未识别到交易数据涉及个人信息及重要数据的情况，考虑到数据本身为公开数据，且经过标签化及剔除个人信息、新闻标题及新闻内容的处理，深数所认为数库科技主动防范了数据跨境交易的安全风险，该交易基本符合法律法规的要求。

4.4.3. 数据产品创新点和亮点

SmarTag 的最大特点在于其标准化的数据体系。算法所提取的公司、行业、产品、地区等标签都与数库科技知识图谱体系中的公司图谱、产业图谱等图谱中的节点对应，并且带有唯一性的标识 ID。因此，在提取标签的同时，实体链接的问题得以解决，标签得以对应到知识图谱上的具体实体，并且在下游应用中可通过知识图谱进行进一步的图计算。

SmarTag 以自然语言处理技术为基础，通过对金融资讯的解析、提取和标准化，形成了一套完整的资讯分析算法和系统。这能够实现对金融资讯的清洗和去重，得以从资讯中提取出公司、行业、产品、概念、事件、地区等多种标准化标签，分析资讯及资讯中具体主体的正负面舆情，并将标签等结果注入数库的数据体系，形成规范化、标准化的知识图谱，从而实现了海量资讯的实时分析，为各种金融应用和计算提供了数据支撑。

4.4.4. 应用成效

(1) 量化投资应用

数库科技的 SmarTag 可对新闻文本的结构化解析，从而实现对全篇新闻及新闻中的主体情绪解析。并且，通过各维度的标签及情绪分析数据的结合，可对各公司主体的情绪进行定量研究。同时，也可以构建 A 股全市场的新闻情绪，例如，A 股个股情绪因子、A 股行业情绪指数和 A 股市场情绪指数等，为相关量化人士提供更多 Alpha 挖掘机会。

(2) 荣誉奖项

数库科技的“智能文档资讯分析技术服务”荣获上海市高新技术成果转化项目。在首届应用算法实践典范 BPAA 中，数科科技“智能文档与资讯分析技术”荣获“金融算法赛道全球 10 强”。

4.5. 数字贸易：基于数字贸易资产的融资解决方案

融资是中小企业的发展过程中长期面临的难题，联易融（Linklogis）基于自身在供应链科技方面的领先优势，与国际清算银行创新中心启动数字贸易资产（Digital Trade Asset, DTA）项目，共同探索数字技术在金融领域的应用，推动科技赋能和产品创新，为拓宽中小微型企业融资渠道提供有力支持。该项目提供了一个原型平台，核心买家及供应链上游供应商可利用数字贸易资产实现附条件支付。中小型企业可在未满足既定条件之前利用 DTA 向机构投资者寻求融资。

4.5.1. 案例背景

(1) 行业现状

在迅速发展的全球供应链格局中，中小微企业在经济增长和技术创新中发挥着至关重要的作用，为全球经济和社会发展提供了不可或缺的力量。世界银行的研究表明，中小企业占有所有企业的 90% 以上，贡献了全球 50% 以上的就业机会，也在全球供应链中发挥着重要作用。尽管中小企业发挥着如此重要的作用，但因为缺乏抵押品或在档的信用和运营记录而较难得到传统投资方的资金支持，面临着长期的融资难题。

(2) 业务挑战

在传统的供应链中，核心买家经常以赊账（Open Account, OA）的方式从一级供应商那里采购货物或服务，因为核心买家往往具有更强的议价能力。负责交付产品的一级供应商又根据 OA 或信用证（Letter of Credit, LC）条款将某些制造流程外包给二级供应商，或从二级供应商处购买零件或材料。这是供应链的基本运作模式。但由于缺乏抵押品和/或已建立的信用和运营记录，且保理和发票等贸易融资产品不能实时更新贸易信息，投资者给中小企业的贸易融资意愿大大降低。同时企业运营规模较小，这导致中小企业贸易资金周转困难，营运风险陡增。

4.5.2. 技术方案

(1) 解决方案思路

基于传统的供应链结构，联易融构建了一个原型平台，核心买家及其供应链上的供应商可以在该平台上使用 DTA 进行交易可编程支付。在不同的贸易阶段，DTA 有不同的状态体现，分别为：未实现的（unrealised）、“确认的（confirmed）”、和“已实现的（realised）”。核心买家根据贸易合同将基于行为、数据和时间的 DTA 状态转移的条件编码到智能合约上，当供应链上贸易流程的某一环节被确认，DTA 就根据上述预设条件自动完成相应的状态转移。当 DTA 的附加条件均

已满足，下游供应商就可以向发行方兑换 DTA，获得等值的法定货币。通过区块链和智能合约等去中心化技术，充分保障供应链上各参与方之间贸易的正确执行与资产的安全转让。

(2) 平台功能架构

假设必要的监管已经到位，DTA 可由平台上核心买家要求的商业银行发行。图 8 说明了 DTA 在供应链上贸易结算中的应用：

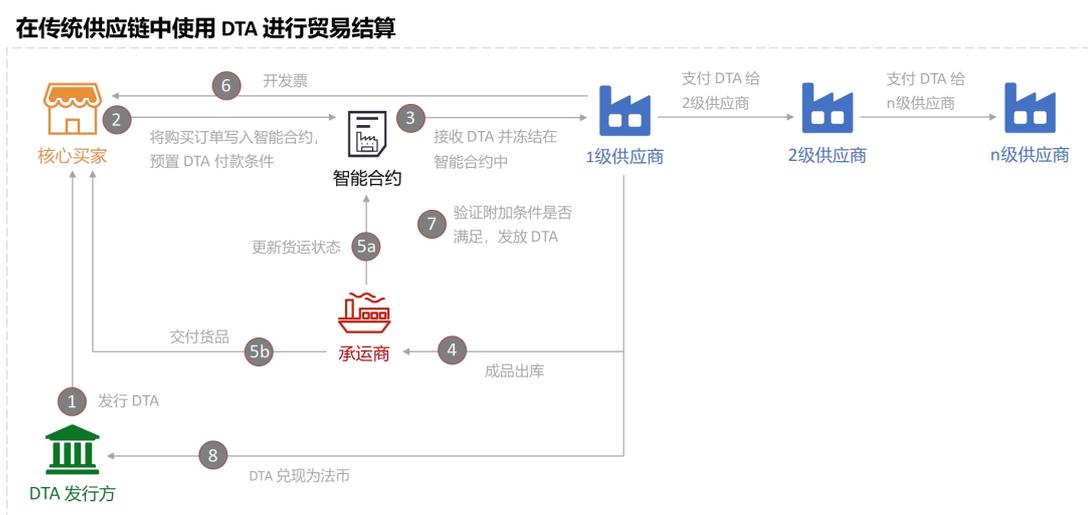


图 8 传统供应链中 DTA 的应用流程图

核心买家与一级供应商签订采购订单，然后从 DTA 发行方处获得 DTA，并使用（与合同金额等额的）DTA 向一级供应商进行有条件付款。DTA 可以由核心买家根据时间、行为和数为条件进行编程预设，预设条件举例如下：

- 1) 基于时间的条件：仅在特定日期向 DTA 接收者付款。
- 2) 基于行动的条件：只有当核心买家表示接受付款时，才会向 DTA 的接收者付款。
- 3) 基于数据的条件：仅当某个贸易平台或承运商已发出电子提单时，才会向 DTA 的接收者付款，或者当供应商达到一定的 ESG 级别时，才会向供应商支付奖金。

这些条件被编码在区块链上的智能合约上，一旦满足预设条件，付款就会自动执行。图 9 展示说明了在多层级的供应链上，DTA 如何应用在发行、转让、融资和兑现等场景中。

在多级供应链中使用 DTA

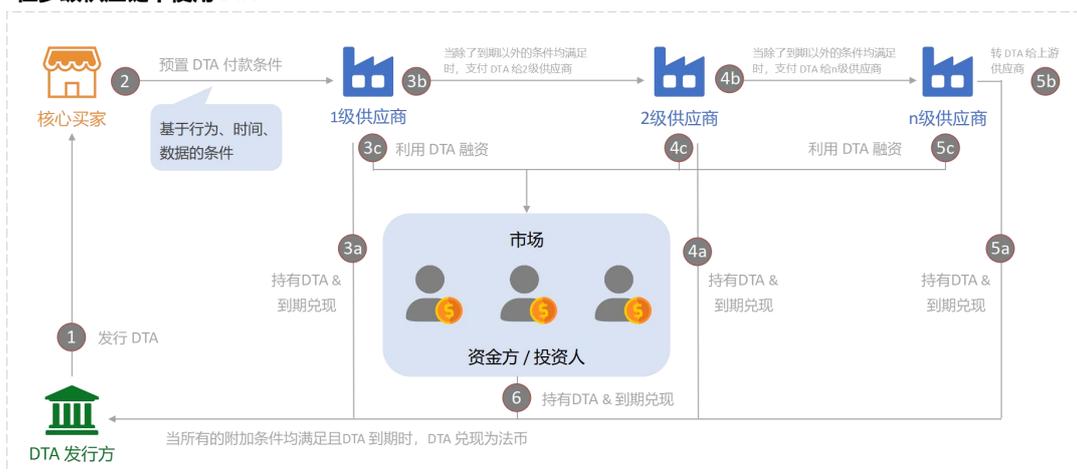


图 9 多级供应链中 DTA 在发行、转让、融资和兑现场景中的应用

供应链上持有 DTA 的供应商可以通过兑现、转让或融资等方式来获取营运支持:

- 1) 兑现: 在 DTA 发行处兑现满足条件的 DTA (见 3a/4a/5a) ;
- 2) 转让: 将全部或部分避免双重征税条约转让给上游供应商, 以支付其欠上游供应商的全部或部分债务或应付款项 (见 3b/4b/5b) ;
- 3) 融资: 在条件满足之前, 通过 DTA 平台与投资方 (机构投资方) 利用全部或部分 DTA 融资。以 DTA 为预付款项去做投资。在这种情况下, 投资方承担的信用风险是来自供应商的履约风险和 DTA 发行方的信用风险的 (投资方不承担核心买家的信用风险, 因为索赔是针对 DTA 发行方的) (见 3c/4c/5c) 。

4.5.3. 方案创新点和亮点

- 1) **流程创新:** 更流畅地衔接供应链贸易与中小企业融资的场景。
- 2) **模式创新:** 运用 DTA 实现贸易信息的实时更新, 解决了传统融资场景中投资方无法及时信息同步的问题, 使得中小企业的信用评估变得更快、更容易, 也提升了投资者的投资意愿。
- 3) **融资方式创新:** 核心买家可利用 DTA 实现附条件支付, 中小型企业可在未满足既定条件之前利用数字资产向机构投资者寻求融资。这不仅为中小型企业开拓了空前丰富的融资选择, 也为投资者开辟了新的投资机会。
- 4) **科技创新:** 本项目方案展示了去中心化金融技术在贸易金融行业领域的创新运用, 它提供了一个突破性原型, 用数字资产用与智能合约技术来促进中小企业在供应链上的融资。

4.5.4. 应用成效

中小企业在大多数经济体中发挥着重要作用，数字贸易资产项目原型可以为以前无法获得传统融资的中小企业提供新的融资途径，从而有助于刺激经济增长。利用区块链技术，原型平台还为参与贸易交易的各方以及投资方提供透明和即时可用的贸易信息。这些中小企业基础贸易和业绩记录的信息将使中小企业的信用评估变得更快、更容易，鼓励投资者向中小企业提供融资。同时，这也是为投资方开辟新的投资机会。对于核心买家来说，财务弹性更强的供应商意味着供应链更具弹性，可以促进其建立更稳健、更绿色、更具社会责任感的供应链。

4.6. 跨境金融：港股开户跨境可靠电子签署

为了实现大陆居民、香港居民在线开立香港地区银行账户，深圳 CA 在项目中对持不同身份证件的两地居民提供统一标准的身份核验服务、数字证书服务和电子签署服务。且本项目在大陆和香港两地电子签名互认的司法框架下合法开展，深圳 CA 依据《中华人民共和国电子签名法》《粤港电子签名互认策略》等法律法规签发的数字证书签署的文件，在中国大陆和香港具有法律效力。

4.6.1. 案例背景

随着各行各业信息化的迅猛发展，传统的商业模式逐渐转变成互联网的方式，证券行业同样需要顺应互联网的潮流，基于互联网模式的证券网上开户业务不仅有利于证券公司快速占据客户群和拓展业务中取得先机，同时互联网业务的运行成本低、覆盖面广的优势也将很好解决证券公司网点少、分布不均问题，促进券商业务创新与发展。为了实现大陆居民远程完成港股账户开立全流程，深圳 CA 港股开户电子认证服务平台对持身份证件的大陆居民提供统一标准的身份核验服务、数字证书服务和可靠电子签署服务。

4.6.2. 技术方案

(1) 方案思路

港股开户电子认证服务平台是深圳 CA 依托于跨境粤港互认电子认证服务资质，基于 PKI/CA 密码技术，围绕港股无纸化网上开户业务场景与需求，建设的跨境电子认证及签署服务平台，为港股网上开户提供可靠电子签名服务，确保网上开户与传统线下纸质开户协议具备同等法律效力，为券商业务创新提供支撑与保障，实现大陆居民无需现场面签，即可远程完成港股账户开立全流程。

(2) 方案流程实现

深圳 CA 根据港股远程开户业务中对申请用户身份的认证需求，以及跨境电子认证服务的业务规范，以 PKI/PMI 技术为基础，依托深圳 CA 作为第三方 CA 机构所提供的电子认证服务为核心，为券商提供一个完整的跨境电子认证及可靠电子签署服务平台。通过券商开户系统、APP 集成深圳 CA 的相关 SDK/H5 组件和接口，在券商部署签署服务系统并与深圳 CA 的身份认证服务平台、证书认证系统实现无缝对接，为大陆投资者港股远程开户业务提供完善的身份鉴证、证书签发、在线签署、电子存证、粤港互认等服务。本项目总体架构如图 10 所示：



图 10 深圳 CA 港股开户电子认证服务平台总体架构图

4.6.3. 方案创新点和亮点

本方案将大陆居民身份核验及电子签署 SDK/H5 组件集成在券商的 APP 上，大陆客户可通过券商 APP，无需现场面签，即可远程完成港股账户开立全流程。产品体轻量，实施效率高，客户体验感好。

4.6.4. 应用效果

通过此项目，极大推动了大陆客户在香港股市开设账户，投资港股的进程，也为日后香港资本市场吸引更多大陆客户打下了基础。目前深圳 CA 已经与超过六十家国内及香港券商合作，为近 400 万客户提供港股开户在线电子认证及可靠电子签署服务。多家券商通过实施此港股远程开户项目，使得港股开户业务走在整个行业前列，也为促进两地金融科技合作提供了范本。

4.7. 卫生健康：跨境就医结算服务平台

久远银海跨境就医结算服务平台支持跨区域和跨境接入，实现就医和结算信息共享及业务对接，平台支持机构快速接入及医疗保险快速结算赔付和机构监管等业务。跨境就医结算服务平台提供了机构间互联互通、线上一站式快赔和监管等功能，并支持多方联合确认对象资格、多方审核互认、多方整合赔付路径及确认理赔结果等业务，能够缩短报销等待期，提高结算和赔付效率，并有效支撑对骗保行为的监管等。

4.7.1. 案例背景

随着粤港澳大湾区建设的加速，湾区内居民交流日益密切，越来越多港人到大湾区就医，也会有大陆居民赴港就医的情况，涉及基本医保和商业保险等一站式赔付和监管需求，传统理赔模式存在报销等待期长、报销手续复杂、报销需提交材料多，和个人需要对接多家保险公司等问题，并且由于数据不互通，有可能违反诚信原则，存在骗保行为，监管难度大。

表 2 医保可能存在的赔付群体情况和传统理赔步骤

	大陆医保	大陆商业健康险	香港医保	香港商业健康险	传统理赔步骤
香港居民	✓	✓	✓	✓	优先报销大陆医保，并由参保人凭单据自行选择先行赔付机构，剩下部分可由另外两机构依次赔付；可能存在骗保行为（数据不互通）。
	✓	×	✓	✓	优先报销大陆医保，并由参保人凭纸质单据自行选择先行赔付机构，剩下部分可由另一机构赔付。
	✓	×	×	✓	优先报销大陆医保，再凭纸质单据报销香港商业健康险。
	✓	×	✓	×	优先报销大陆医保，再凭纸质单据报销香港医保。
	×	×	✓	×	所有费用自行垫付，再凭纸质单据报销香港医保。
	×	×	×	✓	所有费用自行垫付，再凭纸质单据报销香港商业健康险。
	×	×	✓	✓	所有费用自行垫付，参保人凭纸质单据自行选择先行赔付机构，剩下部分可由另一机构赔付。
大陆居民	✓	×	×	✓	优先报销大陆医保，参保人自行缴纳自费部分，然后凭纸质单据到香港商业保险公司进行评估、报销。
	✓	✓	×	✓	优先报销大陆医保，并由参保人凭纸质单据自行选择先行赔付机构，剩下部分可由另一机构赔付。可能存在骗保行为（数据不互通）。
	✓	✓	×	×	优先报销大陆医保，再凭纸质单据报销大陆商保。

4.7.2. 技术方案

(1) 方案思路

跨境就医结算服务平台的核心机制在于其实现了大陆医疗保障、大陆医疗机构、香港医疗机构、香港健保和香港商保公司、大陆商保公司之间的数据共享与业务协同。在严格遵守数据不出境的前提下，该平台通过患者（保险消费者）的授权，针对性地解决了理赔难、报销速度慢以及手续繁杂等长期以来的痛点。这

一创新举措不仅极大地提升了医疗保险的消费体验，也显著提高了商保赔付的准确率和效率，同时降低了管理成本和风险。

(2) 功能结构

跨境就医结算服务平台主要由跨境就医理赔中心、跨境就医数据中心和管理规范体系三个核心部分构成。其中，跨境就医理赔中心是处理所有理赔申请的核心机构，负责确认理赔对象的资格、实施多方审核互认，并提供线上一站式快赔服务。

跨境就医数据中心则是处理所有医疗保障数据、医院医疗数据、商保数据的关键机构。该中心对所有数据进行集成和治理，确保数据的准确性和共享的统一管理。这个中心包括数据处理子系统和数据监测子系统，用以实现高效的数据处理和实时监测。

管理规范体系是跨境就医结算服务平台的重要组成部分，它制定了一套全面的跨境医商协同业务规范。这些规范对医疗保障、医疗机构与商保公司之间的数据共享和数据产品应用进行了严格的约束，包括保险产品登记、项目登记、数据使用申请、参保人授权等方面的详细规定。这一体系旨在确保所有数据的合法使用，保护参保人的隐私权，并进一步提升了整个平台的规范性和高效性。

(3) 平台架构

平台的总体框架分为“五层二体系”，如图 11 所示：

系统接入层包括医疗机构接口、医保系统接口、商保理赔接口，可以通过接入这些接口来连接不同的系统，实现数据的共享和交互。

应用服务层包含跨境就医结算服务平台的双中心及所有应用，提供平台的所有业务处理和数据处理。

应用支撑层包括任务管理引擎、控费规则引擎和风控规则引擎等，这一层为上层的应用程序提供了各种支撑服务，用于处理特定的业务需求。

数据资源层包括三目病种库、医院知识库、结算清算库等，涵盖了系统运行所需的各种数据资源。

基础设施层包括云计算平台、分布式存储和云虚拟网络等，提供了平台的基础运算资源和网络支持。

商保理赔数据标准体系和数据安全保障体系可以提高商保理赔效率和准确性，保护保险公司信息安全和客户隐私。



图 11 跨境就医结算服务平台框架结构图

(4) 业务流程

跨境就医结算服务平台是一个集数据处理、业务处理和医疗服务支持于一体的先进平台。该平台的核心是数据中心，它负责处理和存储来自香港的商业保险数据和理赔模型，这些数据和模型是支持跨境就医结算服务的核心组件，为平台的运行提供了重要的参考依据。参保人在深圳医院就诊后，可以通过线上申请理赔并签署授权。申请后，平台通过接口获取医疗保障数据中台及就诊医院 HIS 的基础数据，在数据中心进行数据清洗、数据确权、数据加工、数据流通等处理，处理完的数据将导入一站式理赔子系统。在理赔子系统中，会根据商保数据和理赔模型进行自动化的理赔计算，减少人为错误的可能性，提高理赔处理的效率和准确性。计算得出的理赔结果将输出给香港商保公司，并经其确认无误后，商保公司即向参保人赔付相应的金额。平台业务流程图如图 12 所示。

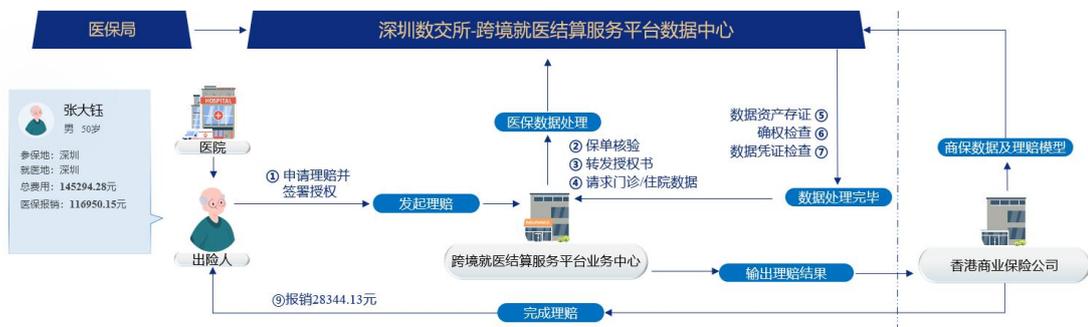


图 12 平台业务流程图

(5) 技术架构

跨境就医结算服务平台的技术架构能够实现高效的数据采集、处理和分析，保障数据的安全和隐私。同时具备可扩展性和灵活性，能够适应不断变化的需求和业务场景。

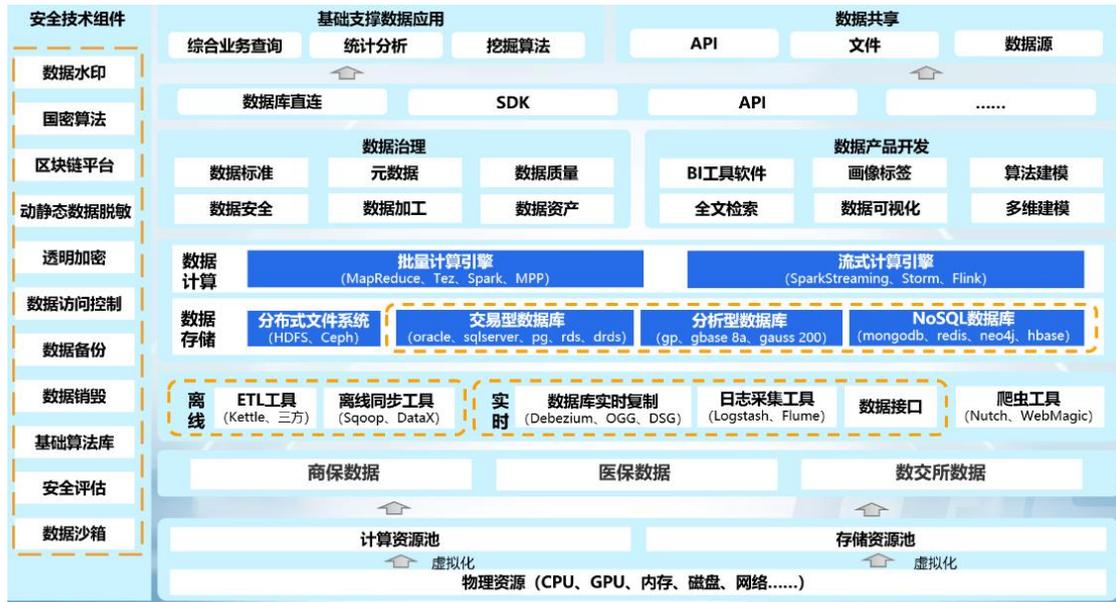


图 13 跨境就医结算服务平台技术架构图

4.7.3. 方案创新点和亮点

跨境就医结算服务对数据安全和隐私保护的要求较高，为此平台采用了多重安全技术与策略。首先，平台应用数据脱敏技术，包括动态脱敏和静态脱敏，以保护患者等敏感信息的真实性和隐私性；平台采用数据加密技术，以确保数据的完整性和机密性，防止未经授权的访问和泄露；平台引入了数据水印技术，能在数据中添加难以察觉的溯源信息，以便在数据发生泄露时能够迅速定位源头，及时采取应对措施；平台运用数据沙箱技术，在保证数据安全的同时，确保数据的使用和分析过程完全在安全的环境中进行；平台采用 API 安全监测与访问控制技术，能够实时监控并识别敏感数据的流动风险，从而及时发现并阻止任何可能的安全威胁，保证数据的安全与稳定传输。

4.7.4. 应用效果

跨境就医结算服务平台对患者（保险消费者）、商保公司、医疗机构和医疗保障部门都有明显的好处。

患者（保险消费者）无需再为了理赔而奔波于香港、大陆和医院、医保局、保险公司之间，大大简化了流程。商保公司不再需要投入大量的人力物力去核实理赔

申请的真实性和完整性，因为平台已经实现了对医疗数据的实时抓取和验证。这不仅提高了理赔的效率和准确率，也降低了商保公司的运营成本，提高了他们的工作效率。通过平台，医疗机构可以减轻工作负担，使其能够专注于提供医疗服务。通过与商保公司的信息共享，医疗机构可以及时获取理赔情况，这有利于提高医疗资源的合理配置。

4.8. 跨境征信：海外用户信用风险评估报告

本案例涉及某大型贸易公司，该公司在全球范围内经营业务，业务板块涉及大量海外贸易场景。由于海外贸易的复杂性、不确定性及信息不对等，导致该公司对其海外客户及供应链上下游合作伙伴的信用风险评估存在挑战。为了有效管理这些海外客户及供应链上下游合作伙伴风险并保护自身利益，该公司决定引入中诚信征信有限公司（简称“中诚信征信”）的海外用户信用风险评估报告。

4.8.1. 案例背景

在国际贸易中，合作客户及供应链合作伙伴信用风险是一个重要的考虑因素。由于交易双方可能存在信息不对称、资金链断裂等问题，导致交易无法按时完成或出现违约情况，应收账款违约损失常年高于 5%；信用交易订单的处理时效低于行业平均水平，也导致公司损失大量业务，限制了业务规模的增长。该大型贸易公司前期希望通过一系列海外报告来监控和管理其海外客户及供应链之间的信用违约风险，以便及时采取措施减少损失，同时为业务规模增长提供支持。

4.8.2. 技术方案

在该案例中海外用户信用风险评估报告,是中诚信征信通过收集和整合来自不同渠道的数据，包括海外供应商和海外客户的信用评级、财务状况、经营活动、诉讼负债等数据，以及中诚信征信基于近 20 年在企业信用风险评估领域积累沉淀的风险评估维度和指标，最终生成满足客户需求的各种类型的海外信用报告，提出风险分析观点和风险评级结果；帮助用户识别其海外客户潜在信用风险，并生成相应的预警信号,方便用户监控海外客户及供应商信用风险状况并进行决策。图 14 为用户信用风险评估报告的处理系统的作业流程示意图，实际以落地系统为准。



图 14 用户信用风险评估报告处理系统作业流程示意图

(1) 技术特点

- 1) 数据收集和整合：系统基于 CCX 编码进行数据的深度关联和检索，从多个渠道获取相关数据，包括公共数据、企业财务报告、社交媒体、生产经营等。
- 2) 机器学习算法：系统使用监督学习和无监督学习算法对数据进行分析 and 建模，以识别潜在的信用风险。
- 3) 知识图谱：系统通过知识图谱和 NLP 算法，挖掘各主体之间的各类关联关系，通过各类关系及关联方的串联识别与展示，排查多维度风险事件，防止风险蔓延。
- 4) 分析和评价结果可视化：系统将模型结果用可视化图表的形式展现，使用户能够快速了解信用风险状况，并做出相应决策。

(2) 技术架构

该系统采用分布式架构，包括数据采集模块、数据处理模块、模型训练模块、风险预警模块和可视化展示模块等。各个模块之间通过 API 进行数据交换和通信。

(3) 工作/业务流程

- 1) 数据采集：系统从不同渠道收集相关数据，包括客户的信用评级、历史交易、财务状况、工商信息、司法信息、生产经营数据等。
- 2) 数据处理：系统对采集到的数据进行清洗、转换和整合，以便后续分析处理。
- 3) 模型训练：系统利用机器学习算法对数据进行训练和建模，以识别潜在

的信用风险。

4) 风险预警：系统根据模型的结果生成相应的预警信号，提醒用户注意潜在的信用风险。

5) 决策支持：用户可以查看风险评分结果，了解信用风险状况，并根据建议额度和自身需要进行相应决策。

4.8.3. 方案创新点和亮点

该系统通过人工智能技术和大数据分析技术，搭建企业评级模型和风险监测模型。能够帮助贸易类进出口公司筛选优质的客户，实时监测和管理与客户之间的信用风险，及时发现潜在问题并采取相应措施，从而降低违约风险和损失。同时，系统提供的可视化图表使用户能够直观地了解信用风险状况，并做到决策流程和审批流程留痕，支持科学决策。

4.8.4. 应用效果

该案例中海外用户信用风险评估报告,在该公司正式使用后取得了显著的应用成效。图 15 为报告模板示意图，实际报告以落地为准。



图 15 征信报告模板示意图

(1) 风险筛查，提高客户质量

通过海外用户信用风险评估报告，快速完成海外客户及供应商的筛选，精准识别优质客户及供应商，极大提高准入筛选效率，提升了对其质量的判断能力，不仅从事前就降低了客户及供应商的信用违约风险，而且使业务规模提高 200%。

(2) 科学审批，提高效率和准确性

该公司业务审批决策流中融入海外用户信用风险评估报告，帮助补足该公司海外客户及供应商信用风险评估数据空缺，使其单位时间内的订单审批数量提高了 150%，审批效率提高 100%，决策更有科学依据。

(3) 动态监测，提高风险处置效率

通过对客户信用风险的定期监测和管理，该公司成功降低了违约风险和损失。

(4) 风险可视化，提高风险感知

海外用户信用风险评估报告内，针对海外客户及供应商信用风险情况，内置多款的可视化图表和风险评估数据，使决策链各环节能够更好地了解海外各客户及供应链合作伙伴信用风险状况，并及时做出决策。

4.9. 健康医疗：临床试验数据跨境合规

在全球医疗创新和数字化高度发展背景下，健康医疗数据的跨境流动需求日益增多。在临床研究中，有时需要通过国内外高水平的多个医学中心合作研究和跨境数据对比分析，研究某种新技术或者新疗法的疗效。医疗机构基于临床研究跨境合作需求，开展数据出境安全评估申报，并成功获得审批，由此，该国际多中心临床研究项目成为数据合规出境示范案例。本案例介绍信联科技作为此项目的支撑单位，通过优质的数据出境咨询服务，协助医疗机构实现数据跨境合规。

4.9.1. 案例背景

(1) 法律层面难点

根据《数据出境安全评估办法》第五条规定，开展数据出境风险自评估，应重点评估以下事项：

- 1) 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；
- 2) 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；
- 3) 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；

4) 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；

5) 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；

6) 其他可能影响数据出境安全的事项；

以上评估事项涵盖临床研究、法律和数据安全等多种维度的合规性，评估报告涉及专业方向多而广，数据出境自评估难度较大。

(2) 业务层面难点

健康医疗数据在跨境合规的评估过程中，医疗出境数据种类繁多，涵盖了病人的病历、诊断结果、治疗方案、药品信息等敏感信息，同时也包括了医生的学术研究、医疗系统的运营数据等重要信息。这些数据的梳理面临诸多困难，如数据量大、处理复杂度高、涉及的隐私和安全问题多等，因此需要专业的第三方数据跨境服务机构协助医疗机构开展数据跨境合规建设。

4.9.2. 合规方案

(1) 数据出境安全评估具体流程

依据《数据出境安全评估申报指南》（第一版），相关医疗数据出境评估流程如下图所示：

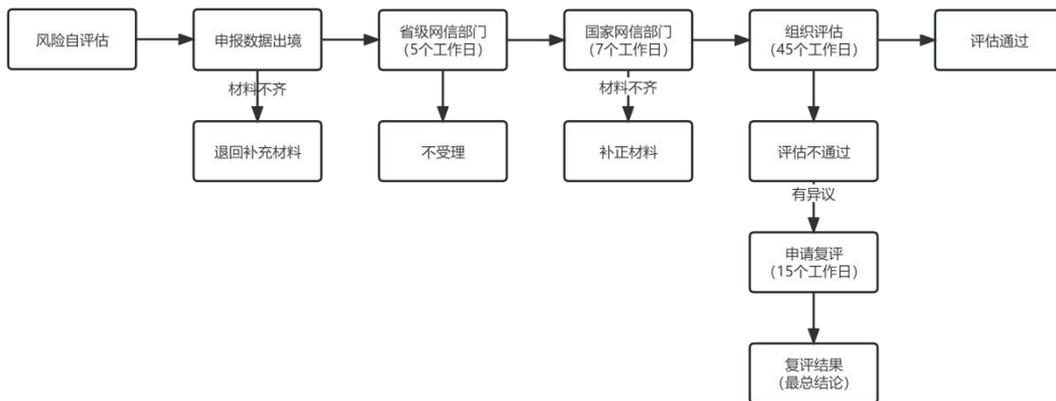


图 16 数据出境安全评估流程

(2) 自评估工作流程

本次自评估咨询服务分为五个阶段：确定评估范围、制定评估计划、收集评估信息、开展评估工作和形成评估报告。



图 17 自评估流程图

各阶段的实施过程说明如下：

1) 确定评估范围：首先，需要明确数据出境的范围和内容，确定需要进行安全评估的出境活动和数据类型。

2) 制定评估计划：根据确定的评估范围，制定详细的评估计划，包括评估时间、评估人员、评估方法等。

3) 收集评估信息：收集与数据出境相关的信息，包括出境活动的具体情况、数据类型、数据量、数据用途、数据安全措施等。

4) 开展评估工作：根据制定的评估计划，开展评估工作，对数据出境的安全性进行评估。需要评估数据出境活动是否符合法律法规的要求，是否采取了必要的措施来保护数据安全。

5) 形成评估报告：在评估工作结束后，形成评估报告，包括评估结果、评估结论、建议等。需要明确指出数据出境活动存在的问题和不足，并提出改进建议。

4.9.3. 方案创新点和亮点

信联科技在数据资产梳理、数据安全保障能力评估、数据安全体系建设等方面对医疗机构（数据处理者）进行深入评估并设计相关整改方案。

(1) 在出境数据层面，信联科技通过盘点医疗机构数据资产，梳理出境临床医疗数据的规模、范围、种类、敏感程度，识别出境数据中是否包含敏感个人信息或重要数据，是否存在不必要的出境数据等。针对出境数据风险，引导医疗机构筛除不必要的出境数据字段，对敏感个人信息和重要数据采取脱敏、去标识等必要的技术手段，以降低出境数据可能对国家安全、公共利益、个人或者组织合法权益带来的风险。

(2) 在业务层面，信联科技协助医疗机构梳理业务流程，识别其是否与当前国家法律法规要求、行业主管部门规定和国家标准建议等存在差距。针对业务合规性风险，引导医疗机构在业务流程中增加数据出境合法性确认环节，例如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。

(3) **在数据安全体系方面**, 信联科技通过人员访谈、查验安全管理制度, 识别医疗机构是否明确数据安全管理机构、设立数据安全负责人、建立数据安全管理制度体系、落实管理监督考核机制等。针对数据安全风险, 建议医疗机构建立或完善数据安全管理体系, 设立数据安全负责人等关键岗位, 健全数据处理活动全流程、数据分类分级、应急处置、个人信息权益保护等管理制度, 并建立数据安全技术保障机制, 搭建数据出境风险防控体系。

4.9.4. 应用效果

(1) **强化数据跨境制度保障**, 信联科技协助医疗机构全面建立包括但不限于明确数据跨境传输管理机制, 建立数据跨境合规评估制度与流程, 建立出境数据分级分类目录及重要数据目录, 提升医疗机构数据跨境安全保障能力。

(2) **培育数据跨境合规理念**, 以数据跨境法规为指引, 推动医疗机构树立全面数据跨境合规理念, 纳入机构数据治理的宏观策略管理, 实现与机构高层领导、业务管理、骨干员工达成数据跨境业务合规共识。

(3) **赋能健康医疗跨境合作**, 本次成功案例为强化医疗健康数据出境安全管理、促进国际医疗研究合作提供了参考示范和实践指引, 推动医学的进步并造福于患者, 为提升全人类生命健康水平作出贡献。

4.10. 跨境贸易：基于区块链的两岸跨境贸易商品溯源系统

为促进两岸经贸文化交流深度融合, 中共中央国务院和福建省政府出台了一系列政策措施, 包括支持两岸企业在数字经济领域开展合作、推进数字基础设施建设、促进数字经济与实体经济深度融合等。

两岸跨境贸易商品溯源应用以促进两岸数字经济融合发展为目标, 厦门海峡链科技有限公司, 与两岸企业携手合作, 运用区块链、IPFS 分布式存储、去中心化验证器等技术, 构建了两岸跨境贸易商品溯源系统, 助力两岸贸易合作、商品数据协同, 促进两岸数字经济融合发展。

4.10.1. 案例背景

根据海关总署的统计数据, 2022 年 1 至 11 月, 两岸贸易总额已达到 2943.9 亿美元。随着两岸产业合作的不断深化, 产业链供应链基本稳固, 越来越多的商品需要在海峡两岸之间进行跨境贸易, 跨境贸易需求逐年稳步增长。然而, 由于两岸在政策、基础设施、行业标准、技术规范等方面存在差异, 导致了数据孤岛

效应，这极大限制了两岸商品数据的跨境流通和应用，严重阻碍了两岸实体经济和数字经济的融合发展。

因此，两岸企业之间迫切需要一套低成本且可信赖、多方协同的跨境贸易商品数据流通方案。这套方案需要在确保商品数据的安全性和防止篡改的前提下，高效地进行商品数据协同与应用，从而加速两岸数字经济的融合发展。

4.10.2. 技术方案

(1) 解决方案思路

海峡链为两岸跨境贸易商品溯源应用提供了关键的技术支持，包括区块链底层平台、IPFS 分布式存储以及 SC-DValidator 去中心验证器等。这些技术的应用在很大程度上保障了贸易商品数据的安全性和共享效率。

区块链技术的分布式、公开透明和防篡改特性为应用提供了坚实的基础。同时，IPFS 分布式存储基于内容的快速寻址和数据永久保存等特性，进一步增强了数据的可靠性和安全性。

在两岸跨境贸易商品溯源应用的设计中，充分考虑了数据的采集、存储、验证和共享等各个环节的需求，结合区块链、物联网以及数字签名技术，对贸易商品数据进行采集、加密、上链、存证，实现安全高效的数据确权、验证和共享。

通过引入去中心验证器和 IPFS 分布式存储等关键技术，应用实现了第三方系统数据的快速核验上链和分布式加密存储，从而进一步保障了贸易商品数据的安全性和可靠性。

(2) 系统框架与功能模块

两岸跨境贸易商品溯源应用基于区块链、IPFS 分布式存储、去中心验证器等技术构建，并结合了物联网、第三方物流系统和供应链系统。如图 18 所示，应用分为四层架构，从下到上依次是区块链层、服务层、物理层以及应用层。

1) 区块链层：整个系统的基础，为数据提供安全保障，确保数据的不可篡改和透明性。其中包括 P2P 网络、共识算法、智能合约、数字签名、IPFS 去中心化存储、分布式身份标识、去中心验证器等海峡链基础设施。

2) 服务层：连接区块链层和物理层，负责管理和操作数据，确保数据的准确性和实用性。提供从品牌到商品的精细化溯源管理服务，包括品牌商管理、信息上链管理、溯源查询、溯源统计、溯源码管理、产品管理等。

3) 物理层：配合应用层，结合物联网技术和物理设备，进行数据采集和数据协同。支持一物一码锚点商品，提供多标识（如条形码、二维码、RFID、NFC 芯片）的全生命周期管理，包括规则配置、标识生成、查询标识、下载标识。

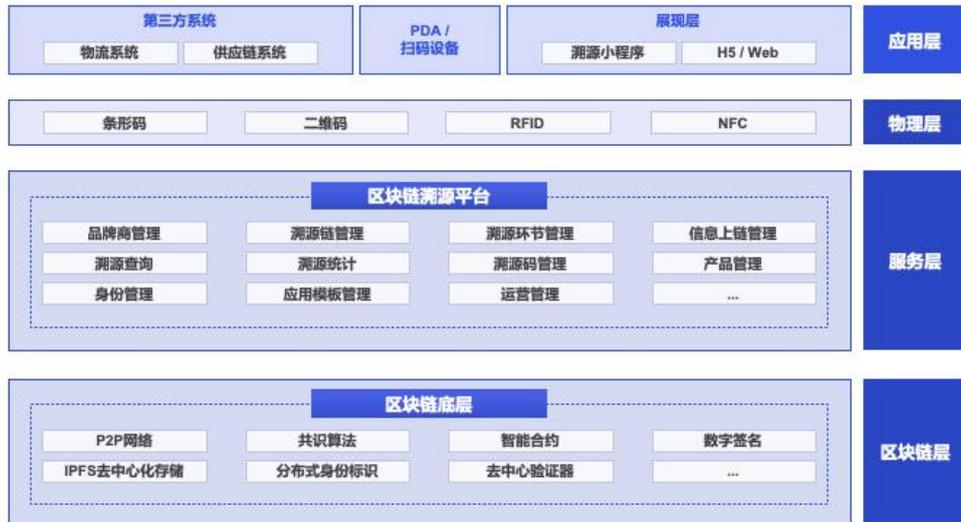


图 18 两岸跨境贸易商品溯源应用技术架构图

4) 应用层：是最接近用户的层级，主要负责数据的展示和交互，为各个应用提供数据支持。支持通过 API 接入第三方物流系统、PAD 或扫码设备的数据，可在小程序、H5、Web 多端展示商品溯源信息、客群分布热力图、扫码统计等功能。

在跨境贸易业务流程中，涉及到多角色和多场景的数据协同。两岸跨境贸易商品溯源应用以区块链和 IPFS 去中心化存储技术为架构基础，确保跨境贸易业务流程中数据协同的高效、稳定和真实性。同时，支持产品从生产制造到终端销售的全流程信息记录上链，并通过微信小程序或区块链浏览器，让消费者快速查验商品。两岸跨境贸易商农产品溯源应用数据上链流程如图 19 所示。

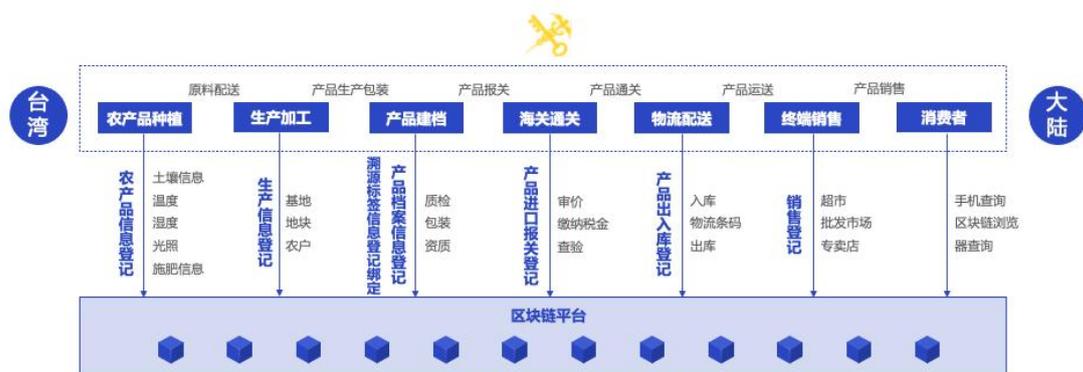


图 19 两岸跨境贸易商农产品溯源应用数据上链流程

图 20 是台湾某有机茶厂的祈韵红茶的数据采集示例：茶园物联网设备实时采集茶叶生长环境数据，如气温、湿度、土壤 PH 值和虫情，并通过 IPFS 进行分布式存储，上链确保数据真实可追溯。平台利用区块链 NFT 作为凭证，每罐

茶叶产品都铸有专属溯源码。全链路数据上链保证了商品信息的真实和可信，实现了茶产量和商标用量的数字化精细管理，从而全面提升茶产品质量。图 21 展示了两岸跨境贸易商品溯源应用案例。



图 20 两岸跨境贸易商品溯源应用数据采集示例



图 21 两岸跨境贸易商品溯源应用案例

4.10.3. 方案创新点和亮点

两岸跨境贸易商品溯源应用具备以下显著特点和创新：

(1) **数据透明可溯源**：区块链的共识机制和链式结构，确保数据的透明和可溯源。

(2) **数据安全防护篡改**：利用区块链的不可篡改特性，结合 IPFS 去中心化存储技术，保障了数据的安全且不可篡改。

(3) **商品唯一可信**：每件商品都通过“一物一码”的方式进行标识，全流程信息被记录上链，确保商品从生产到销售每一个环节的唯一性和可信度。

(4) **数字签名确权**：在信息上链的过程中，每一个环节的参与主体都对所负责的环节的上链数据进行签名，确保信息的真实性，不可抵赖和可追溯。

(5) **数据高效协同**：贸易商品全流程信息上链，确保数据的公开透明和高效协同，解决了多方参与、信息碎片化和重复审核等问题，这大幅降低了沟通和审核成本，提升了跨境贸易的整体效率。

4.10.4. 应用效果

两岸跨境贸易商品溯源应用已经记录多家台湾企业的商品数据信息，涵盖农业、工业、制造业等多个领域，为两岸企业在商品溯源、跨境电商等场景提供服务。通过扫描溯源码，消费者能够查看产品的真实信息，有效降低购买假货风险。应用运营的台湾企业负责人之一在接受大陆媒体采访时表示：通过两岸跨境贸易商品溯源应用，将产品信息和相关证书记录上链，从而方便客户随时查询和验证商品，提高了品牌信用和价值。

两岸跨境贸易商品溯源应用是跨境数据流通的一次全新探索和尝试，其充分发挥区块链技术的优势，解决两岸商品数据孤岛问题，为两岸贸易企业创建高质量的贸易商品数据协同平台。

4.11. 跨境电商：跨境数据推动电商企业 ESG 供应链改进

九鑫智能专注于为跨境电商卖家提供数据管理、决策辅助和智能化等技术手段，帮助他们应对存量竞争激烈和增量天花板的挑战。目前跨境卖家面临着建立核心竞争壁垒和与低价竞争企业抗衡的问题。本案例客户应用九鑫智能行业 ESG AI 模型实现 ESG 目标的持续评估和核心指标监测，通过对全球供应链数据的分析和优化帮助跨境电商卖家大幅降低未销库存比，并引入客户全球市场销售数据跨境，整合历史和目标市场数据，利用行业 AI 模型进行分析和模拟，快速重构业务流程，抓住以价值观为导向的消费群体的新增量机会，实现可持续发展。



图 22 方案功能展示图

4.11.1. 案例背景

(1) 行业现状

中国跨境电商卖家面临着存量竞争激烈和增量天花板的现实问题。一方面，低价内卷策略下的企业通过迎合全球经济下行趋势和消费者对折扣的追求，成为低价市场的领导者。另一方面，中国跨境电商卖家面临欧美等市场需求减缓的巨大挑战。在这种极端竞争下，这些卖家的生产发展空间持续受到压缩。因此企业需要寻求新增量，升级自身的核心竞争壁垒，以应对激烈竞争的局面。

(2) 业务挑战

1) 产品多渠道出海，从“产品第一”到“多渠道出海”需要面对跨境电商的挑战。

2) 在不同国家和地区经营跨境电商需要遵守各自的数据、财务、税务和法律法规。确保数据合规和本土合规是一个复杂的任务。

3) 在可持续发展的背景下，企业需要承担社会责任。在跨境电商中，公司需要确保供应链的可持续性和社会责任的落实。

4) 跨境电商的快速发展可能会对环境造成负面影响，绿色生产和环境友好成为必须关注的问题，需要采取措施减少环境影响。

(3) 应用场景与需求

在不进行重构的前提下，面向后续业务变化、需要灵活调整流程和功能的场景下，客户希望实现以下需求：

1) **可持续供应链管理：**通过全域数据和跨境数据流通，建立透明、可追溯

的供应链系统，以减少资源浪费和环境污染为目标。

2) **基于 AI 和数据驱动的产品设计：**与全球设计师合作，利用 AI 和数据分析预测市场需求，实现按需生产，从而降低成本和库存浪费，并减少侵权事件的发生。

3) **促进可持续消费和经济增长：**通过降低生产成本，将成本优势回馈给全球消费者，促进负担得起的可持续消费。通过可持续转型创造就业机会，与当地消费市场融合并贡献经济增长。

4.11.2. 技术方案

本案例技术方案思路以客户可以实现全域数据驱动的可持续发展，快速提高 ESG 供应链相关评分为目标，采用了统分结合的灵活部署方式，实现数据来源授权可获取、数据分析过程可管理，以及数据执行结果和传输可记录的目标。

(1) **数据整合与共享：**建立一个统一的数据平台，整合全球供应链和业务部门的数据，实现数据的实时共享与更新。采用安全加密和身份验证机制，确保数据来源的授权获取。

(2) **AI 驱动的预测与优化：**建立企业 AI 模型，利用九鑫行业 AI 模型和数据分析技术对全球供应链和业务部门的数据进行实时分析和预测。通过预测市场需求、优化生产计划和库存管理，实现供应链的及时性优化。

(3) **按需生产模式：**基于 AI 预测和需求信号，实现按需生产模式，减少过剩库存和资源浪费。通过实时数据分析和供应链协同，优化生产计划，提高生产效率和供应链的可持续性。

(4) **减少产品设计侵权事件：**对设计师方案内容进行内部审查，减少产品设计侵权事件风险。后继可结合区块链技术，提升知识产权保护，促进全球设计师的合作与创新。

(5) **供应链数据共享与协作：**建立实时数据共享平台，通过协作工具和沟通平台，促进企业内部和供应链合作伙伴之间的高效沟通和协作。实时数据共享和协作能够提高工作效率，优化供应链的整体协同性。

(6) **促进可持续消费和经济增长：**为一些地区建立生产基地，为当地创造就业机会匹配市场扩张需求的项目提供生产成本可控，当地负担得起的可持续消费选择，提供可持续消费分析数据，在获取市场增长同时做好 ESG 专项评估和分析预测。

4.11.3. 方案创新点和亮点

(1) 数据整合与实时共享

通过建立统一的数据平台，整合全球供应链和业务部门的数据，并实现实时的数据共享与更新。这一特点使得企业能够获得准确、全面的数据，同时能够及时了解市场变化并做出相应的决策。

(2) 提高数据及时性

数据能够迅速在全球供应链和业务部门之间流动，实时更新和共享。这种实时性的数据流动使得企业能够更快地获取最新的市场信息和需求变化，从而能够更快地做出决策和调整策略。

(3) 快速响应市场变化

由于数据平台的建立和连接可用技术提升数据的实时性，企业能够更快速地响应市场变化。这种快速响应能力为企业带来了竞争优势，提高了市场反应速度和决策的准确性。

通过跨境数据流通实现企业内部全域数据流动互通，使得数据分析及时有效显著提升，让企业能够更好地应对市场挑战和需求变化。全域数据平台达到供应链协作支撑要求，保障在既定时间实现供应链 ESG 可持续发展的目标和具体指标。

4.11.4. 应用效果

跨境电商在供应链 ESG 挑战中，可通过跨境数据快速实现数据整合与实时共享、及时响应市场变化，基于数据的准确分析和有效预测可大幅降低消耗对提高供应链 ESG 评分至关重要，并且有机会通过更好的 ESG 表现获取新增量市场。本案例以下输出成果可以为行业应用提供参考：

(1) 数据整合与实时共享：通过统一数据平台整合全球供应链和业务部门的数据，并实现实时的数据共享与更新。通过提高供应链数据的准确性和可靠性，预计可提高供应链 ESG 评分约 10%。

(2) 快速响应市场变化：通过准确的数据和实时的信息，该企业能够更快速地响应市场变化，能够更及时地调整供应链和生产计划，提高供应链效率约 12%。

(3) 可持续发展：通过分析提供可持续消费选择、提供促进可持续消费计划。预计可持续发展措施将提高整体 ESG 评分约 10%。

4.12. 数据合规：企业数据出境风险评估

A 为中国境内外资企业，向境外 B 企业提供产品和服务，A 企业向 B 企业交付产品和服务同时通过系统提供 A 企业在中国境内运营和收集的相关数据。广东卓建律师事务所受委托评估 A 企业长期存在的数据出境活动是否合规，以及是否应当立即向网信部门申报数据出境安全评估备案需要从法律方面进行评估，以防范未履行法定义务的法律风险。

4.12.1. 案例背景

根据我国《数据安全法》《个人信息保护法》《数据出境安全评估办法》规定，关键信息基础设施的运营者需要进行数据出境的应通过安全评估，数据处理者确需向中国境外提供个人信息的，需满足法定条件，数据处理者进行数据出境应履行法律规定的义务，出境数量达到法定标准还需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，在申报出境安全评估之前应先进行数据出境风险自评估等。《数据出境安全评估办法》明确规定，在 2022 年 9 月 1 日起前已经开展的数据出境活动，不符合规定的，应当在 6 个月内完成整改，否则应承担相应法律责任。

4.12.2. 合规评估

(1) 聚焦问题及分析思路

问题 1：A 企业在数据出境活动中的具体法定义务有哪些？

《个人信息保护法》第五十五条的规定，向境外提供个人信息的，应当进行个人信息保护影响评估。通过梳理企业的业务流和数据流，A 企业向境外提供的数据包含个人信息，因此，A 企业应当先就个人信息出境事宜进行个人信息保护影响评估。

《数据出境安全评估办法》第五条的规定，在申报数据出境安全评估之前，应先进行数据出境风险自评估，自评估应当对包括数据出境的合法性、正当性、必要性等内容进行评估，并制作数据出境风险自评估报告，作为申报数据出境安全评估的材料之一提交。

《个人信息保护法》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：（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；《数据出境安全评估办法》第六条，申报数据出境安全评估应提交申报书、自评估报告、与境外接收方拟订立的法律文件、安全评估工作需要的其他材料。根据《数据出境安全评估办法》第八条的规定，A 企业与境外接收方签订的相应法律文件

应明确约定双方的数据安全保护责任及义务，确保出境数据的安全以及个人信息权益能够得到充分保障等。因此，除了自评报告之外，A企业还需要与境外接收方订立网信部门制定的标准合同和相应的法律文件。

《个人信息保护法》第三十九条的规定，如需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，并取得个人的同意。因此，针对个人信息出境的情况，A公司应当采取适当的方式告知相关个人，并取得其同意。

数据处理者数据安全保障能力包括数据安全管理能力、数据安全技术能力、数据安全保障措施有效性以及其他应当遵守数据和网络安全相关法律法规的情况等。因此，对A企业与境外接收方B企业的数据安全保障能力需要通过尽调评估和技术测评等手段进行风险排查，以及对于不合规事项应提前予以整改。

问题2：A企业主体资格、出境数据类型、数量以及敏感程度是否达到法定申报评估备案的条件？

通过A企业提交的材料、访谈、会议等方式调查了解，A企业不涉及公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务、国防科技工业等重要行业和领域，未被认定关键基础设施运营者，出境数据类型未列入重要数据白名单，但属于自上年1月1日起累计向境外提供10万人个人信息的数据处理者。结合《数据安全评估办法》规定，A企业应当进行申报备案。

问题3：A企业未申报数据出境安评估的法律责任有哪些？

根据《数据出境安全评估办法》第十八条、第二十条和《个人信息保护法》第六十六条的规定，对于已经开展的数据出境活动，应当在《数据出境安全评估办法》施行之日（即2022年9月1日）起6个月内完成整改；同时，违反《数据出境安全评估办法》对于应当向网信办申报数据出境安全评估但未申报的，可能面临责令改正、警告，拒不改正的，并处一百万以下的罚款，直接负责的主管人员或其他直接责任人员则可能被处一万元以上十万元以下罚款。如果被认定为情节严重的，可能面临责令改正、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，暂停相关业务或者停业整顿、吊销相关业务许可或者吊销营业执照；直接负责的主管人员和其他直接责任人员则可能被处以十万元以上一百万元以下罚款，并可能被禁止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。

(2) 结论

A企业应当对现有的数据出境活动进行全面的风险识别，开展相关评估和申报备案工作，否则直接面临如上所述相关法律责任。具体工作包括但不限于按照

法律规定进行个人信息保护影响评估以及数据出境安全自评估工作, 评估内容包括数据出境及境外接收方数据处理的合法性、正当性、必要性、出境可能对国家安全、公共利益、个人或组织合法权益带来的风险等法律规定的内容; 另外, 还需要准备与境外接收方签订网信部门制定的标准合同和相关法律性文件; 依法提交申报书等安全评估工作需要的其他材料等。

4.12.3. 方案创新点和亮点

《数据出境安全评估办法》规定了企业的出境活动应向监管部门进行申报的条件、提交材料、评估要点、报备流程、备案单位等, 且有时限的要求。如果企业不经专项评估直接进行申报, 必然造成人力、资金、时间等成本支出, 企业的日常运营也会有一定影响, 如果不申报, 又会直接导致承担高额处罚和相关责任, 对企业经济、声誉均会带来重大损失。因此, 对于企业是否应当启动评估申报备案程序、何时启动显得非常重要。本专项风险评估需要投入的工作时间、人力资源、经济支出以及对业务的影响程度, 相较正式的申报评估工作具有周期短、成本低的特点, 如本团队在其他项目中也评估出有的企业不需要向监管部门申报备案, 则可以通过认证、自评估报告、标准合同等方式达到监管对数据出境的要求, 大大节省了企业的各项成本。因此, 通过专业法律分析, 及时解决法律施行后对企业影响的不确定性, 帮助企业在合规的情形下继续开展数据出境活动。

4.12.4. 结语建议

数据合规是企业行稳致远的基础, 数据跨境的违规成本较其他情形的违规成本来说较大, 因此, 企业提前开展是否需要申报的风险评估, 对于企业控制成本与风险具有非常重要的作用, 也是充分发挥数据合规律师专业水平, 提升企业的合规意识, 促进企业高质量发展。

第五章 数据跨境流通与技术应用发展建议

目前我国以《国家安全法》《网络安全法》《数据安全法》《个人信息保护法》和《密码法》等法律法规为框架，国务院、国家网信办、发改委、工信部、公安部、安全部、财政部等单位相继出台了《关键信息基础设施安全保护条例》《商用密码管理条例》《网络数据管理条例（征求意见稿）》《网络安全审查办法》《数据出境安全评估办法》《个人信息出境标准合同办法》《数据出境安全评估申报指南（第一版）》和《规范和促进数据跨境流动规定（征求意见稿）》等配套规范性文件，初步建立了数据保护与数据跨境流动管理体系，为我国企业规范数据跨境处理活动、监管单位审查和监督数据跨境处理活动提供了法律依据。数据跨境除了法律上的合规管理的保障，同时也需要在技术上维护安全可信环境，国家鼓励和支持开展数据流通相关安全技术研发和服务，目前广泛使用的技术包括但不限于区块链、联邦学习、安全多方计算等。

我国现阶段存在市场主体对数据跨境评估审批认知不一、供应链风险控制与管理难、技术与标准难适应、合规人才严重不足、缺乏安全有效的流通模式等问题，既阻碍了数据跨境的安全有序流通，也影响了企业的数据安全能力建设和跨境业务的发展。现结合法律法规的现状和部分企业积极探索的实践经验，开展如下探讨并提出相关建议。

5.1. 数据跨境安全管理底线坚持与便利化探索

为了保障数据跨境流通过程中的合法合规，同时提升数据合规出境的效率，建议可以补充以下方式辅助现有数据出境管理体系：

(1) 企业在向管理部门报送相关材料时，可附上由独立第三方专业机构出具“安全评估风险意见”

在目前的数据出境安全管理框架中，向主管机关申报数据出境安全评估时，数据处理者除了提供“数据出境风险自评报告”之外，可事先委托独立第三方专业机构进行合规、安全和风险的评估，并出具无保留意见的“意见书”，以独立第三方专业机构的专业资质、实践经验及技术能力等为担保，增加监管对申报企业的信心，以期加快审批流程。

(2) 通过拟出境数据自愿预备案模式，为企业提供数据出境合规缓冲区

允许企业根据国家网信办发布的数据出境相关规定，结合实际情况，参照“互联网服务算法”等预备案制度，在正式申请数据出境安全评估前自愿向有关部门申请预备案，待正式申报数据出境安全评估时，可相应简化具体审核的内容和流

程，提高数据出境安全评估行政审核效率。预备案的主要内容可以包括企业基本情况，境外接收方基本情况，出境情况，如数据出境的目的、范围、方式等，出境数据情况，如数据的种类、来源、规模、范围、敏感程度等。预备案模式，不仅有助于国家网信部门事先对拟出境企业数据跨境处理活动的进行合规指导，也有助于提升企业后续申报过程中材料准备的效率。

(3) 根据申报业务场景和数据安全程度，分级分类设置数据出境安全评估行政审核流程，节约审批时间

根据企业申请数据出境的数据种类、来源、规模、范围、敏感程度、潜在风险，数据出境的目的、范围、方式等，可以在流程的繁简程度、审批的时间长短等方面归类处理。如针对数据类型少、敏感程度低、数据量小等数据出境活动，可以适当减化审批环节和时间；或根据数据所涉行业、用途、特点、应用领域等进行分类，适用不同的审查程序等，既帮助企业解决业务的现实合规性，又极大提高审核质量和效率。

因此，建议以粤港澳大湾区为试点，在实践中探索建立数据出境监管的新模式、新方法、新手段。

5.2. 企业全面建成数据跨境合规体系

5.2.1. 企业数据安全性与隐私保护

涉及跨境业务的企业应当依法建立数据出境安全评估和风险监测机制，以保护个人数据、敏感数据、重要数据的跨境流动安全，保证数据出境的合规性、正当性以及必要性。建议企业构建以跨境数据资产盘点与风险识别、跨境数据安全风险监测与预警、跨境数据响应处置与数据留档为核心的跨境数据安全技术体系架构。



图 23 企业跨境数据安全技术体系架构图

(1) 以跨境数据资产盘点与风险识别完善为首要

企业可通过跨境数据资产探测探针等工具主动探测跨境应用、FTP、各种邮件服务、文库等数据资产，梳理各类跨境数据资产的数据资产类型、跨境方式、跨境区域、跨境组织、跨境组织联系人、跨境组织地址等相关信息，并对这些资

产进行多维度管理,用于辅助企业判断数据跨境合规性;针对跨境数据敏感程度、安全防护措施、企业安全保障能力等多方面按照实际情况判断是否需要依法向国家网信办申报数据出境安全评估。

(2) 以跨境数据安全风险监测与预警实效为核心

通过跨境数据风险监测分析引擎,对数据资产探针所采集的各类原始告警,以及各类专项检测引擎输出的告警,进行跨境数据初步关联分析,采取可信技术进行监控和存储,进而输出准确程度更高、更加多方可信的跨境数据安全告警信息。因跨境数据安全分析工作往往是动态的、多变的,需要基于各类实际应用场景灵活调整关联分析策略,以便更有效地应对跨境数据安全监管合规要求,跨境数据风险监测分析引擎类型包括合规性符合风险分析引擎、跨境数据资产脆弱性及弱点分析引擎等。

(3) 以跨境数据响应处置与数据留档夯实为基础

针对跨境数据安全风险监测并预警的风险,跨境数据安全运营专员结合企业自身业务发展情况,制定的安全风险等级和前期制定好的应急预案做通报与处置,相关责任部门根据安全风险预警通报情况制定合理的跨境数据安全治理方案并做相应整改,整个过程数据通过区块链等多方可信技术,全部留档,便于跟踪和安全追溯。

5.2.2. 企业供应链风险控制与管理

供应链合规对于企业顺利安全地开展数据出境业务有重要意义。供应链风险具有关联性,传递性、复杂性和“牛鞭效应”,企业要在国内合规数据的基础上根据国家关于数据出境的相关法律法规的要求评估自身数据处理情况,按照规定流程进行数据出境,最终保障跨境数据的全流程合规。为了加强企业供应链风险评估和监控,保证数据链的畅通和完整,建议可以从以下路径改进供应链合规管理模式的实施。

(1) 企业应建立供应商审核和评估机制,确保潜在供应商的合规性和可靠性。

企业针对与外部供应商的数据流动合作事宜,按照数据安全能力成熟度指南标准,根据自身已达到的标准,对外部供应商的对应能力进行评估,确认供应商在数据安全生命周期过程中可达到的数据安全能力成熟度,不低于企业自身已达到的或数据流动过程中需要达到的最低等级要求,实现对供应商的安全要求选型,降低供应商的数据安全隐患导致的数据泄露或损失。

(2) 企业通过可追溯性系统对供应链进行动态合规管理和监督。

企业应采用信息技术工具和评估系统，加强对供应链合规情况的监控和跟踪。供应链可追溯性是指企业能够追踪和掌握供应链中产品或服务的来源、流向等信息。通过建立可追溯性系统，企业可以更好地监控供应链的合规性，及时发现和解决潜在的违规问题，并对供应商进行及时的提醒和整改。

(3) 企业跟进最新法律法规和行业监管动态，及时调整供应链合规管理机制。

企业根据自身多样化业务场景及流程，对不同类型的供应商开展事前、事中、事后的全面合规风险评估和整改。同时，还应深入解读和实时掌握自身所处行业相关的法律法规、规范、监管要求、查处案例等，设置“合规红线”，将合规操作要求有机嵌入供应链合规管理或指导办法中。此外，企业还应与监管机构保持良好的沟通合作关系，了解最新政策动向，及时调整内部合规规程。

(4) 企业与国际合作伙伴和第三方服务商建立长效合作机制。

企业需加强与政府、行业协会、合作企业、组织和个人等的沟通与合作，共同推动跨境数据流通合规的国际标准制定和协作机制建立。明确合作目标和原则、评估合作伙伴和第三方服务商的合规能力、签订权利义务明确的合同或条款、建立沟通渠道和协作机制、加强合规培训和教育、制定应急预案、定期审计和风险评估等，以确保跨境数据流通合规和安全得到有效保障。建议与外部专业的数据安全机构、咨询公司、律师事务所等合作，共同提升数据安全和合规能力。

此外，在跨境数据流通过程中，企业与第三方进行数据共享时，可通过制定行业规则、建立合作机制、签订数据共享协议等方式，明确数据的使用范围和使用方式、各方在数据合规方面的职责与义务等，实现用户数据的跨平台流通和使用。合作期间，还应不定期对外部服务提供商的安全管理水平和措施进行监督和风险评估，保障供应链管理的有效性。

5.2.3. 企业跨境数据流通合规能力建设

在满足日益增长的数据跨境流通需求的同时确保数据安全和合规、建立健全的跨境数据流通合规管理体系，已成为各国政府和企业共同面临的挑战。作为一个关键性的任务，跨境数据流通合规能力建设涉及到数据安全、隐私保护、合规义务等多方面的问题。

(1) 在战略层面重视跨境数据流通合规能力建设，充分了解并遵守目的国家和地区相关法律法规。

企业需在战略层面重视跨境数据流通合规性，作好整体的合规性规划，并确

保落实数据流通的合规性和安全性。由于不同国家和地区对于数据管理有着不同的法规，例如欧洲的 GDPR、美国的 CCPA 等，企业在进行数据跨境处理活动时必须要遵守业务所在国法律法规，提前全面评估数据跨境传输合规风险，包括数据泄露、数据安全事故、违反相关法规等风险，做好应对和整改措施，以确保数据跨境的合规性。此外，还应加大培养熟悉境外法律法规的数据安全和合规专业人才。

(2) 成立跨部门协作的企业内部数据合规组织机构

企业可以成立跨部门的数据合规组织，明确各岗位职责和任务，建立良好的沟通和协作机制。数据合规组织的成员应该来自企业的各个部门，包括但不限于法务、信息安全、合规、技术等部门，共同探讨数据跨境的业务场景、评估合规风险，制定合规政策和操作规程、开展合规意识和能力的培训和教育，必要情况下，可聘请外部专业的数据安全机构、咨询公司、律师事务所等专家进行内训。此外，数据合规组织还应制定数据跨境安全事件的应急预案（包括启动条件、响应程序、恢复措施等），以应对可能发生的数据跨境安全事件或违规行为。第五，数据合规组织还需定期开展个人信息保护风险评估和审计（包括审计内容、审计时间、审计人员等），以确保数据跨境的数据安全和隐私政策的执行符合要求。

(3) 建立标准、完善的数据安全管理制度，强化数据跨境传输安全保障措施

企业应采用创新的数据安全和合规管理模式，如采用人工智能、区块链等技术手段，提高数据管理和监管的效率和准确性。标准、完善的数据安全管理制度包括但不限于对数据进行分类与标记、设置访问控制、开展定期审查与监测、记录操作日志、实施数据备份与恢复等。建立一套数据流通审计机制，追溯数据流通的路径；建立一套完善的数据保护机制，包括数据加密、数据脱敏、数据备份、数据访问权限控制、数据恢复等，定期评估数据风险；建立一套数据合规风险应急响应机制，及时处理风险问题；建立数据跨境传输审批和监管机制，与相关监管机构保持密切联系（及时了解相关法规和要求），明确审批流程和责任人，确保数据的合规性和安全性。

5.3. 推动跨境数据流通合规技术产业发展

建构跨境数据流通友好型的技术与标准体系，有利于解决数据跨境风险不可见和流转不可知的问题。这套技术体系可包括跨境数据流量采集与还原技术、跨境敏感数据传输发现技术、跨境数据安全风险发现技术、大数据关联分析和事件分析技术、区块链可信确权监管技术等。沉淀在数据跨境过程中的发现敏感数据、预警和及时应对风险的能力，从技术上保障数据的跨境安全和有序流动。

(1) 通过数据采集传输的技术标准，助力发现跨境场景的敏感数据

针对敏感数据发现的问题，企业可借助相关技术标准如跨境数据流量采集与还原技术、跨境敏感数据传输发现技术等予以解决。如跨境数据流量采集与还原技术，即通过对企业互联网侧或者跨境专线流量进行采集和还原，并结合单边、空洞和碎片化流量的补全检测技术，提高流量还原的能力，同时也有效提升敏感数据的检测能力和威胁分析能力。

跨境敏感数据传输发现技术是通过流量还原及特征识别技术对互联网流量进行深度分析还原，利用特征分析、自然语言识别、OCR 等技术实现对传输敏感数据的应用、API 接口进行敏感数据识别、提取、去重，并记录访问时间、数据流入地址等信息。

这些技术标准可以帮助企业保护敏感数据，减少不安全的访问传输导致泄露的风险，实现在相应场景下的技术标准推广，确保数据的安全性和可用性。

(2) 通过跨境数据安全风险发现技术标准，加强数据跨境的风险识别

构建跨境数据安全风险发现技术标准体系，可以有效地提升数据跨境的风险识别能力。跨境数据安全风险发现技术标准体系包括：数据库漏洞发现技术、弱口令风险发现技术、数据爬取风险发现技术、接口鉴权风险发现技术、接口安全漏洞风险发现技术、接口误暴露风险发现技术等。

跨境数据安全风险发现技术标准体系，支持通过技术手段识别和分析数据存储、访问、传输的过程中可能存在的安全漏洞，保障数据跨境的合规机制在技术方面落地，从而确保数据的机密性、完整性和可用性。相关技术标准的推动有助于预研措施保障数据跨境安全，发现处理任何可能的跨境数据泄露事件，避免潜在的损失和风险，提高跨境数据流通的安全性和可靠性。

(3) 跨境数据安全事件发现技术标准，提升数据跨境安全事件的防范能力

构建跨境数据安全事件发现技术标准体系，可以有效地降低数据跨境安全事件带来的安全风险。跨境数据安全事件发现技术标准体系主要包括：利用对威胁情报、攻击事件、敏感数据传输等多维度关联分析，建立攻击者与敏感数据传输通道关联关系，基于敏感数据窃取事件发现技术挖掘攻击者窃取行为的重要信息；基于访问时间、访问源、访问账号、传输方式、传输内容等访问行为相关的多维度敏感数据，通过统计分析手段精确地追踪敏感数据违规传输事件；利用监测手段构建“境内-境外”的数据流转态势，精确追踪敏感数据全路径信息和行为的敏感数据违规出境事件。该标准的发布和推行能够支持企业和监管机构及时发现重要数据违规出境、敏感数据未通过加密链路传输出境、个人敏感数据出境数量超过申报数量或法律法规要求等违规出境传输事件，从而实现数据跨境场景安全事件的防范能力、内部核查和政府监管的能力提升。

(4) 通过区块链及隐私计算的标准，实现跨境数据安全可信流通

为解决数据流通中多方共治、共管的安全和隐私保护，可以通过区块链及隐私计算等新技术基础设施相关标准的指引，保障数据可用不可见，能有效降低不同地区跨境政策和法规可能导致的合规冲突可能性。如区块链作为分布式数据库技术，通过去中心化和共识机制确保数据的安全性和可信度，其分布式、点对点的特点，支持针对跨境场景数据流通和安全审查的技术基础设施层的解决方案，可实现数据不可篡改、透明和可追溯；隐私计算技术在政府管控敏感数据流动的场景下，使数据备份、流通、交易、交换更加安全和高效。

数据跨境场景的区块链及隐私计算的技术标准体系，应包含数据结构标准、网络通信标准、加密算法标准、身份验证标准、隐私计算标准等。推广区块链及隐私计算的技术标准，实现不可篡改的数据链条，实现数据操作分级、确权和监控，保障数据流动的完整性、安全性和可靠性。

5.4. 重视合规人才培养与产业共生

随着跨境数据流通日益频繁，企业对数据合规专业人才的需求也在加速增长。目前，我国数据跨境专业合规人才紧缺，高校、专业培训机构、行业协会、企业等均应重视对数据跨境专业人才的培养。

高校通过设立数据合规相关专业、研究机构等，针对性的开展中国数据出境相关法规、欧盟 GDPR、美国 CCPA、中国数据出境相关法规等课程教学，培养后备力量，为企业和社会提供人才。行业协会可建立数据跨境人才培养机制，聘请行业内外专家开展数据跨境法规和案例培训、宣讲，每年进行数据跨境合规人才和实践案例的选拔和评选等。企业可内部挖掘和培养跨境数据流通合规人才。通过聘请外部专家对数据跨境业务所涉及的国家或地区的法律法规、监管政策、实务场景和处罚案例等进行宣贯，以培训、考试等方式进行内部培养。同时，鼓励和奖励内部员工考取数据合规相关资质证书和认证资格。也可支持和安排合规人才短期出国访问或实习，了解国际最佳实践（包括参与国际项目和与国际数据传输相关的工作内容等），积累国际经验。

企业可以联合高校（如南方科技大学深圳国家应用数学中心、深圳职业技术大学）、行业协会等机构建立合作共享和交流平台，开展数据跨境理论与实践的研讨与交流，互通有无，共同学习和进步。目前，各数据交易所在全国范围内培养数据合规、数据跨境、数据交易、数据价值挖掘等方面的复合人才，如深圳数据交易所开展的 DEXCO（数据交易合规师）的培训认证，帮助企业开展数据合规、数据治理、数据交易、数据资产入表等，取得较好的社会效果。

5.5. 深化开放合作实现跨境合规应用多样化

《数据二十条》提出，深入参与国际高标准数字规则制定，构建数据安全合规有序跨境流通机制。开展数据交互、业务互通、监管互认、服务共享等方面国际交流合作，推进跨境数字贸易基础设施建设，以《全球数据安全倡议》为基础，积极参与数据流动、数据安全、认证评估、数字货币等国际规则和数字技术标准制定。坚持开放发展，推动数据跨境双向有序流动，鼓励国内外企业及组织依法依规开展数据跨境流动业务合作，支持外资依法依规进入开放领域，推动形成公平竞争的国际化市场。实践中，如何建立相互信任，其实是数据跨境的最大挑战。

(1) 积极深入推进国际性数据跨境流通的顶层设计

积极参与联合国、G20、上合组织等国际组织，共同制定多边国际数字规则，推选相关机构和个人参与国际数字化规则的具体制定；积极参与、主导国际、地区间的数据跨境流通协定制定，探索在东盟、一带一路、中非合作等区域性国际合作组织加入区域性国际数据跨境流动制度。推动数据跨境流动双边多边协商，在中日韩、东盟、中欧、中俄、一带一路等双边或多边国际合作中推进建立互利互惠的规则。在国际顶层设计的国际组织、国际交流中倡导反对数据霸权和数据保护主义，探索新的数据主权保护规则。

(2) 积极推进国际标准化和交流合作平台搭建

鼓励并推进国内企事业单位和标准化组织参与 ISO、IET 等国际标准组织，推进数据要素跨境、数据要素安全等国际标准的研究和制定，积极组织相关机构和个人在国际标准组织中组建、参与相关标准工作组，牵头、主导、参与数据流动、数据安全、认证评估、数字货币和数字技术标准的制定。利用现有国际贸易交流合作平台、组建新的数字贸易合作交流平台，面向国际、区域性合作、双边或多边合作，积极开展数据交互、业务互通、监管互认、服务共享等方面国际交流合作。

(3) 面向数据跨境开展顶层设计和制度建设

强化和完善数据跨境法律法规体系的构建。鼓励并组建国家级、区域性智库和研究机构对国际规则、国际数字化协定进行研究，支撑我国主导、参与国际化数字规则的制定；加强对美国、欧盟、日本等国家和国际组织的数据跨境相关规则、法律法规的研究，支撑国内相关机构开展数据跨境合作和业务开展。

对影响或者可能影响国家安全的数据处理、数据跨境传输、外资并购等活动依法依规进行国家安全审查，建立能够统筹国内国外两个循环的安全审查制度、安全评估制度。按照对等原则，对维护国家安全和利益、履行国际义务相关的属于管制物项的数据建立出口管制制度，保障数据用于合法用途，防范数据出境安

全风险。探索构建多渠道、便利化的数据跨境流动监管机制，健全多部门协调配合的数据跨境流动监管体系。加强对国际主流国家相关标准规则的参考，增强我国数据跨境制度与其他国家或地区的国际协定与贸易谈判相衔接。

(4) 积极开展数据跨境流通试点和推广

鼓励在北京、深圳、上海和海南等地面向国际贸易合作国探索数据跨境流动与合作的新途径新模式，鼓励国内外企业及组织依法依规开展数据跨境流动业务合作，支持外资依法依规进入开放领域，推动形成公平竞争的国际化市场。探索建立数据海关、数据保税区等新型跨境数字贸易基础设施。支持北京、深圳、贵阳、上海、海南等数据交易机构试点探索构建国际数据交易市场，积极与国际数据交易场所和机构开展合作，并面向国际组织和企业开展数据跨境交易活动。协同推进数据要素合法合规在各类国际组织间流通，协调好数据走出去与数据走进来的关系。针对跨境电商、跨境支付、供应链管理、服务外包等典型应用场景，探索安全规范的数据跨境流动方式，并适时面向东盟、俄罗斯、一带一路等主要贸易合作对象开展数据跨境试点，推进数据要素的高效跨境流入和流出，并在国际数字贸易具体场景中进行试点和推广。探索建立健全符合数据跨境白名单制度，适当减弱对数据跨境的严格限制，鼓励企业、社会组织积极参与数据国际流通，激活数字经济市场的活力。

(5) 探索粤港澳大湾区数据跨境发展的先行先试

《数据二十条》指出，积极鼓励试验探索。坚持顶层设计与基层探索结合，支持香港作为国际数据中心，辐射推广至整个大湾区，积极发挥高水平开放平台作用，支持有条件支持高端智造、生物医药、绿色低碳、合作办学的等产业加快突破数据可信流通、安全治理等关键技术，建立创新容错机制，探索完善数据要素产权、定价、流通、交易、使用、分配、治理、安全的政策标准和体制机制，更好发挥数据要素的积极作用。因此，应充分发挥粤港澳大湾区的跨境区域协调优势，从湾区的实践和需求出发，通过制定双向或多向清单、互认协议等方式促进湾区内部数据流通循环，建立重点行业如金融数据出境标准建设，积极探索数据要素跨境流通的治理协同标准化，为参与国际数据治理规则的制定作出有益的探索和总结。

因此，一方面要积极主动开展国际交流合作、参与国际规则及标准制定，通过国际组织、智库平台积极开展数据安全、认证评估的相互认可，数据可信空间或者“数据可用不出境”的数据跨境流通系统等探讨，促成相互信任的机制的建立，维护国家安全和利益；另一方面在粤港澳大湾区等重要区域或城市先行先试，建立数据跨境标准体系，鼓励探索数据跨境流动与合作的新途径新模式。

参考文献

- [1] 《区域全面经济伙伴关系协定》,中华人民共和国商务部.
http://fta.mofcom.gov.cn/rcep/rcep_new.shtml
- [2] 陶斌智、蔡彦, 中国对接 CPTPP 数据跨境流动规则的难点及对策, 服务外包, 2023 年 3 月, 34-39
- [3] 王蕊、潘怡辰、袁波、宋云潇, 从 CPTPP 与 RCEP 差异看我国应对数字贸易规则竞争的思路, 国际经贸, 2022 年第 3 期, 12-18
- [4] 石静霞、陆一戈, DEPA 框架下的数字贸易核心规则与我国的加入谈判, 数字法治, 2023 年第 1 期, 107-129
- [5] 中方正式提出申请加入《数字经济伙伴关系协定》(DEPA),
<http://perth.mofcom.gov.cn/article/jmxw/202111/20211103214091.shtml>
- [6] 中国加入《数字经济伙伴关系协定》(DEPA) 工作组正式成立,
<http://jp.mofcom.gov.cn/article/jmxw/202208/20220803343570.shtml>
- [7] https://www.ogcio.gov.hk/sc/about_us/facts/doc/Fact_Sheet-HK_as_ICT_Hub-SC.pdf
- [8] https://www.itib.gov.hk/zh-cn/digital_economy_committee/terms_of_reference/dedc_index.html
- [9] https://www.pcpd.org.hk/sc_chi/data_privacy_law/ordinance_at_a_Glance/ordinance.html
- [10] <https://apps.sfc.hk/edistributionWeb/api/circular/openFile?lang=TC&refNo=22EC69>
- [11] <https://www.hkex.com.hk/-/media/HKEX-Market/Services/Circulars-and-Notices/Participant-and-Members-Circulars/SEHK/2023/CT04423B.pdf>
- [12] https://www.pcpd.org.hk/tc_chi/news_events/media_statements/press_20141229.html
- [13] 杨晓伟,张誉馨,贾丹.粤港澳大湾区数据跨境流动的挑战与对策研究[J].工业信息安全, 2023 (04) :73-78.
- [14] <https://new.qq.com/rain/a/20210820A0FSOQ00>
- [15] 《澳门民法典》第 79 条第 3 款
- [16] 《澳门个人资料保护法》第 3 条
- [17] 方宪文. 我国台湾地区个人资料保护法制研究[D].西南政法大学, 2014.
- [18] <https://mp.weixin.qq.com/s/gPCSWXzxI-flqjYBkqpb-A>
- [19] <https://cbprs.org/government/>
- [20] <https://mp.weixin.qq.com/s/NUZaJ1FTbNX-DIHm0R7Rbw>
- [21] https://mp.weixin.qq.com/s/_WRhYyt0TYPhTft27PnKzQ
- [22] <https://mp.weixin.qq.com/s/6TJyKyEaEZfaABdTYFMunA>
- [23] <https://mp.weixin.qq.com/s/8OHX5pLsZzbu0aKUShm7OA>

- [24] <https://mp.weixin.qq.com/s/8OHX5pLsZzbu0aKUShm7OA>
- [25] <https://ws.ndc.gov.tw/Download.ashx?u=LzAwMS9hZG1pbmlzdHJhdG9yLzEwL3JlbGZpbGUvMC8xMjA2My9IMzMyMjIzMS1jOTM4LTRmZjUtYmZmNi1kNGI1MGYwMGYzZWMu cGRm&n=6KuW6KGhMTYtM180LuWQjeWutuIngOm7njAyX0dEUFLoiIfmiJHlnIvlgIvkurros4fmlpnkv53orbfms5XkuYvmr5TovIPlIbmnPaucGRm&icon=..pdf>
- [26] <https://law.asia/zh-hans/taiwan-cybersecurity-regulations-2022/>
- [27] https://www.ndc.gov.tw/Content_List.aspx?n=726A44EA5D724473
- [28] 王秀哲.我国台湾地区个人资料立法保护评析[J].理论月刊, 2015 (12) :96-101+150.
- [29] <https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan>.
- [30] 曾丽凌.两岸间个人信息跨境提供的规范省思及其完善[J].台湾研究集刊, 2022 (06) :121-140.
- [31] 朱珊珊,王建学.台湾地区特种个人资料的刑法保护及启示[J].台湾研究集刊, 2020 (04) :84-91.
- [32] 张伯超.数据跨境流动的标杆城市: 新加坡[J].上海信息化, 2021 (03) : 54-56
- [33] Vietnam - DLA Piper Global Data Protection Laws of the World
<https://www.dlapiperdataprotection.com/index.html?t=law&c=VN>
- [34] G20 发布《大阪数字经济宣言》(全文中译版),
https://www.sohu.com/a/326519514_500652, 2023
- [35] 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
- [36] CAICT 互联网法律研究中心《印度个人数据保护法案为何历经四度更迭? (附 2022 版全文翻译)》, <https://www.secrss.com/articles/49609>
- [37] 印度《2023 年数字个人数据保护法案》(DPDP) 的英文文本
<https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf>
- [38] The Digital Personal Data Protection Bill, 2023
<https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023>
- [39] Compliance Geeks 合规小组: 《印度公布 2023 年<数字个人数据保护法>》
<https://zhuanlan.zhihu.com/p/653305241>
- [40] CAICT 互联网法律研究中心《印度<2023 年数字个人数据保护法案>(DPDP) 变动解析》, <https://www.secrss.com/articles/58234>
- [41] 《数据合规专栏|印度<数字个人数据保护法>和中国<个人信息保护法>异同》,
https://mp.weixin.qq.com/s/J0y_t9hncOVVQFgmr-kTQ
- [42] Законопроект № 340741-4 «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной

инфраструктуры».

[43] N 152-ФЗ "О персональных данных"

[44] Закон "О персональных данных"Статья 14. Право субъекта персональных данных на доступ к его персональным данным

[45] 沈浩蓝, 《欧盟数据治理的新发展》,

<https://www.chinacourt.org/article/detail/2022/11/id/6994275.shtml>

[46] Orrick 美国奥睿律师事务所.《修订后的 <美国数据隐私和保护法>: 十大要点》.

https://mp.weixin.qq.com/s/MuYsf_wFEM1ajQQQBcUYkA

[47] 赛智时代.《中欧美数据跨境流动研究》,

<https://mp.weixin.qq.com/s/fJlwn-Efum-17OWGDnOBA>

附录 A:数据跨境流通域外法律解析

1. 香港

1.1. 香港《跨境资料转移指引：建议合约条文范本》规定及简析

(1) 《跨境资料转移指引：建议合约条文范本》对《私隐条例》的解读³

根据《跨境资料转移指引：建议合约条文范本》（以下简称“《指引》”），《私隐条例》中的保障资料第 3 原则（个人资料的使用）规定，“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」主要指原本收集资料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」包括披露及转移资料。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，否则保障资料第 3 原则规定需要就有关转移获得资料当事人的订明同意”。

尽管就跨境资料转移施加规限的《私隐条例》第 33 条尚未生效，公署仍鼓励资料使用者遵循《指引》，并在跨境资料转移中应用《指引》建议的合约条文范本，作为其资料管治责任的一部分，以保障及尊重资料当事人的个人资料。资料使用者引入《指引》建议的合约条文范本，有助于其考虑《私隐条例》的相关规管要求以及佐证以下两个方面的行动：（1）资料使用者聘用资料处理者在香港境外代为处理个人资料时，该资料处理者已采取合约规范方法或其他方法以保障个人资料，防止转移给该资料处理者的个人资料的保存时间超过处理该资料所需的时间，以及防止该资料未获准许或意外地被查阅、处理、删除、丧失或使用（该等要求规定在《私隐条例》中的保障资料原则之第 2 原则“个人资料的准确性及保留期间”和第 4 原则“个人资料的保安”）；以及（2）资料使用者在转移资料到香港境外的使用者时，已采取所有合理的预防措施及已作出所有应作出的努力，以确保有关资料不会在获转移资料一方所属的司法管辖区以违反《私隐条例》规定的方式（假如该等活动在香港发生）收集、持有、处理或使用（该要求体现于《私隐条例》中尚未生效的第 33 条（2）（f）项下的规定“（2）除非符合以下条件：否则资料使用者不得将个人资料转移至香港以外的地方：……（f）凡假使该资料在香港以某方式收集、持有、处理或使用，便会属违反本条例下的规定，该使用者已采取所有合理的预防措施及已作出所有应作出的努力以确保该

³https://www.pcpd.org.hk/tc_chi/resources_centre/publications/files/guidance_model_contractual_clauses.pdf

资料不会在该地方以该方式收集、持有处理或使用”）。

(2) 《范本》的适用范围

公署在《指引》中提供了两套范本（该《范本》是可自由组合的独立性条文，也可被纳入资料转移者与资料接收者之间的一般性商业协议中），分别供两种不同的跨境资料转移的情况应用，包括：

第一套：由一个资料使用者转移个人资料给另一个资料使用者的情况，其中资料转移者和资料接收者均分别使用有关个人资料用作其业务用途（例如：为它们各自的商业活动合作共享资料）；

第二套：由资料使用者转移个人资料给资料处理者的情况，其中资料接收者只会为资料转移者指定的用途处理个人资料（例如：一家香港公司订立使用境外的云端服务的安排）。

(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（即一名香港境外的资料使用者）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) 只为与资料转移者协议的转移目的（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）；

2) 确保就与资料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) 采取协议并载列于资料使用者转移资料予资料使用者的建议合约条文模板的资料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，删除有关资料（第 4.5 条）；

6) 采取所有切实可行的步骤，以确保在顾及与资料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，但双方在资料转移一览表作出协议或资料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资料使用者转移资料予资料使用者的

建议合约条文范本或资料使用者转移资料予资料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) 就资料当事人的查阅及改正资料权利，履行作为资料使用者的责任（第 5 条）；及

13) 在收到资料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》，第二套《范本》要求资料转移者（作为一名资料使用者）有责任遵从《私隐条例》的要求，以确保资料处理者依从《私隐条例》的规定，而资料处理者的接收资料一方应满足以下要求：

1) 只为资料转移者指示的目的（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) 确保就资料转移者指示的目的（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，正如资料使用者转移资料予资料处理者的建议合约条文范本中的资料转移一览表所载列（第 3.3 条）；

4) 保留个人资料的时间只会是达致资料转移者指示的目的（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（或按资料转移者的指示），删除有关资料（第 3.5 条）；

6) 采取所有切实可行的步骤，以确保在顾及资料转移者指示的目的（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，但双方在资料转移一览表作出协议或资料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，会符合资料使用者转移资料予资料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，但有资料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	<p>个人资料（personal data）指符合以下说明的任何资料——（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。</p>	<p>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。</p>	<p>香港并未使用中国大陆常用的“个人信息”“个人数据”概念，而是采用“个人资料”一词来指代“Personal Data”。根据《私隐条例》的定义，“个人资料”需要具有“确定性”，即可以确定个人身份的资料才算作“个人资料”，而中国大陆的“个人信息”定义则遵循“可识别性”的思路，涵盖具体个人身份信息和个人关联信息，较香港地区的定义更为宽泛。⁴此外，香港未对匿名化处理后的信息作出规定。</p>

⁴ <https://new.qq.com/rain/a/20210820A0FSOQ00>

2	个人信息处理者	<p>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;</p> <p>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。</p> <p>3.资料处理者 (data processor) 指符合以下两项说明的人——</p> <p>(a) 代另一人处理个人资料; 及</p> <p>(b) 并不为该人本身目的而处理该资料。</p>	<p>第七十三条 本法下列用语的含义:</p> <p>(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。</p> <p>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。</p> <p>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。</p>	<p>中国大陆“个人信息处理者”的含义与香港“资料处理者”的含义有明显区别, 在香港《私隐条例》语境下, 与大陆“个人信息处理者”相似的概念为“资料使用者”, 而《私隐条例》中的“资料处理者”更偏向于大陆《个保法》中受托处理个人信息的“受托人”角色。</p>
---	---------	---	---	---

3	敏感个人信息	未作明确规定	<p>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。</p>	<p>低于中国大陆保护水平，大陆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。</p>
4	同意	<p>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。</p>	<p>根据第十三条、第十四条等的规定，在无第十三条第一款（二）至（七）的情形下，处理个人信息前均需取得个人同意。</p>	<p>低于中国大陆保护水平，大陆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。</p>
5	本地化存储	未作明确规定	<p>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。</p>	<p>香港的保护水平低于中国大陆，大陆对特殊主体所收集和产生的数据进行本地化存储有明确要求，香港未有明确规定。</p>

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	<p>第七条 敏感资料的处理</p> <p>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。</p> <p>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：</p> <p>（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；</p> <p>（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；</p> <p>（三）资料当事人对处理给予明确许可。</p> <p>三、当出现下列任一情况时，亦得处理第一款所</p>	<p>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。</p> <p>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。</p>	<p>低于中国境内保护水平，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。</p>

		<p>指 的资料：</p> <p>(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；</p> <p>(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；</p> <p>(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；</p> <p>(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。</p> <p>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。</p>		
--	--	--	--	--

2	对企业的行政处罚	<p>第三十二条履行义务的不作为或有瑕疵的履行</p> <p>一、基于过失，实体未履行第二十一条第一款和第五款规定的将个人资料的处理通知公共当局义务、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：</p> <p>（一）对自然人科处澳门币 2,000 至 20,000 元罚款；</p> <p>（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。</p> <p>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</p>	<p>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。</p> <p>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，并处五十万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</p>	<p>低于中国境内的保护水平中国境内法律对违反个人信息保护义务的企业处罚力度更大、处罚额度更重。</p>
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	<p>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责任等的行政处罚，但澳门并未做规定</p>	

			企业的董事、监事、高级管理人员和 个人信息保护负责人。	
--	--	--	--------------------------------	--

3. 台湾

3.1. 我国台湾地区《个人资料保护法》规定简析

我国台湾地区于 2010 年颁布《个人资料保护法》作为个人信息保护的基本法，并辅以《个人资料保护法实施细则》配套施行。《个人资料保护法》共有六个章节，分别为总则、公务机关对个人资料之搜集、处理及利用、非公务机关对个人资料之搜集、处理及利用、损害赔偿及团体诉讼、罚则和附则。《个人资料保护法实施细则》则规定了两方面的内容：一是对《个人资料保护法》中的某些具体概念进行界定，比如“医疗”和“医疗个人资料”；其二是一些补充和注意性规定。

经过历史演变和几次修正，我国台湾地区的个人资料保护范围逐渐完善，且救济程序也日趋健全，比如鼓励集体诉讼以及举证责任分配等。近期，台湾地区立法院于 2023 年 5 月通过了《个资法》最新修正案（尚未生效），修正了《个资法》第 48 条非公务机关违反安全维护义务的处罚方式及额度，提高罚款上限为新台币 1500 万元。

3.2. 《个人资料保护法》与《个人信息保护法》部分要点对比分析

序号	对比项目/内容	《个人资料保护法》	《个人信息保护法》	对比分析
1	调整范围	<p>第 51 条</p> <p>自然人为单纯个人或家庭活动的目的而收集、处理或利用个人资料，于公开场所或公开活动中所搜集、处理或利用之未与其他个人数据结合之影音数据，以及公务机关及非公务机关，在台湾域外对台湾民众个人数据搜集、处理或利用的，均不适用该法。</p>	<p>第 9 条</p> <p>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。</p> <p>第 59 条</p> <p>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。</p>	<p>低于中国境内保护水平。台湾的《个人资料》对于不适用法律的情况作了更详细的规定。</p>
2	法域管辖	<p>在台湾发生的所有数据收集及处理活动均适用该法，不论信息当事人是否为台湾籍。根据监管部门解读，该法不具有 GDPR 那样的域外效力⁵。</p>	<p>第 3 条</p> <p>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。</p> <p>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：</p> <p>（一）以向境内自然人提供产品或者服务为目的；</p> <p>（二）分析、评估境内自然人的行为；</p> <p>（三）法律、行政法规规定的其他情形。</p>	<p>低于中国境内保护水平。中国境内法律除了属地管辖原则，还有属人管辖和普遍管辖。</p>
3	个人信息的定义	第 2 条	第 4 条	《个资法》采取列举

⁵ <https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan>

		<p>个人资料：指自然人之姓名、出生年月日、国民身份证统一编号、护照号码、特征、指纹、婚姻、家庭、教育、职业、病历、医疗、基因、性生活、健康检查、犯罪前科、联络方式、财务情况、社会活动及其他得以直接或间接方式识别该个人之数据。</p>	<p>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。</p>	<p>的方式，更细致地对个人信息进行了界定，并侧重个人隐私。《个保法》的界定相对笼统，并排除了匿名化处理后的信息。</p>
4	敏感个人信息的划分	<p>第6条 有关病历、医疗、基因、性生活、健康检查及犯罪前科之个人数据，不得搜集、处理或利用。 但有下列情形之一者，不在此限：</p> <ol style="list-style-type: none"> 1. 法律明文规定。 2. 公务机关执行法定职务或非公务机关履行法定义务必要范围内，且事前或事后有适当安全维护措施。 3. 当事人自行公开或其他已合法公开之个人数据。 4. 公务机关或学术研究机构基于医疗、卫生或犯罪预防之目的，为统计或学术研究而有必要，且资料经过提供者处理后或经搜集者依其揭露方式无从识别特定之当事人。 5. 为协助公务机关执行法定职务或非公务机关履行法定义务必要范围内，且事前或事后有适当安全维护措施。 6. 经当事人书面同意。但逾越特定目的之必要 	<p>第28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。</p>	<p>高于中国境内保护水平。 《个保法》中敏感个人信息的范围更广泛，但《个资法》对敏感个人信息规定了特别的保护。</p>

		<p>范围或其他法律另有限制不得仅依当事人书面同意搜集、处理或利用，或其同意违反其意愿者，不在此限。</p> <p>依前项规定搜集、处理或利用个人资料，准用第八条、第九条规定；其中前项第六款之书面同意，准用第七条第一项、第二项及第四项规定，并以书面为之。</p>		
5	信息处理活动	<p>第 2 条</p> <p>(四) 处理：指为建立或利用个人资料文件所为数据之记录、输入、储存、编辑、更正、复制、检索、删除、输出、连结或内部传送。</p>	<p>第 4 条</p> <p>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。</p>	与中国境内保护水平持平。
6	信息处理者	<p>该法没有特别界定“信息处理者”的概念，有类似的宽泛规定但对这类信息处理者的限制较少⁶。</p>	<p>第 73 条</p> <p>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。</p> <p>第 21 条</p> <p>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。</p>	低于中国境内保护水平
7	信息处理者基本义务	<p>第 8 条 告知义务</p> <p>第 17 条 公开义务</p> <p>第 11 条 资料正确性确保义务</p>	<p>第 51 条</p> <p>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</p>	与中国境内保护水平持平

⁶ <https://iclg.com/practice-areas/data-protection-laws-and-regulations/taiwan>

		<p>资料在特定目的利用范围内力求确实、完整及新颖。</p> <p>第 18、27 条 资料安全保障义务</p> <p>资料管控者有防止个人资料被侵害的义务。</p>	<p>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：</p> <p>（一）制定内部管理制度和操作规程；</p> <p>（二）对个人信息实行分类管理；</p> <p>（三）采取相应的加密、去标识化等安全技术措施；</p> <p>（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；</p> <p>（五）制定并组织实施个人信息安全事件应急预案；</p> <p>（六）法律、行政法规规定的其他措施。</p>	
8	信息处理的合法性基础	<p>对于国家机关：</p> <p>第 15 条</p> <p>国家机关对个人数据之搜集或处理，除第六条第一项所规定数据外，应有特定目的，并符合下列情形之一者：</p> <ol style="list-style-type: none"> 1. 执行法定职务必要范围内。 2. 经当事人同意。 3. 对当事人权益无侵害。 <p>第 16 条</p>	<p>第 13 条</p> <p>符合下列情形之一的，个人信息处理者方可处理个人信息：</p> <p>（一）取得个人的同意；</p> <p>（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；</p> <p>（三）为履行法定职责或者法定义务所必需；</p>	<p>《个资法》区分了两大主体分别进行规制，规制力度也不一。</p> <p>《个保法》没有对信息处理者进行区分，采取统一标准。</p>

		<p> 公务机关对个人资料之利用,除第六条第一项所规定数据外,应于执行法定职务必要范围内为之,并与搜集之特定目的相符。但有下列情形之一者,得为特定目的外之利用: </p> <ol style="list-style-type: none"> 1. 法律明文规定。 2. 为维护国家安全或增进公共利益所必要。 3. 为免除当事人之生命、身体、自由或财产上之危险。 4. 为防止他人权益之重大危害。 5. 公务机关或学术研究机构基于公共利益为统计或学术研究而有必要,且资料经过提供者处理后或经搜集者依其揭露方式无从识别特定之当事人。 6. 有利于当事人权益。 7. 经当事人同意。 <p> 对于非公务机关: 第 19 条 非公务机关对个人数据之搜集或处理,除第六条第一项所规定数据外,应有特定目的,并符合下列情形之一者: </p> <ol style="list-style-type: none"> 1. 法律明文规定。 2. 与当事人有契约或类似契约之关系,且已采取适当之安全措施。 3. 当事人自行公开或其他已合法公开之个人数 	<p>(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;</p> <p>(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;</p> <p>(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;</p> <p>(七) 法律、行政法规规定的其他情形。</p> <p>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。</p>	
--	--	---	---	--

		<p>据。</p> <p>4. 学术研究机构基于公共利益为统计或学术研究而有必要, 且资料经过提供者处理后或经搜集者依其揭露方式无从识别特定之当事人。</p> <p>5. 经当事人同意。</p> <p>6. 为增进公共利益所必要。</p> <p>7. 个人资料取自于一般可得之来源。但当事人对该数据之禁止处理或利用, 显有更值得保护之重大利益者, 不在此限。</p> <p>8. 对当事人权益无侵害。</p> <p>非公务机关对个人资料之利用, 除第六条第一项所规定资料外, 应于搜集之特定目的必要范围内为之。但有下列情形之一者, 得为特定目的外之利用:</p> <p>(一)</p> <p>1. 法律明文规定。</p> <p>2. 为增进公共利益所必要。</p> <p>3. 为免除当事人之生命、身体、自由或财产上之危险。</p> <p>4. 为防止他人权益之重大危害。</p> <p>5. 公务机关或学术研究机构基于公共利益为统计或学术研究而有必要, 且资料经过提供者处理后或经搜集者依其揭露方式无从识别特定之当事人。</p> <p>6. 经当事人同意。</p>		
--	--	--	--	--

		<p>7. 有利于当事人权益。</p> <p>非公务机关依前项规定利用个人资料行销者, 当事人表示拒绝接受行销时, 应即停止利用其个人资料行销。</p> <p>(二)</p> <p>非公务机关于首次行销时, 应提供当事人表示拒绝接受行销之方式, 并支付所需费用。</p>		
9	主体权利	<p>第 3 条 数据当事人的权利</p> <p>当事人就其个人资料依本法规定行使之下列权利, 不得预先抛弃或以特约限制之:</p> <ol style="list-style-type: none"> 1. 查询或请求阅览。 2. 请求制给复制本。 3. 请求补充或更正。 4. 请求停止搜集、处理或利用。 5. 请求删除。 <p>第 15-20 条 当事人同意是个人资料收集利用的程序性条件。</p>	<p>第 44-50 条</p> <ol style="list-style-type: none"> (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。 	<p>低于中国境内保护水平。</p> <p>《个保法》对死者个人信息也赋予了法律保护。</p>
10	当事人同意的要件	<p>第 7 条</p> <p>(一) 第十五条第二款及第十九条第一项第五款所称同意, 指当事人经搜集者告知本法所定应告知事项后, 所为允许之意思表示。</p> <p>(二) 第十六条第七款、第二十条第一项第六款所称同意, 指当事人经搜集者明确告知特定目的外之其他利用目的、范围及同意与否对其权益之影响后,</p>	<p>第 14 条</p> <p>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。</p> <p>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</p>	<p>低于中国境内保护水平。</p> <p>中国境内的“同意”必须由当事人明确作出, 没有推定同意。</p>

		<p>单独所为之意思表示。</p> <p>(三) 国家机关或非国家机关明确告知当事人第八条第一项各款应告知事项时，当事人如未表示拒绝，并已提供其个人数据者，推定当事人已依第十五条第二款、第十九条第一项第五款之规定表示同意。</p> <p>(四) 搜集者就本法所称经当事人同意之事实，应负举证责任。</p>	意。	
11	信息最小化原则	<p>该法没有明确规定最小化原则，但第 5 条有类似规定。</p> <p>第 5 条 个人数据之搜集、处理或利用，应尊重当事人之权益，依诚实及信用方法为之，不得逾越特定目的之必要范围，并应与搜集之目的具有正当合理之关联。</p>	<p>第 6 条 处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。</p>	低于中国境内保护水平。
12	重要平台的特殊义务	未作明确规定。	<p>第 58 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； (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</p>	低于中国境内保护水平。

			<p>处理个人信息的规范和保护个人信息的义务；</p> <p>(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；</p> <p>(四) 定期发布个人信息保护社会责任报告，接受社会监督。</p>	
13	国际司法协助	未作明确规定。	<p>第 41 条</p> <p>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。</p>	低于中国境内保护水平。
14	个人信息跨境的要求	<p>第 21 条</p> <p>非公务机关为国际传输个人资料，而有下列情形之一者，中央目的事业主管机关得限制之：</p> <ol style="list-style-type: none"> 1. 涉及国家重大利益； 2. 国际条约或协议有特别规定； 3. 接受国对于个人数据之保护未有完善之法规，致有损当事人权益之虞； 4. 以迂回方法向第三国（地区）传输个人数据规避本法。 	<p>第 38 条</p> <p>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：</p> <ol style="list-style-type: none"> (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 	低于中国境内保护水平。中国境内对数据跨境流动的要求更高。

			<p>务；</p> <p>(四) 法律、行政法规或者国家网信部门规定的其他条件。</p> <p>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条件等有规定的，可以按照其规定执行。</p>	
15	境内存储的要求	未作明确规定。	<p>第 36、40 条</p> <p>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。</p>	<p>低于中国境内保护水平。</p> <p>《个保法》有信息本地化的要求。</p>
16	黑名单制度	未作明确规定。	<p>第 42 条</p> <p>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。</p>	<p>低于中国境内保护水平。</p> <p>《个资法》未明确设定黑名单。</p>
17	对等原则	未作明确规定。	<p>第 43 条</p> <p>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。</p>	<p>低于中国境内保护水平。</p>
18	过错归责及损害	国家机关：依法归责	<p>第 69 条 过错推定原则</p>	<p>高于中国境内保护水</p>

	赔偿	<p>第 28 条 违反该法有关规定的赔偿责任免责事由仅限于天灾、事变及其他不可抗力。</p> <p>非公务机关：依过错归责</p> <p>第 29 条 违反该法有关规定的赔偿责任免责事由为无故意或过失者。</p> <p>损害赔偿 该法统一规定有财产损害赔偿、精神损害赔偿和名誉损害赔偿三种，并对具体赔偿数额标准划定范围。</p>	<p>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。</p> <p>前款规定的损害赔偿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。</p>	<p>平。</p> <p>《个资法》除了财产损害赔偿之外，还明确规定了精神损害赔偿与名誉损害赔偿，更全面。</p>
19	公益诉讼	<p>该法鼓励公益诉讼。</p> <p>第 34 条 对于同一原因事实造成多数当事人二十人以上以面授予诉讼实施权者，得以自己之名义，提起损害赔偿诉讼。</p> <p>第 39 条 财团法人或公益社团法人依当事人联合授权发起的公益诉讼，不得请求报酬。</p> <p>第 34 条 标的额超过新台币六十万元的公益诉讼，超过部分暂免征裁判费。</p>	<p>第 70 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。</p>	<p>高于中国境内保护水平。</p> <p>《个资法》明确鼓励公益诉讼，并规定了免诉讼费等具体措施。</p>
20	行政处罚	<p>行政处罚主要针对非公务机关。</p> <p>第 47、48、49 条 针对非公务机关的违法收集、处理、利用个人资料的</p>	<p>第 66 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</p>	<p>低于中国境内保护水平。</p> <p>境内处罚力度更重，</p>

		<p>行为，不履行告知、通知等义务，拒绝目的事业主管机关进入、检查或处分，情节轻微的，由目的事业主管机关进行行政处罚，非公务机关的代表人、管理人或其他有代表权人的失职行为也应该接受行政处罚。行政处罚的方式是罚款，分为 2 万元以上 20 万元以下，以及 5 万元以上 50 万元以下两个档次。</p> <p>第 50 条</p> <p>非公务机关代表人、管理人或其他有代表权人，除能证明已尽防止义务外，应并受同一额度罚款处罚。</p>	<p>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。</p> <p>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。</p>	<p>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。</p>
--	--	---	--	---------------------------------------

21	刑事责任	<p>该法区别行为主体是否具有“意图盈利”这一主观要件来划分不同程度的刑事责任。</p> <p>第 41 条 公务机关或非公务机关违法收集、处理或利用（包括目的内或目的外利用）个人资料、损害他人权益的，处两年以下有期徒刑、拘役或科处新台币 20 万元以下罚款。意图盈利犯前项之罪者，刑罚则提高到 5 年以下有期徒刑，得并科新台币壹佰万元以下罚金。</p> <p>第 45 条 意图盈利侵犯个人资料犯罪不以告诉论处。</p> <p>第 44 条：特别规定了公务员犯罪的特殊量刑。 公务员假借职务上之权力、机会或方法，犯本章之罪者，加重其刑至二分之一。</p>	<p>第 71 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。</p>	<p>高于中国境内保护水平。</p> <p>《个资法》统一规定了具体的刑事量刑标准，并对特殊情况进行了特殊规定。</p>
----	------	---	--	---

4. 新加坡

4.1. 新加坡《个人数据保护法》与中国《个人信息保护法》部分要点对比分析表

序号	对比项目/内容	新加坡《个人数据保护法》（PDPA）	中国境内《个人信息保护法》（《个保法》）	对比分析
1	适用范围	<p>4.- (1) 第 3、4、5、6、6A 和 6B 部分不对下列主体施加任何义务</p> <ul style="list-style-type: none"> (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，或其他任何类别的组织或个人数据。 <p>(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根据以书面证明或订立的合同代表另一组织和为该组织目的处理个人数据而对其施加任何义务。</p> <p>(3) 在本法项下，对于由数据中介代表其处理的个人数据和为其目的处理的个人数据，视同该组织处理的个人数据，组织对此负有相同的义务。</p> <p>(4) 本法不适用于下列数据： (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) 关于死亡个人的个人数据，但有关死亡 10 年或 10 年以下者的个人数据应适用个人数据披露规定和第 24 条（个人数据保护）的除外。</p>	<p>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。</p> <p>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。</p>	<p>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、保存 100 年以上的个人信息或者死亡超过 10 年个人的个人信息。</p>

		<p>(5) 除明确规定适用于业务联系信息外，第 3、4、5、6 和 6A 部分不适用于业务联系信息。</p> <p>(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，或法定的义务或限制，包括法律特权，但履行合同义务不构成违反本法的免责事由；和 (b) 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。</p>		
2	个人信息的定义	<p>2.- (1) “个人数据”系指不论真实与否，可被识别为个人的：</p> <p>(a) 特定数据；或</p> <p>(b) 组织已获得或可能获得的特定数据和其他信息；</p> <p>“处理”，就个人数据而言，指进行与该等个人数据有关的下列任何一种或一组操作：(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。</p>	<p>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。</p> <p>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。</p>	<p>结合《中华人民共和国民法典》第六章“隐私权和个人信息保护”的相关规定，中国《个人信息保护法》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。</p>
3	个人信息出境的条件	<p>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程度相当的保护标准。</p> <p>(2) 委员会可根据任何组织的申请，以书面通知免除该组织执行第 (1) 款就该组织转移个人数据的任</p>	<p>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)</p>	<p>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 PDPA 规定的方式提供和 PDPA 下同等的数据保护。</p>

		<p>何规定的要求。</p> <p>(3) 第 (2) 款所称的豁免: (a) 可根据委员会书面规定的条件作出; 和 (b) 无须在政府宪报刊登, 可随时由委员会撤销。</p> <p>(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。</p>	<p>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。</p> <p>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条件等有规定的, 可以按照其规定执行。</p> <p>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。</p>	
4	同意的要件	<p>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:</p> <p>(a) 已向该个人提供第 20 条所要求的信息;</p> <p>(b) 该个人根据本法为此目的表示同意。</p> <p>(2) 组织不得:</p> <p>(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</p> <p>(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。</p> <p>(3) 本条第 (2) 款规定的任何情形下给予的任何同意, 不属于本法规定的有效同意。</p>	<p>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。</p> <p>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。</p>	<p>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, 中国境内要求单独同意, 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出同意。</p>

		<p>(4) 本法中关于个人就收集、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。</p>		
5	视为同意	<p>视为同意规则：</p> <p>15.- (1) 如果个人未给予第 14 条所述的实际同意，自愿为此目的（或可合理认为该个人会自愿）向组织提供个人数据，则被视为该个人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；</p> <p>(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；</p> <p>(3) 在不限第 (2) 款规定的情况下，根据第 (9) 款，向组织 (A) 提供个人数据以使 P 与 A 签订合同的</p>	无。	<p>低于中国境内保护水平。 中国境内的同意均要求是个人信息主体明确做出的。</p>

		<p>个人 (P) 被视为同意以下对于订立 P 与 A 之间合同所合理必要的事项:</p> <ul style="list-style-type: none"> (a) A 向另一个组织 (B) 披露该个人数据; (b) B 收集和使用该个人数据; (c) B 向其他组织披露该个人数据。 <p>(4) 如果任一组织收集 B 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, 如同 A 根据第 (3) (a) 款向该组织披露了该等个人数据。</p> <p>(5) 第 (3) 和第 (4) 款适用于个人于 2021 年 2 月 1 日前就其与任一组织(a)在该日期及以后订立或(b)在该日期前订立但截止提供数据时仍有效的合同向该组织提供的个人数据, 如同第 (3) 和 (4) 款 (a) 在提供个人数据时有效; 且 (b) 效力持续直至 2021 年 2 月 1 日。</p> <p>(6) 在不限第 (2) 款的情况下, 根据第 (9) 款的规定, 与组织 (A) 签订合同并根据该合同或与该合同相关向 A 提供个人数据的个人 (P) 被视为同意以下内容:</p> <ul style="list-style-type: none"> (a) A 向另一个组织 (B) 披露该个人数据, 当该等披露为以下情形所合理必要的: (i) 履行 P 与 A 之间的合同; 或 (ii) A 与 B 订立或履行应 P 要求订立的合约, 或理智人士认为符合 P 利益的合约; (b) B 收集和使用该个人数据, 而收集和使用对于 		
--	--	--	--	--

		<p>(a) 段所述的任何目的而言合理必要；</p> <p>(c) B 向另一组织披露该个人数据，而披露对于 (a) 段所述的任何目的而言合理必要。</p> <p>(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，如同 A 根据第 (6) (a) 款向该组织披露了该等个人数据。</p> <p>(8) 第 (6) 和第 (7) 款适用于个人于 2021 年 2 月 1 日前就其与任一组织在该日期前订立且截止提供数据时仍有效的合同向该组织提供的个人数据，如同第 (6) 和 (7) 款 (a) 在提供个人数据时有效；且 (b) 效力持续直至 2021 年 2 月 1 日。</p> <p>(9) 第 (3) 、 (4) 、 (5) 、 (6) 、 (7) 和 (8) 款不影响 P 与 A 之间的合同项下就以下内容所订明或限制的任何义务：</p> <p>(a) A 可能向另一组织披露的由 P 提供的个人数据； 或</p> <p>(b) A 可向另一机构披露由 P 提供的个人数据的目的。</p>		
6	经由通知视为同意	<p>经由通知视为同意：</p> <p>15A.- (1) 本条适用于组织在 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。</p> <p>(2) 根据第 (3) 款，以下情形视为个人同意组织收集、使用或披露有关其个人的个人数据： (a) 组织满</p>	无。	同上。

		<p>足第 (4) 款规定的要求； (b) 个人没有在第 (4) (b) (iii) 款所述的期限届满之前就其不同意组织拟对其个人数据进行收集，使用或披露通知该组织。</p> <p>(3) 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。</p> <p>(4) 就第 (2) (a) 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：</p> <p>(a) 开展评估以确定拟进行的个人数据收集、使用或披露不太可能对个人产生不利影响；</p> <p>(b) 采取合理步骤提请个人注意以下信息：</p> <p>(i) 组织收集、使用或披露个人数据的意图；</p> <p>(ii) 收集、使用或披露个人数据的目的；</p> <p>(iii) 个人可通知组织不同意该组织拟对其个人数据进行收集、使用或披露的合理期限和合理方式；</p> <p>(c) 符合其他任何规定的要求。</p> <p>(5) 就第 (4) (a) 款所述的评估而言，组织必须：</p> <p>(a) 确定为有关目的而拟进行的个人数据收集、使用或披露可能对该个人产生的任何不利影响；</p> <p>(b) 确定并实施合理措施，以 (i) 消除不利影响；</p> <p>(ii) 降低不利影响发生的可能性；或 (iii) 减轻不利影响；以及</p> <p>(c) 遵守任何其他规定的要求。</p>		
--	--	---	--	--

7	撤回同意	<p>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就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给予或被视为已给予的任何同意。</p> <p>(2) 收到第 (1) 款所称通知后，相关组织应告知该个人撤回其同意可能造成的后果。</p> <p>(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，但本条不影响因撤回而引起的任何法律后果。</p> <p>(4) 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，该组织应当停止（并促使其数据中介和代理人停止）收集、使用或披露个人数据（视情况而定），但该类未经个人同意而收集、使用或披露（视情况而定）是本法或其他成文法要求或授权的除外。</p>	<p>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。</p> <p>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。</p> <p>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。</p>	<p>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。</p>
8	“谢绝来电”条款 (Do-Not-Call 或“DNC”	<p>在 PDPA 的第 9 部分，第 36-48 条规定了“谢绝来电” (Do-Not-Call, 以下简称“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。</p> <p>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</p>	<p>无。</p>	<p>高于中国境内保护水平。</p>

	<p>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。</p> <p>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。</p>		
--	---	--	--

5. 越南

5.1. 中越个人数据保护法部分要点对比分析表

序号	对比项目/内容	越南《个人数据保护法令》	中国《个人信息保护法》	对比分析
1	管辖范围	<p>第 1 条 管辖范围和适用主体</p> <ol style="list-style-type: none"> 1. 越南机构、组织和个人； 2. 在越南的外国机构、组织和个人； 3. 在国外经营的越南机构、组织和个人； 4. 在越南直接参与或涉及个人数据处理活动的外国机构、组织和个人。 	<p>第三条</p> <p>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。</p> <p>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：</p> <ol style="list-style-type: none"> （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。 	与中国《个人信息保护法》所覆盖范围基本一致，同样具有域外效力。
2	个人信息	<p>第 2 条 术语解释</p> <p>“个人数据”是指与个人相关或用于识别个人的符号、字母、数字、图像、声音或等价物形式的电子信息。个人数据包括一般个人数据和敏感个人数据。</p>	<p>第四条</p> <p>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。</p>	与中国《个人信息保护法》的定义基本一致。
3	敏感个人信息	<p>第 2 条 术语解释</p> <p>“个人敏感数据”是指与个人隐私相关、受到侵犯时将直接影响个人合法权益的个人数据，包括：</p> <ol style="list-style-type: none"> 1. 政治和宗教观点； 2. 健康档案中记载的健康状况和个人信息，不包括血型信息； 3. 有关种族或民族血统的信息； 	<p>第二十八条</p> <p>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。</p>	与中国《个人信息保护法》的定义基本一致，越南《个人数据保护法令》的列举式描述更多。

		<ol style="list-style-type: none"> 4. 与个人遗传或获得的遗传特征相关的遗传数据信息; 5. 有关个人自身生物识别或生物特征的信息; 6. 有关个人性生活或性取向的信息; 7. 执法机构收集和存储的犯罪和犯罪活动数据; 8. 信贷机构、外国银行分行、支付中介服务提供者和其他授权机构的客户信息, 包括: 法律法规规定的客户身份信息、账户信息、存款信息、存款资产信息、交易信息, 有关信用机构、银行分支机构、支付中介服务提供者的担保人的信息; 9. 通过定位服务识别个人位置; 10. 法律规定需要特别保护的其他特定个人数据。 		
4	主体角色划分	<p>第 2 条 术语解释</p> <p>“个人数据控制者”是指决定个人数据处理目的和方式的组织或者个人。</p> <p>“个人数据处理者”是指通过与个人数据控制者签订的合同或协议, 代表个人数据控制者处理数据的组织或个人。</p>	<p>第二十一条</p> <p>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。</p> <p>受托人应当按照约定处理个人信息, 不得超出约定的处理目的、处理方式等处理个人信息; 委托合同不生效、无效、被撤销或者终止的, 受托人应当将个人信息返还个人信息处理者或者予以删除, 不得保留。</p> <p>未经个人信息处理者同意, 受托人不得转委托他人处理个人信息。</p>	与中国《个人信息保护法》的角色划分思路基本一致。

5	信息处理合法性基础	<p>第 11 条和第 17 条</p> <ol style="list-style-type: none"> 1.取得数据主体的同意; 2.在紧急情况下, 必须立即处理个人数据以保护数据主体或其他人的生命或健康安全; 3.依据法律规定公开披露个人数据; 4.在紧急状态下或有威胁国家安全和国防的危险、但未达到宣布紧急状态程度的情况下, 为国家主管机关处理国防、国家安全、社会治安、重大灾害、危险流行病等服务; 为防范和打击暴乱和恐怖主义、依法防范和打击犯罪和违法行为服务; 5.依法履行数据主体与相关机构、组织和/或个人的合同义务; 6.依照其他法律规定为国家机关服务而处理个人数据。 	<p>第十三条</p> <p>可以处理个人信息的情形:</p> <ol style="list-style-type: none"> (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。 <p>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。</p>	与中国境内保护水平持平
6	个人信息主体权利	<p>第 9 条 数据主体的权利</p> <ol style="list-style-type: none"> 1. 知情权; 2. 同意权; 3. 访问权; 4. 撤回同意权; 5. 删除权; 6. 限制数据处理的权利; 	<p>第四十四条——第五十条</p> <ol style="list-style-type: none"> (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; 	与中国境内保护水平持平。越南《个人数据保护法》列举的个人信息主体权利类型更为多样, 但中国个人信息主体在侵权等法律框架

		<ul style="list-style-type: none"> 7. 获得数据的权利; 8. 反对数据处理的权利; 9. 投诉、检举和提起诉讼的权利; 10. 索赔权; 11. 自我保护权。 	(七) 权利行使请求权。	下同样享有诉讼、索赔等这些寻求救济的权利, 因此越南个保法与中国个保法在个人信息主体权利方面并无实质性差别。
7	告知同意机制	<p>第 11 条 数据主体的同意</p> <ul style="list-style-type: none"> 1. 除法律另有规定外, 数据主体的同意应适用于个人数据处理中的所有活动。 2. 数据主体的同意仅在数据主体自愿并完全了解以下内容时有效: <ul style="list-style-type: none"> a) 要处理的个人数据的类型; b) 个人数据处理的目的; c) 有权进行个人数据处理的组织和个人; d) 数据主体的权利和义务。 3. 数据主体的同意应通过书面文书、语音、同意框勾选、短信、技术设置选择或其他类似的操作明确作出。 4. 同意应为单一目的。对于多种目的, 个人数据控制者和个人数据控制者和处理者应列出需获取数据主体同意的一个或多个目的。 5. 数据主体的同意应以可以书面打印和/或复制的格式表达, 包括电子或可验证的格式。 6. 数据主体的沉默或不回应不应被视为其同意。 	<p>第十四条</p> <p>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。</p> <p>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。</p> <p>第二十九条</p> <p>处理敏感个人信息应当取得个人的单独同意; 法律、行政法规规定处理敏感个人信息应当取得书面同意的, 从其规定。</p>	高于中国境内保护水平

		<p>7. 数据主体可以给予部分或有条件的同意。</p> <p>8. 关于敏感个人数据的处理，应告知数据主体要处理的数据是敏感的个人数据。</p> <p>9. 在数据主体另有决定或国家主管当局书面要求之前，数据主体的同意应有效。</p> <p>10. 如果发生争议，个人数据控制者和/或个人数据控制者和处理者应负责证明数据主体的同意。</p> <p>11. 如果数据主体已按照本条第 3 款的规定确认并同意，组织和个人可以通过《民法典》授权的方式代表数据主体执行与个人数据控制者或个人数据控制者和处理者处理数据主体个人数据有关的程序，法律另有规定的除外。</p>		
8	将个人数据用于广告营销服务	<p>第 21 条 营销和广告业务中的个人数据保护</p> <p>1. 开展营销和广告业务的组织和/或个人只有在征得数据主体同意的情况下，才能使用在运营过程中收集的客户端个人数据进行营销和广告业务。</p> <p>2. 为营销和广告业务处理客户端个人数据，应在客户知悉产品介绍的内容、方法、形式和频率的基础上，征得客户的同意。</p> <p>3. 提供产品营销和广告服务的组织和/或个人应负责证明根据本条第 1 款和第 2 款向其介绍产品的客户端个人数据的使用。</p>	<p>第二十四条</p> <p>通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。</p>	高于中国境内保护水平
9	个人数据跨境传输	<p>第 25 条 个人数据的跨境传输</p> <p>1. 如果跨境数据传输者已准备了用于评估个人数据跨</p>	<p>第三十八条</p> <p>(一) 依照通过国家网信部门组织的安全评估；</p>	低于中国境内保护水平

	<p>境传输影响的档案并执行了本条第 3、4 和 5 条规定的程序，则越南公民的个人数据可被转移到国外。跨境数据传输者包括个人数据控制者、个人数据控制者和处理者、个人数据处理者和第三方。</p> <p>2. 个人数据跨境传输影响评估档案应包括：</p> <p>a) 越南公民个人数据的数据传输者和接收者的信息和联系方式；</p> <p>b) 越南公民的个人数据传输者和接收者相关负责组织和/或个人的全名和联系方式；</p> <p>c) 描述和解释跨境传输后越南公民个人数据处理的目的；</p> <p>d) 描述和澄清跨境传输的个人数据类型；</p> <p>dd) 遵守此处规定的个人数据保护法规的描述和明确声明，详细说明适用的个人数据保护措施；</p> <p>e) 评估个人数据处理的影响、可能造成的负面后果和损害，以及减少或消除此类后果和损害的措施；</p> <p>g) 本法第 11 条规定的数据主体的同意，该同意应是数据主体在对出现问题/需求时的反馈/投诉机制的充分了解的基础上给予的；</p> <p>h) 数据传输者和接收者之间的关于处理越南公民个人数据的保护义务和责任的相关文件。</p> <p>3. 个人数据跨境转移影响评估档案应随时备存，以供公安部检查和评估。</p> <p>跨境数据传输者应在处理个人数据之日起 60 天内，以本</p>	<p>(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；</p> <p>(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；</p> <p>(四) 法律、行政法规或者国家网信部门规定的其他条件。</p> <p>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。</p>	
--	--	---	--

		<p>法附录中的第 06 号表格向公安部（网络安全与高科技犯罪预防司）提交 01 份原件。</p> <ol style="list-style-type: none">4. 数据传输者在成功完成数据传输后，应将相关数据传输的信息及负责组织和/或个人的联系方式以书面形式通知公安部（网络安全与高技术犯罪预防司）5. 公安部（网络安全与高技术预防犯罪司）应进行评估，如果档案不完整且不符合规定，可要求跨境数据传输者完善个人数据跨境传输影响评估档案。6. 跨境数据传输者应在提交公安部（网络安全和高科技犯罪预防司）的个人数据跨境传输影响评估档案内容发生变化时，以本法附录中第 05 号表格对其进行更新和修改。数据输出方应在内容发生变化之日起 10 天完成对评估档案的更新。7. 除发现违反此处规定的个人数据保护规定或发生越南公民个人数据泄露和丢失事件等的特定情况外，公安部可根据具体情况决定每年进行一次个人数据跨境传输检查。8. 有下列情形之一的，公安部应当决定要求数据跨境传输者停止跨境传输个人数据：<ol style="list-style-type: none">a) 检测到传输的个人数据被用于侵犯越南社会主义共和国利益和国家安全的活动；b) 跨境数据传输者未遵守本条第 5 款、第 6 项的规定；c) 越南公民的个人数据被泄露或丢失。		
--	--	---	--	--

10	<p>违规后的通知义务</p>	<p>第 23 条 违反个人数据保护法规的通知</p> <ol style="list-style-type: none"> 1. 在发现违反个人数据保护规定的行为时，个人数据控制者或个人数据控制者和处理者应在发生本法附录第 03 号表格中的违规行为后 72 小时内通知公安部（网络安全和高科技犯罪预防司）。如果在 72 小时后通知，则必须包括延迟或延迟通知的原因。 2. 个人数据处理者应在发现违反个人数据保护规定时尽快通知个人数据控制者。 3. 违反个人数据保护条例的通知应包括以下内容： <ol style="list-style-type: none"> a) 违反个人数据保护法规的性质描述，包括：时间、地点、行为、组织、个人、个人数据类型和相关数据量； b) 负责数据保护的工作人员或负责个人数据保护的组织或个人的联系方式； c) 描述因违反个人数据保护规定而可能造成的后果和损害； d) 描述为处理和尽量减少违反个人数据保护法规的危害而采取的措施。 4. 如果无法完全通知本条第 3 项规定的内容，可以分期和分阶段通知。 5. 个人信息控制者和/或个人数据控制者和处理者应准备书面记录，确认违反个人数据保护规定的情况，并协调公安部（网络安全与高科技犯罪预防司）处理违规行为。 6. 组织和个人发现下列情况，应当通知公安部（网络安 	<p>第五十七条</p> <p>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：</p> <ol style="list-style-type: none"> （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。 <p>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。</p>	<p>高于中国境内保护水平</p>
----	-----------------	--	--	-------------------

		<p>全与高技术犯罪预防司) :</p> <ul style="list-style-type: none">a) 在个人数据方面存在违法行为;b) 出于不正当目的处理个人数据或不符合数据主体与个人数据控制者和/或个人数据控制者和处理者之间的原始协议或违反法律;c) 数据主体的权利未得到保障或未正确实施;d) 法律规定的其他情况。		
--	--	---	--	--

6. 日本

6.1. 境内境外（具体国家或的确与大陆）法律要求对比（日本）

序号	域外规定	法律条文	中国境内规定	法律条文	与中国境内对比 (高-持平-低)
1	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	个人信息保护法	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。	《个人信息保护法》 第三十八条	低
2	无境内存储特殊要求	个人信息保护法	关键信息基础设施运营者在境内运营收集生产的个人信息或重要数据应当在境内储存	《中华人民共和国网络安全法》第三十七条 条	低
3	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	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。	《个人信息保护法》 第三十九条	低

4	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	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。	《个人信息保护法》 第四条	低
---	-----------------------------------	---------	--	------------------	---

7. 印度

7.1. 印度数据保护法各草案比较

2018 年《个人数据保护法案草案》	2019 年《个人数据保护法案》	2021 年议会联合委员会的建议	2023 年《数字个人数据保护法案》
范围和适用性			
个人数据处理： (i) 印度境内； (ii) 印度境外（如果是为了在印度开展业务、提供商品和服务或分析个人）	扩大 2018 年法案的范围以涵盖某些匿名个人数据	扩大 2018 年法案的范围，包括非个人数据和匿名个人数据的处理	不包括离线个人数据和非自动化处理
报告数据泄露			
受托人通知数据保护机构有关可能造成损害的违规行为，机构将决定是否通知数据委托人	与 2018 年法案相同	所有违规行为，无论潜在危害如何，都必须在 72 小时内向管理局报告	每一起个人数据泄露事件都必须按照规定方式向印度数据保护委员会和每个受影响的数据主体报告
法案在国家安全、公共秩序、预防犯罪等方面规定的豁免。			
处理必须根据法律并按照法律规定的程序获得授权，并且必须是必要的和相称的	中央政府可以根据命令，在必要或方便的情况下豁免机构，但须遵守一定的程序、保障措施和监督	补充说明了命令应当明确程序，公平、公正、合理	中央政府可以通知免除；不需要指定任何程序或保障措施

数据可携带权和被遗忘权			
数据主体将拥有数据可携带权（以可互操作格式获取数据）和被遗忘权（限制通过互联网披露个人数据）	提供两种权利	提供两种权利	不提供
处理个人数据造成的损害			
损害包括金钱损失、身份盗窃、声誉损失和不合理的监视 数据受托人应采取措施尽量减少和减轻损害风险 数据主体在受到损害时有权寻求赔偿	与 2018 年法案相同	中央政府应该有权规定额外的损害	不提供
监管机构			
规定建立： (i) 印度数据保护局来监管该部门 (ii) 上诉法庭。	与 2018 年法案相同	与 2018 年法案相同	规定设立印度数据保护委员会（DPB），其主要职能是裁决违规行为；TDSAT 已被指定为上诉法庭
在印度境外传输个人数据			
每个受托人在印度至少存储一份个人数据副本 如果获得同意，可以转移到印度境外的某些允许的国家或根据管理局批准的合同 某些关键数据只能在印度处理	敏感个人数据的副本应保留在印度 仅在获得明确同意的情况下才能传输某些敏感个人数据，对其他个人数据没有限制 关于关键个人数据，与 2018 年法案相同	补充说明，未经中央政府事先批准，敏感个人数据不会与外国机构或政府共享	删除敏感和关键的个人数据分类 中央政府可能会通过通知将个人数据限制在某些国家/地区

7.2. 印度《2023 年数字个人数据保护法案》和中国《个人信息保护法》的对比

序号	对比要点	印度《2023 年数字个人数据保护法案》	中国《个人信息保护法》
1	数字个人数据定义	本法的规定应适用于在印度境内处理数字个人数据，如果该个人数据收集时是：	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。

		a. 以数字形式 (in digital form) ; 或 b. 以非数字形式 (in non-digital form) 但其后被数字化的;	
2	立法目的	保护个人权利 (the right of individuals to protect their personal data) 和满足处理需求 (need to process such personal data) , 后者与促进数据合法利用的含义相似。	保护个人信息权益, 规范个人信息处理活动, 促进个人信息合理利用。
3	生效时间	不同条款的效力由中央政府 (Central Government) 指定, 不同条款的生效时间可能不同。	自 2021 年 11 月 1 日起施行。
4	儿童个人信息	儿童意味着年龄上不满 18 岁的个体。 处理儿童个人信息的要求包括: (1) 不对儿童身心健康 (well-being) 带来有害影响 (detrimental effect); (2) 禁止追踪 (tracking) 或者行为监控 (behavioural monitoring) 或者针对儿童推送个性化广告 (targeted advertising directed at children) 。	个人信息处理者处理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同意。 个人信息处理者处理不满十四周岁未成年人个人信息的, 应当制定专门的个人信息处理规则。
5	地域范围	本法的规定也应适用于在印度境外处理数字个人数据, 如果此类处理与向印度境内数据委托人提供商品或服务的任何活动有关。	在中华人民共和国境内处理自然人个人信息的活动以及境外处理中华人民共和国境内自然人个人信息的活动: (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。
6	主体概念	数据持有者 (“Data Fiduciary”) : 是指决定数据处理目的和方式的组织或者个人。	个人信息处理者: 个人信息处理活动中自主决定处理目的、处理方式的组织、个人为个人信息处理者。
		重大数据持有者 (Significant Data Fiduciary) : 是指由中央政府根据特定因素通知确定的数据持有者。	大型互联网平台 (“守门人”) : 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。
		数据主体 (“Data Principal”) : 是指与个人数据相关的个人	无明确对应定义, 一般对应“个人/自然人”。

		<p>数据受托人 “Data Processor” : 是指按照数据控制者指示处理个人数据的人。</p>	<p>受托人: 受托人应当按照约定处理个人信息, 不得超出约定的处理目的、处理方式等处理个人信息。</p>
		<p>数据保护负责人 (“Data Protection Officer”) : 是指由重大数据持有者设立的职位。</p>	<p>个人信息保护负责人: 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。</p>
		<p>同意管理人 (“Consent Manager”) : 意为在一个在委员会注册的人 (person), 作为单一联络点, 使数据委托人能够通过一个可访问、透明和可互操作的平台给予、管理、审查和撤销其同意。</p>	<p>中国没有类似的主体设立概念, 个人信息保护责任一般同时具备同意管理经理的职责。</p>
7	排除适用的范围	<p>不适用于个人为个人或者家庭目的处理的个人数据, 也不适用于个人数据主体主动公开或者任何人依据现行有效的法律公开的公开数据。</p>	<p>自然人因个人或者家庭事务处理个人信息的, 不适用本法。 个人信息处理者可以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。</p>
8	处理个人数据的合法性基础	<p>(1) 任何人只能根据本法的规定并出于合法目的处理数据委托人的个人数据, (a) 在数据委托人已同意的情况下; 或 (b) 在特定合法使用 (certain legitimate uses) 的情况下。 特定合法适用的情形包括: ① 自愿提供数据并且未向数据受托人表示不同意使用其个人数据的; ② 提供补贴、福利、服务、证书、执照或许可证时: 接受人同意为此处理其个人数据, 或得中央政府通知从官方数据载体中获取; 相关处理需按中央政策或现行有效的数据管理法律之标准进行;</p>	<p>处理个人数据的合法理由为: (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</p>

		<p>③ 履行职能：依据印度现行有效的法律履行或为了印度的主权和领土完整或国家安全；</p> <p>④ 为履行印度现行有效法律中向国家及国家机构披露义务，并遵循有关披露条款进行的；</p> <p>⑤ 遵守依据印度现行有效的任何法律发布的任何判决、法令或命令，或根据印度境外现行有效的任何法律提出的与合同或民事性质的索赔有关的任何判决或命令的；</p> <p>⑥ 用于响应涉及对数据委托人或其他个人的生命或健康直接威胁的医疗紧急情况；</p> <p>⑦ 在流行病、疾病爆发或任何其他公共健康威胁期间，采取措施向个人提供医疗或保健服务；</p> <p>⑧ 在灾害或公共秩序崩溃期间，采取措施确保个人的安全，或向个人提供援助或服务；</p> <p>⑨ 出于与雇佣相关的目的或与保护雇主免受损失或责任有关的，如防止企业间谍活动，维护商业秘密、知识产权、机密信息，向作为雇员的数据委托人提供其所寻求的服务或利益。</p>	<p>已经合法公开的个人信息；</p> <p>(七) 法律、行政法规规定的其他情形。</p>
9	告知同意	<p>根据个人同意处理个人信息的，个人信息持有者必需通知其将处理的个人数据及目的、个人数据主体权利、向数据保护委员会投诉的途径。如果在印度法律生效前已经获得个人同意的，应当补充通知上述事项。告知同意的语言为英语或者印度宪法规定的语言。同意必需是自愿、特定、充分告知、无条件和清晰、清楚的肯定行为且目的限定。个人享有撤回同意的权利。</p>	<p>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。</p> <p>第十七条 个人信息处理者在处理个人信息前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：</p> <p>(一) 个人信息处理者的名称或者姓名和联系方式；</p> <p>(二) 个人信息的处理目的、处理方式，处理的个人信息种类、</p>

			<p>保存期限；</p> <p>(三) 个人行使本法规定权利的方式和程序；</p> <p>(四) 法律、行政法规规定应当告知的其他事项。</p> <p>前款规定事项发生变更的，应当将变更部分告知个人。</p> <p>个人信息处理者通过制定个人信息处理规则的方式告知第一款规定事项的，处理规则应当公开，并且便于查阅和保存。</p>
10	数据持有者的一般义务	<p>数据持有者的一般义务</p> <p>(2) 数据持有者仅可在有效合同下 (only under a valid contract) 雇佣、指定、使用或通过其他方式引入数据处理者代表其为与向数据委托人提供商品或服务相关的任何活动处理个人数据。</p> <p>(5) 数据持有者应通过采取合理的安全措施来防止个人数据泄露从而保护其拥有或控制的个人数据, 包括由其自身进行的处理或是代表其的数据处理者进行的处理。</p> <p>(6) 如果发生个人数据泄露, 数据持有者应以规定的形式和方式通知委员会和每个受影响的数据持有者。</p> <p>(7) 除却保留数据是遵循任何现行有效法律之必要外, 数据持有者应:</p> <p>a. 删除个人数据 (erase personal data) , 在数据委托人撤回同意 (withdrawing her consent) 或一旦有理由假定不再符合特定目的, 以孰早为准;</p> <p>b. 使其数据处理者删除数据持有者为相应数据处理者处理数据而提供的任何个人数据。</p> <p>(8) 第七款 (a) 项中的“目的”应当被视为不再符合, 如果数据委托人没有:</p>	<p>第五十一条 个人信息处理者应当根据个人信息处理目的、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:</p> <p>(一) 制定内部管理制度和操作规程;</p> <p>(二) 对个人信息实行分类管理;</p> <p>(三) 采取相应的加密、去标识化等安全技术措施;</p> <p>(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;</p> <p>(五) 制定并组织实施个人信息安全事件应急预案;</p> <p>(六) 法律、行政法规规定的其他措施。</p> <p>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:</p> <p>(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;</p> <p>(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</p>

		<p>a. 要求数据持有者履行特定目的； 以及</p> <p>b. 行使其与数据处理有关的任何权利，</p> <p>在所规定的期限内，另外对于不同类别的数据受托人和不同的目的可以规定不同的期限。</p>	<p>害的措施；</p> <p>(三) 个人信息处理者的联系方式。</p> <p>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。</p>
11	个人数据主体权利	<p>个人数据主体享有知情权 (access)、更正权 (correction)、完整权 (completion)、更新权 (updating)、删除权 (erasure)，数据持有者应当提供充分的救济机会 (grievance redressal)；在数据主体死亡或者丧失能力时，指定行使数据主体的权利。</p>	<p>《个保法》在第四章第四十四条至第五十条规定了个人在个人信息处理活动中的权利，包括以下：</p> <p>(1) 个人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；</p> <p>(2) 个人有权向个人信息处理者查阅、复制其个人信息；</p> <p>(3) 个人请求将个人信息转移至其指定的个人信息处理者，符合国家网信部门规定条件的，个人信息处理者应当提供转移的途径；</p> <p>(4) 个人发现其个人信息不准确或者不完整的，有权请求个人信息处理者更正、补充；</p> <p>(5) 有特定情形之一的，个人信息处理者应当主动删除个人信息；个人信息处理者未删除的，个人有权请求删除；</p> <p>(6) 个人有权要求个人信息处理者对其个人信息处理规则进行解释说明；</p> <p>(7) 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；</p> <p>(8) 个人信息处理者应当建立便捷的个人行使权利的申请受理</p>

			和处理机制。
12	数据安全事件通知	发生数据安全事件 (data breach) , 数据持有者应当通知数据保护委员会和受影响的个人数据主体。	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。
13	数据存留期限	除非为遵守任何现行法律而有必要保留, 否则数据持有者应 - (a) 在数据主体撤回其同意或合理假设不再服务于指定目的时 (以较早者为准) 删除个人数据; (b) 导致其数据处理器删除数据持有者提供给该数据处理器处理的任何个人数据。	第四十七条 有下列情形之一的, 个人信息处理者应当主动删除个人信息; 个人信息处理者未删除的, 个人有权请求删除: (一) 处理目的已实现、无法实现或者为实现处理目的不再必要; (二) 个人信息处理者停止提供产品或者服务, 或者保存期限已届满; (三) 个人撤回同意; (四) 个人信息处理者违反法律、行政法规或者违反约定处理个人信息; (五) 法律、行政法规规定的其他情形。 法律、行政法规规定的保存期限未届满, 或者删除个人信息从技术上难以实现的, 个人信息处理者应当停止除存储和采取必要的安全保护措施之外的处理。
14	数据审计和评估	重要数据持有者应 - (a) 任命一名数据保护官; (b) 任命一名独立的数据审计员; (c) 定期进行数据保护影响评估、定期审计和其他措施。	第五十四条 个人信息处理者应当定期对其处理个人信息遵守法律、行政法规的情况进行合规审计。 第五十五条 有下列情形之一的, 个人信息处理者应当事前进行个人信息保护影响评估, 并对处理情况进行记录: (一) 处理敏感个人信息; (二) 利用个人信息进行自动化决策; (三) 委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息;

			<p>(四) 向境外提供个人信息；</p> <p>(五) 其他对个人权益有重大影响的个人信息处理活动。</p> <p>第五十六条 个人信息保护影响评估应当包括下列内容：</p> <p>(一) 个人信息的处理目的、处理方式等是否合法、正当、必要；</p> <p>(二) 对个人权益的影响及安全风险；</p> <p>(三) 所采取的保护措施是否合法、有效并与风险程度相适应。</p> <p>个人信息保护影响评估报告和处理情况记录应当至少保存三年。</p>
15	个人数据跨境传输	<p>中央政府可以通过通知限制数据持有者将个人数据传输到可能通知的印度以外的国家或地区进行处理。</p> <p>本节中的任何内容均不限制印度现行法律的适用性, 该法律规定对印度境外的数据持有者传输与任何个人数据或数据持有者或其类别有关的个人数据提供更高程度的保护或限制。</p>	<p>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：</p> <p>(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；</p> <p>(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；</p> <p>(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；</p> <p>(四) 法律、行政法规或者国家网信部门规定的其他条件。</p> <p>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。</p> <p>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。</p>
16	监管主体	<p>中央政府通过通知可以设立印度数据保护委员会 (Data Protection Board of India), 其主要办公地址 (headquarters)、主席 (chairperson)、成员 (members)、官员 (officers) 和雇</p>	<p>第六十条 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。国务院有关部门依照本法和有关法律、行政法规的规定, 在各自职责范围内负责个人信息保护和监督管理工</p>

		员 (employees) , 均由中央政府规定, 均是公务员 (public servants) , 主席和成员任期均为两年, 可连任。	作。 县级以上地方人民政府有关部门的个人信息保护和监督管理职责, 按照国家有关规定确定。 前两款规定的部门统称为履行个人信息保护职责的部门。
17	处罚	如果委员会在调查结束时认定某人严重违反本法的规定或根据本法制定的规则, 委员会可在给予该人陈述意见的机会后, 处以附表中规定的罚款。 董事会根据本法实施的罚款实现的所有款项应贷记印度统一基金。	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。

8. 欧盟

8.1. 欧盟数据理立法进程

<p>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。</p>
<p>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。</p>
<p>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。</p>
<p>2020年,欧盟发布《欧洲数据战略》,提出形成九个由安全的技术基础设施和治理机制组成的公共数据空间,允许欧盟各地的公共部门和企业以可信的方式和低成本交换数据,使欧盟成为世界上最具竞争力的“数据敏捷经济”。</p>
<p>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。</p>
<p>2022年6月,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,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。法案将数据分为健康数据、移动数据、环境数据、农业数据和公共行政数据五大类,为公共部门与企业、企业之间等进行数据共享搭建了基础性制度。该法案还规定了“数据中介”制度:明确“数据中介服务提供商”独立于数据主体、数据持有人和数据用户,其主要功能为通过技术、法律或其他手段在前述主体之间建立以数据共享为目的的商业关系,仅从事数据交易过程中的中介服务,不能作为数据交易方参与数据交易的过程,以此促进数据交易与流通。2022年2月23日,欧盟委员会正式公布《数据法案》(草案),该法案解决了</p>

导致数据未被充分利用的法律、经济和技术问题。该草案将使更多的数据得到利用，并将确保数字环境的公平性，刺激数据市场竞争，使所有人更容易获取数据，从而为数据驱动的创新提供机会。同时，欧盟委员会于 2022 年 9 月提出了《网络弹性法案》草案 (Cyber Resilience Act)，将推动欧盟围绕网络安全制定更加严格的管理规定。

2022 年 6 月 23 日，欧盟的《数据治理法案》正式生效并将在生效 15 个月后适用（即 2023 年 9 月），该法案建立公共部门数据再利用新机制，针对可以被再利用的数据进行敏感性方面的限制，倡议建立非营利性质的“数据中介机构”并要求数据中介机构在指定的主管当局进行备案。

2023 年，欧盟委员会通过的一项关于网络和信息系统安全的修订指令（“NIS2 指令”）的提案于 2023 年 1 月 16 日生效。NIS2 指令的目的是提高在欧盟运营的各组织的整体网络安全水平。根据对经济和社会的重要性增加新的需要符合最低网络安全要求的产业，以及加强受影响企业的网络安全义务，包括侧重于有效解决供应链和供应商关系中网络安全风险的要求的义务，组织治理和运营风险管理以及网络安全事件报告，以及对国家机构采取更严格的监督措施。同年，欧洲网络安全认证小组 (ECCG) 宣布对新的《欧盟云服务网络安全认证计划草案》展开审查，要求云服务数据需在欧盟存储和处理，并限制欧盟外实体对云服务提供商 (CSP) 的控制。

2023 年 6 月 27 日，欧洲委员会宣布，根据《关于在自动处理个人数据方面保护个人的公约》（《108 号公约》）的修订议定书，通过了跨境数据传输合同示范条款的第一个模块。欧洲委员会强调，该示范条款规范了数据控制者之间的数据流动，并且已准备好由国家当局预先审核，以便将其纳入国家和区域转让文书和机制。这些条款可以被纳入更广泛的合同中，或添加到其他条款或额外的保障措施中，前提是后者不与示范条款或适用的法律相抵触，也不损害《108 号公约》所承认的人权和基本自由。在管理方面，示范条款将受数据出口方所在国家法律管辖，除非该国不承认第三方受益人⁷。

8.2. 欧盟 GDPR 处罚案例

GDPR 从生效至 2023 年 5 月 22 日，累计罚款执法案例 1701 件，罚款总额累计 40.1 亿欧元。2023 年 5 月 22 日，元宇宙（即脸书）位于爱尔兰的主体 Meta Platforms Ireland Limited 被爱尔兰数据保护机构处以 12 亿欧元的罚款，是迄今为止单笔最高的 GDPR 罚款。2021 年，国内某知名短视频社交平台由于“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。2023 年，该公司再次由于违反 GDPR 第 5 (1) a)、12 条、及 13 条被处罚 1450 万欧元罚款。整体而言，GDPR 生效五年来，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。

⁷ <https://www.dataguidance.com/news/international-coe-publishes-model-contractual-clauses>



图A-1 GDPR 执法案件数量走势



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，如表 A-1 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	未遵守数据处理原则	537
2	不遵守数据处理的合法依据	439
3	未采取足够措施确保信息安全	236
4	不遵守主体权利保护保障措施	158
5	不遵守信息义务	76
6	不与数据保护机构合作	48
7	未能实施足够的措施确保信息	37

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。

8.3. 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	<p>GDPR 不在欧盟范围内对各国执法部门的个人制定法律对这一类个人数据处理进行规制。</p> <p>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。</p>	<p>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。</p>	<p>低于中国境内保护水平。</p>
2	法域管辖	<p>第 3 条</p> <p>1. “经营场所原则”既带有属地管辖、也兼有大润属人管辖的成分：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；</p> <p>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据主体的行为进行监控</p> <p>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具有管辖权。</p>	<p>第三条</p> <p>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；</p> <p>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，</p> <p>3. “普遍管辖原则”：法律、行政法规规定的其他情形。</p>	<p>与中国境内保护水平持平</p>

3	个人信息	<p>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。</p>	<p>第四条第二款以电子或以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”</p>	<p>与中国境内保护水平持平</p>
4	敏感个人信息	<p>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。</p>	<p>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。</p>	<p>高于中国境内保护水平</p>
5	信息的处理	<p>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。</p>	<p>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。</p>	<p>与中国境内保护水平持平</p>

6	信息处理者	<p>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。</p> <p>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临更大的风险。</p>	<p>第七十三条</p> <p>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。</p>	<p>低于中国境内保护水平</p>
---	-------	--	---	--------------------------

7	个人信息保护负责人	<p>第 37 条</p> <p>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）</p>	<p>第五十二条</p> <p>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。</p> <p>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 万人的个人信息或者处理超过 10 万人的个人敏感信息的处理者。</p>	高于中国境内保护水平
8	信息处理合法性基础	<p>第 6 条</p> <p>1、基于同意的处理</p> <p>2、无须同意即可处理个人数据的情形：</p> <p>（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现数据主体要求的行为所必需的数据处理；</p> <p>（二）为履行数据控制者的法定义务所必要的数据处理；</p> <p>（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；</p> <p>（四）为履行涉及公共利益的责任或实施已经授予</p>	<p>第十三条</p> <p>可以处理个人信息的情形：</p> <p>（一）取得个人的同意；</p> <p>（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；</p> <p>（三）为履行法定职责或者法定义务所必需；</p> <p>（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；</p> <p>（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；</p>	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。

		<p>数据控制者的职务权限所必要的数据处理；</p> <p>(五) 数据控制者或第三方为追求合法利益目的而进行的必要数据处理，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。</p>	<p>(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；</p> <p>(七) 法律、行政法规规定的其他情形。</p> <p>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。</p>	
9	主体权利	<p>第 18 条、第 15 条、第 20 条、第 12 条、第 17 条</p> <p>(一) 限制处理权 (Right to restriction of processing)，(与知情决定权对应)；</p> <p>(二) 数据主体访问权 (Right of access by the data subject) (与查阅复制权对应)</p> <p>(三) 可携带权 (Right to data portability)</p> <p>(四) 更正权 (Right to Rectification)</p> <p>(五) 删除权 (Right to Erasure) 与被遗忘权 (Right to be forgotten)；</p> <p>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。</p>	<p>第四十四条——第五十条</p> <p>(一) 知情权与决定权；</p> <p>(二) 查阅复制权与可携带权；</p> <p>(三) 更正补充权；</p> <p>(四) 删除权；</p> <p>(五) 解释说明权；</p> <p>(六) 死者个人信息保护权；</p> <p>(七) 权利行使请求权。</p>	<p>低于中国境内保护水平。</p> <p>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。</p>

10	信息处理者基本义务	<p>第 24 条第 1 款、第 32 条第 1 款、第 2 款</p> <p>(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;</p> <p>(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。</p>	<p>第五十一条</p> <p>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:</p> <p>(一) 制定内部管理制度和操作规程;</p> <p>(二) 对个人信息实行分类管理;</p> <p>(三) 采取相应的加密、去标识化等安全技术措施;</p> <p>(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;</p> <p>(五) 制定并组织实施个人信息安全事件应急预案;</p> <p>(六) 法律、行政法规规定的其他措施。</p>	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	<p>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：</p> <p>（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；</p> <p>（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；</p> <p>（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；</p> <p>（四）定期发布个人信息保护社会责任报告，接受社会监督。</p>	<p>低于中国境内保护水平</p> <p>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中介服务提供者的规定。</p>
----	----------------	---	--	---

12	跨境传输个人数据途径	<p>第五章</p> <p>合法数据跨境流动的方式：</p> <p>（一）数据接收国已经达到充分保护水平的数据跨境流动；</p> <p>（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。</p>	<p>第三十八条</p> <p>（一）依照通过国家网信部门组织的安全评估；</p> <p>（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；</p> <p>（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；</p> <p>（四）法律、行政法规或者国家网信部门规定的其他条件。</p> <p>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。</p>	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	<p>第四十条</p> <p>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。</p>	低于中国境内保护水平

14	国际司法协助	无	<p>第四十一条</p> <p>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。</p>	低于中国境内保护水平
15	黑名单制度	无	<p>第四十二条</p> <p>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。</p>	低于中国境内保护水平
16	对等原则	无	<p>第四十三条</p> <p>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。</p>	低于中国境内保护水平

17	泄露补救措施与通知	<p>第 33 条 第 34 条</p> <p>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。</p> <p>无须告知情形：</p> <p>（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；</p> <p>（二）无须通知数据主体的法定情形：</p> <p>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 ；</p> <p>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；</p> <p>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</p>	<p>第五十七条</p> <p>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：</p> <p>（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；</p> <p>（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；</p> <p>（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。</p>	低于中国境内保护水平
----	-----------	---	---	------------

		<p>开告知或者相类似的举措。</p> <p>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。</p>		
18	行政处罚	<p>第 83 条</p> <p>(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营业额 2%的金额的罚款, 两者取其高的一项罚款;</p> <p>(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营业额 4%的金额的罚款, 两者取其高的一项罚款。</p>	<p>第六十六条</p> <p>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。</p> <p>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</p>	与中国境内保护水平持平

			<p>事、高级管理人员和个人信息保护负责人。</p> <p>第六十七条</p> <p>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。</p>	
19	无过错责任	<p>第 82 条</p> <p>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。</p>	<p>第六十九条 过错推定原则</p> <p>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。</p> <p>前款规定的损害赔偿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。</p>	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	<p>以依法向人民法院提起诉讼。</p> <p>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。</p>	低于中国境内保护水平

9. 美国

9.1. 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	在加利福尼亚州开展	《中华人民共和国个人信息保护法》第	低于中国境内保护水平

		<p>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司，满足下列情形之一的，需要遵守 CCPA 所规定的各项要求：</p> <p>(1) 年总收入超过 2500 万美元；</p> <p>(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；</p> <p>(3) 年收入的 50%或以上来自于出售消费者个人信息。</p>	<p>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司，满足下列情形之一的，需要遵守 CPRA 所规定的各项要求：</p> <p>(1) 年总收入超过 2500 万美元；</p> <p>(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；</p> <p>(3) 年收入的 50%或以上来自于出售消费者个人信息。</p>	<p>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。</p> <p>《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。</p>	<p>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息的受托人；而美国 CCPA/CPRA 仅规制符合一定条件的企业。</p>
--	--	---	---	---	---

3	敏感个人信息	未规定敏感个人信息。	<p>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止出售、共享和使用该等信息。敏感个人信息包括：</p> <p>(1) 显示社会保障、驾驶执照、州身份证或护照号码的信息；</p> <p>(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；</p> <p>(3) 精确定位；</p> <p>(4) 种族或族裔血统、宗教或哲学信仰或工会会员身份；</p> <p>(5) 邮件、电子邮件和短信的内容；</p>	<p>《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。</p>	<p>与中国境内保护水平持平</p> <p>虽然 CCPA 未对敏感个人信息作出规定，但 CPRA 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。</p>
---	--------	------------	--	---	--

			<p>(6) 基因数据;</p> <p>(7) 用于识别某人的生物特征信息;</p> <p>(8) 收集和分析的有关个人健康、性生活或性取向的信息。</p>		
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。	<p>《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。</p> <p>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。</p>	<p>低于中国境内保护水平</p> <p>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。</p>	

5	不属于个人信息的情形	<p>美国 CCPA/CPRA 对于个人信息的定义排除了：</p> <ul style="list-style-type: none"> (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。 	<p>《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。</p>	<p>低于中国境内保护水平</p> <p>《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，“个人信息”包含的内容更加丰富。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。</p>
6	合法性基础	<p>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。</p>	<p>《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：</p> <ul style="list-style-type: none"> (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 	<p>高于中国境内保护水平</p> <p>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。</p>

			<p>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；</p> <p>(三) 为履行法定职责或者法定义务所必需；</p> <p>(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；</p> <p>(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；</p> <p>(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；</p> <p>(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。</p>	
--	--	--	--	--

7	同意机制	美国 CCPA/CPRA 采取选择退出模式 (opt-out) 为主要机制。		<p>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。</p> <p>《中华人民共和国个人信息保护法》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。</p>	<p>低于中国境内保护水平</p> <p>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，要求个人数据处理活动应具有合法基础，而美国 CCPA/CPRA 选择退出模式 (opt-out) 为主要机制，仅要求特定的数据处理活动取得个人同意，其他情况下则可以不经个人事先同意而处理数据，但个人可以选择退出。</p>
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	<p>不具备可比性。</p> <p>虽侧重点不同，均为对权利的救济。</p>

				门确定的组织可以依法向人民法院提起诉讼。	
9	行政处罚力度	<p>(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 7500 美元的罚款。</p> <p>(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。</p>	<p>(1) 特别加重了对 16 周岁以下未成年人的隐私权侵权行为的处罚规定。</p> <p>(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。</p> <p>(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。</p>	<p>《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。</p> <p>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</p>	<p>低于中国境内保护水平。</p> <p>在处罚力度方面，中国《个人信息保护法》的处罚力度更大。</p>

				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。	
--	--	--	--	---	--

9.2. 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

9.2.1. 法案背景

2022年6月14日，美国国会众议院能源和商业委员会消费者保护和商业小组委员会正式就《美国数据隐私保护法》（American Data Privacy and Protection Act，以下简称“《法案》”）草案召开听证会，将美国联邦层面的隐私保障纳入立法日程，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，能源和商业委员会通过了修订后的《法案》，该法案即将进入全众议院投票阶段。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。

9.2.2. 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、完全从多个独立来源的公开信息中做出的不会泄露与个人敏感数据的信息。

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) 雇主处理的与以专业身份为雇主工作的员工有关的信息，但这些信息的收集、处理或传输仅用于与该雇员代表雇主开展的专业活动有关的目的；

c) 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；

d) 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；

e) 与员工（或该员工的亲属或受益人）有关的信息，但这些信息被雇主收集、处理或传输仅是为管理该员工（或该员工的亲属或受益人）因其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；同时要求适用主体以明确和显著的方式公开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；

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；

——超过 200,000 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“同意”。

4) 禁止事先同意

不得通过以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;
- 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、电话或短信记录、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。如果此类信息是从雇主提供给雇员的设备中发送或接收的, 且雇主已明确告知可以访问此类信息, 则此类信息不属于本段所指的敏感信息。
- 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. 识别一段时间内个人在第三方网站或在线服务上的在线活动的信息。
- o. 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护数据主体所需求的特定产品或服务所绝对必要的，或对于实现本法第 101 条 (b) 款 1-12 项、14-15 项所列举的目的是绝对必要的。

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之的传输行为；

d) 在政府指示下行事的服务提供商，或向政府提供服务的适用实体，仅在法律授权的范围内，为防止、侦察、防范或应对公共安全事件（包括非法入侵、自然灾害或国家安全事件）而必须进行的传输；

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之的遗传信息传输行为；

g) 以本法第 101 (b) 条第 13 项描述的方式转让资产。

d. 对于广播电视服务、有线电视服务、卫星服务、流媒体服务或 1934 年《通信法》(47 U.S.C. 613 (h) (2)) 第 713 (h) (2) 节中所述的其他视频节目服务的提供商，向非关联第三方传输披露个人从该等服务中请求或选择的视频内容或服务的相关数据，除非个人明确表示同意，或符合第 101 (b) 条第 (1) 至 (15) 项中列举的允许目的之一。

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) 消费者的数据权力

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；相关数据的类别；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、删除和可迁移权

a. 权利内容：

可迁移权（Portability Of Covered Data）：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；或者是可迁移的、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 45 天内完成相应访问、更正、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推送定制化广告服务。

b. 对于明知是未成年人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. 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。

1) 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. 对于大型数据持有者，法案额外要求指定至少一名隐私官、数据安全官直接向大型数据持有者的首席执行官进行汇报，由其负责大型数据持有者的隐私安全政策、实践的评估和更新、进行员工培训、作为大型数据持有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进行一次隐私影响评估，评估内容包括大型数据持有者收集、处理、传输的数据的性质、量级以及对个人隐私构成的潜在重大风险，评估需要形成书面的评估报告，并经前述被指定的大型数据持有者的隐私官、数据安全官批准。

9.2.3. 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，国内尚无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，明确禁止向儿童和未成年人投放定向化广告。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。

(4) 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, 对于大型数据持有者, 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。不过, 对于个人数据可携带权、数据安全官、漏洞和风险评估等义务, 法案对中小企业加以豁免。这也体现了美国立法者的对数字经济加以保护的立法取向。

附录 B：编写单位简介⁸

北京市汉坤 (深圳) 律师 事务所	北京市汉坤律师事务所是一家经司法主管部门批准设立的合伙制律师事务所，是一家以提供资本市场法律服务为基础，同时擅长在政府监管、反垄断、知识产权、劳动关系和争议解决等业务领域提供高质量法律服务的综合性领先律师事务所。
北京市京师 (深圳) 律师 事务所	北京市京师（深圳）律师事务所成立于 2018 年，构建了强大的专业法律服务团队，并与外部生态合作方形成全方位的企业服务能力；同时依靠着深圳独特的地理优势与政策优势，依托国际业务中心，联合所内众多国际法律业务的专业部门，将业务触手延伸至全球，包括北美、南美、东南亚、欧洲、非洲等多个地区。
北京万商天 勤律师事务 所	万商天勤律师事务所是一家提供全面法律服务的综合型律师事务所，主要业务包括证券及资本市场、金融、项目融资、城市基础设施、建设工程及地产开发、环境保护、资源与能源、保险、国际业务、政府法律事务、诉讼与仲裁等。
北京信联数 安科技有限 公司	北京信联数安科技有限公司成立于 2009 年，是国家互联网应急中心（CNCERT）网络安全应急服务支撑单位。公司数据安全团队长期从事数据安全相关政策研究、咨询服务和数据安全治理项目。涵盖互联网、汽车、金融、医疗、制造等多行业多场景。目前，已协助十余家企业通过了最终的数据出境安全评估。
北京植德（深 圳）律师事 务所	植德前身为 2006 年设立的北京市昊凯律师事务所，秉持“公司制、一体化”的管理与运营，以及有方向、有质量的适度规模化，设有 9 家办公室的综合性律所，多个区域办公室已在筹建之中。2023 年 5 月，植德荣获《亚洲法律杂志》（ALB）中国法律大奖“年度最具潜力律所大奖”。
北京中企数 安咨询有限 公司	中企数安（北京）咨询有限公司，作为国内专业的管理咨询公司和业务外包服务提供商，专注于为客户提供各类商业管理和网络安全解决方案，为处于不同发展阶段的企业提供多元化的咨询。从市场准入、公司设立运营、网络安全监管等各个领域提供专业的指导，帮助客户准确了解中国市场的准入条件，熟悉合规要求。
大数据协同	大数据协同安全技术国家工程研究中心，是国家发改委唯一批复成立的国家

⁸ 按单位名称首字母排序

安全技术国家工程研究中心	级大数据安全工程研究中心，由北京奇虎科技有限公司承建。中心围绕大数据驱动安全和保障数据安全两个领域，培养和汇聚高端技术人才，积极承担国家和行业的重大科研项目，在威胁情报、态势感知、漏洞挖掘、数据安全治理等重点方向取得一大批关键技术成果。
福建旭丰律师事务所	福建旭丰律师事务所（以下简称“旭丰”）成立于2000年，福建省首批特殊合伙制律师事务所，是海西具有行业影响力的大型综合性律师事务所，也是福建省唯一一家荣膺中华全国律师协会、司法部评定的“全国优秀律师事务所”荣誉称号的“双国优”律师事务所。
广东广和律师事务所	广和律师事务所成立于1995年，是国内最早成立的合伙制律师事务所之一。广和所在华南地区创立了多个第一：第一家律师人数过百的律师事务所、第一家收入过亿的律师事务所、第一家获得省著名商标的律师事务所……现有执业律师千余名。
广东际唐律师事务所	广东际唐律师事务所是2009年成立的普通合伙制律师事务所。际唐崇尚“明法析理，厚德载道”的宗旨和“勤若牛、信若山、谦若水、势若雷”的精神。际唐服务领域已涵盖商事犯罪预防与辩护、重大民商事与仲裁、证券与资本市场、家族财富传承等商事法律服务全领域。
广东经天律师事务所	经天所成立于1985年1月，原名深圳特区经济贸易律师事务所，作为深圳经济特区成立初期规模最大的国办律师事务所、深圳经济特区最早从事证券法律业务的律师事务所、深圳经济特区最早一批转为合伙制的律师事务所之一。
广东卓建律师事务所	广东卓建律师事务所自2007年成立，大型综合制“全国优秀律师事务所”，深圳市数据要素发展协会常务理事单位，深圳市网络与信息安全行业协会理事单位，亚洲法律杂志ALB提名最具潜力律师事务所及最佳中国南部律师事务所，开放群岛开源社区“2022-2023年度优秀共建单位”。
贵州财经大学	贵州财经大学创办于1958年，是贵州省委、省政府重点建设的贵州省经济管理人才培养基地。在数据要素领域获批了贵州省高等学校数据要素流通安全创新团队、贵州省高等学校金融科技与区块链重点实验室、贵州省人文社科大数据产业创新重点实验室。
邓白氏中国	邓白氏（Dun & Bradstreet）是全球数据和分析驱动的决策赋能机构。致力于构建全球信任网络，协助客户将未知转化为信心、将风险转化为机遇、将潜力转化为增长。在商业信用、供应链管理、合规、销售与营销、普惠金融等

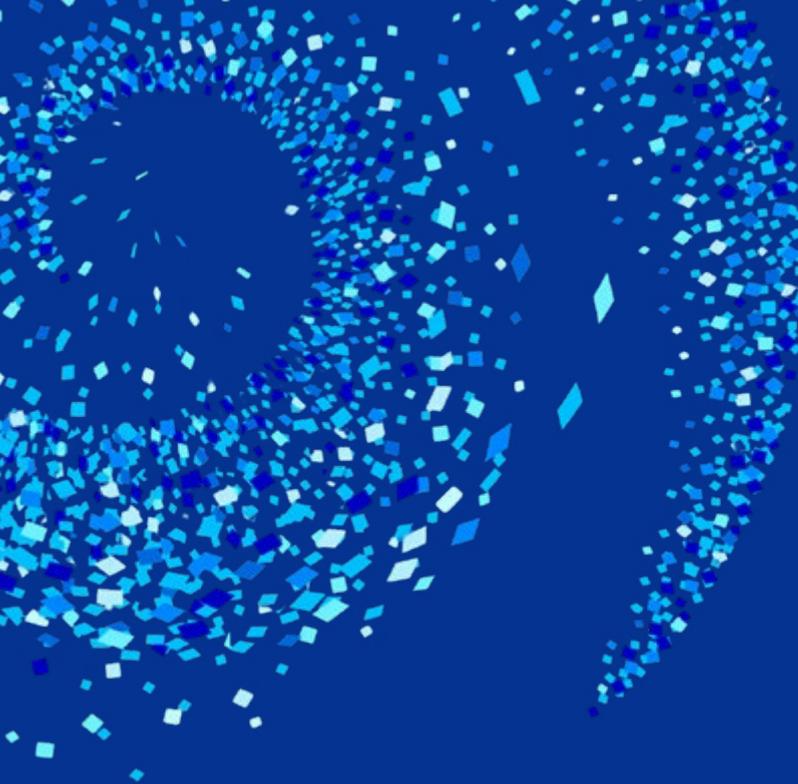
	多个应用场景中，帮助客户提高营收、降低成本、管控风险和实现数字化转型。
华东江苏大数据交易中心股份有限公司	华东江苏大数据交易中心，是在实施“国家大数据战略”大背景下，2015年成立的华东地区首个省级大数据交易中心。华东数交提出“以场景促应用，以服务促交易，以生态促创新”交易场所运营思路，建设国内首个“特色行业+区域性”的标杆数据交易场所。
江苏无锡大数据交易有限公司	江苏无锡大数据交易有限公司（简称“锡数交”）于2022年3月建成并正式运营，是无锡地区首家拥有国资背景的数据要素交易平台。锡数交打造集数据登记、数据交易和数据运营管理一体化的无锡数据交易服务平台，坚守准公益平台性质，提供合法合规的数据交易场所和设施，保障数据交易市场的正常运行。
联易融数字科技集团有限公司	联易融数字科技集团有限公司（Linklogis，简称“联易融”）2016年2月成立于深圳前海。2021年4月于港交所主板正式挂牌，成为首家上市的中国供应链金融科技 SaaS 企业。联易融响应国家普惠金融的号召，聚焦于 ABCD（人工智能、区块链、云计算、大数据）等先进技术在供应链生态的应用，以线上化、场景化、数据化的方式提供创新供应链金融科技解决方案。
领禹智通数据科技（上海）有限公司	领禹智通数据科技（上海）有限公司致力于打造数据要素流通“中国方案”，用智慧让数据便捷流通，做数据时代的大禹。聚焦数据共享流通领域，坚持“价值驱动、框架引领、产品支撑、方案落地”的发展理念，打造 1+M+N 模式的数据共享流通平台产品体系，提供数据流通安全、可信、便捷的解决方案。
南财合规科技研究员	南财合规科技研究院，隶属于南方财经全媒体集团，聚焦数据合规流通、人工智能治理、个人信息保护、反垄断与反不正当竞争、网络未成年人保护等数字经济前沿课题，通过新闻报道、行业调研、产品测评、论坛研讨等方式，深入剖析政策思路与行业发展，提供一体化合规监测、咨询与分析服务。
南昌大学	南昌大学是国家“双一流”建设高校、教育部与江西省部省合建高校、江西省一流大学整体建设高校。学校地处“英雄城”南昌市，拥有前湖、青山湖、东湖 3 个校区，其中前湖主校区占地面积 4264.54 亩，校舍建筑面积 150 万平方米。
南方科技大学深圳国家	深圳国家应用数学中心是全国首批十三个国家应用数学中心之一、深圳市第一个国家级数学中心。聚焦网络信息体系中的建模与计算、精准医疗应用中

应用数学中心	的建模与计算、科学工程计算与设计软件、数字经济-金融科技中的建模与计算等四个核心方向开展应用数学和数学应用研究。
南方科技大学智能管理与创新发展研究中心	南方科技大学智能管理与创新发展研究中心针对深圳发展亟需解决的重大理论与现实问题，聚焦数字经济、智能管理与社会治理创新发展、智能供应链管理三个重点研究方向，组织高水平理论研究的科研平台，通过学术交流与信息建设，与政府、企事业单位深度合作，打造具有影响力的“思想智库”。
奇安信	奇安信科技集团股份有限公司（以下简称奇安信）成立于2014年，专注于网络空间安全市场，向政府、企业用户提供新一代企业级网络安全产品和服务。奇安信集团是国内领先的基于大数据、人工智能和安全运营技术的网络安全产品及服务提供商，专注于向政府、企业用户提供新一代全面有效的网络安全解决方案。
勤达睿（中国）信息科技有限公司	Kyndryl 勤达睿是一家价值数十亿美元的跨国 IT 技术服务提供商，备受全球四千多家客户的信赖。在中国我们拥有 2600 位技术精湛的顶尖技术人才，4 个服务交付中心以支持 33 个城市的业务。我们思客户所想，利用 30 多年的行业经验，为客户的数字化转型目标时刻奋斗。
青岛国创智能家电研究院有限公司	青岛国创智能家电研究院有限公司是国家高端智能家电创新中心的运营公司，在数据安全领域，国创中心提供专业化咨询+系统化工具+定制化服务的整体解决方案，赋能企业提升数据安全治理、个人信息保护、数据出境安全、合规审计等方面的能力。
日本野村综合研究所	野村综合研究所是 1965 年成立的日本第一个成熟的民间综合智库。目前业务涵盖智库，咨询业务，金融和产业领域的解决方案，IT 基盘服务等。集团在北美、欧洲、亚洲和大洋洲均有分公司，遍及 16 个国家和地区，为客户的业务发展提供多方面支持。
三六零数字安全科技集团有限公司	360 数字安全集团（三六零数字安全科技集团有限公司）是数字安全的领导者，专注为国家、城市、大型企业、中小微企业提供数字安全服务。帮助城市、政府、企业数字安全体系的规划和建设数字安全体系，构建“摸清家底、感知风险、看见威胁、处置攻击、提升能力”5 大安全能力，形成应对数字安全复杂威胁的完整能力。
深圳赛西信息技术有限公司	深圳赛西信息技术有限公司（以下简称“公司”）是中国电子技术标准化研究院分支机构。公司依托赛西实验室、赛西认证、赛西培训、赛西信息服务

公司	等平台，在电子信息、新能源、先进制造等工业和信息化重点领域，面向政府提供标准研究、政策研究、行业管理和战略决策的专业支撑，面向市场和客户提供专业的标准制定、检验检测、计量校准、认证评估、培训咨询等服务。
深圳市电子商务安全证书管理有限公司	深圳 CA（全称：深圳市电子商务安全证书管理有限公司）是国内领先的综合性密码应用服务商，平安集团金融生态圈成员企业。深圳 CA 以密码为核心，依托国际领先的数字认证生态平台，融合人工智能、区块链、大数据等技术，为金融、政务、医疗、企业等多领域提供权威、可信的全方位网络安全服务。
深圳市星创数字研究中心	深圳市星创数字经济研究中心（以下简称“研究中心”）是在深圳市市场监督管理局主管下，由深圳赛西信息技术有限公司、深圳市卓越绩效管理促进会、深圳市电子信息产业联合会、深圳市标准技术研究院、深圳市标准化协会 5 家单位共同发起成立的民非组织，承接 IEEE 数字化转型联合会亚太秘书处。
深圳信息通信研究院	深圳信息通信研究院（中国信息通信研究院南方分院）是由工业和信息化部直属科研事业单位中国信息通信研究院与深圳市人民政府合作建设的深圳市市属事业单位。在大政策、大通信、大数字化、大安全等融合咨询业务领域，为政府、高等院校、企事业单位提供了信息通信领域政策咨询、技术培训等服务。
深圳职业技术大学	深圳职业技术大学是一所公办本科学校，其前身是 1993 年创建的深圳职业技术学院。2023 年 6 月，教育部批准以深圳职业技术学院为基础整合资源设立深圳职业技术大学。2019 年，学校入选教育部、财政部“双高计划”首批 10 所 A 档高水平学校建设单位。
数交数据经纪（深圳）有限公司	数交数据经纪（深圳）有限公司是全国首家以数据经纪为主营业务和登记名称的企业，该公司获得了全国首张由数据交易所颁发的数据经纪人登记凭证，并成为深圳市前海首批试点数据经纪人公司之一。该公司设计了全国首个数据经纪交易结构，是国内数据流通交易经纪方案的首个提出者和实践者。
四川久远银海软件股份有限公司	四川久远银海软件股份有限公司是国家鼓励的重点软件企业和高新技术企业，股票代码 002777。公司 30 余年来专注民生领域的信息化服务与创新，聚焦医疗医保、数字政务、智慧城市三大战略方向，面向政府和行业生态主体，利用大数据、人工智能、区块链、移动互联等技术实现科技赋能民生，为客户和社会创造价值。

腾讯科技（深圳）有限公司	腾讯公司担任粤港澳大湾区标准创新联盟工业互联网委员会秘书处单位，主任委员任职，正在联合粤港澳三地数百家技术开发与服务、产业应用与实践相关的政府、科研、企业、以及众多著名专家学者，共同开展大湾区三地适用的数据要素流通和安全等技术标准。
万商天勤（深圳）律师事务所	万商天勤律师事务所成立于1996年，秉承专业、务实、优质、高效的服务宗旨，追求法律法律服务国际化，多元化。拥有网络空间数字技术、数字资产交易与评估、数字安全等领域丰富的资源，为数字产业及数字化转型提供全产业链法律及合规、数字安全、数据资产评估咨询服务等。
厦门海峡链科技有限公司	厦门海峡链科技有限公司是一家致力于区块链底层技术研发的科技企业。核心产品“海峡链”由中国工合国际委员会、中国技术市场协会、国际科技合作委员会、数字中国研究院等权威机构共同发起打造而成。团队汇聚了阿里、腾讯、联想等知名企业的精英，在数据开放、数据安全、区块链底层研发拥有丰富的实战经验。
优刻得科技股份有限公司	UCloud 优刻得（股票代码：688158），坚持中立，不涉足客户业务领域，致力于打造安全、可信赖的云计算服务平台。UCloud 自主研发 IaaS、PaaS、大数据流通平台、AI 服务平台等一系列云计算产品，依托遍布全球的32个可用区，为全球上万家企业级客户提供云服务支持。
粤港澳大湾区大数据研究院	粤港澳大湾区大数据研究院是按照2018年11月国家信息中心与深圳市人民政府签署战略合作协议要求组建的民办非企业法人机构。研究院聚焦数据、算力、算法三大方向，强化央地协同、粤港澳协同、产学研协同和全要素协同四类机制，全力打造“前沿技术—政策研究—工程落地—产业孵化”四位一体的业务体系。
浙江九鑫智能科技有限公司	九鑫智能是一家数据智能服务商，业务围绕 AI 行业模型精准定位需求、流程自动化提高效率、ESG 能力实现可持续发展。服务3万+跨境店铺，产品运行5800万小时，客户GMV超300亿美元，致力于用数据算法支持中国企业国际竞争力。
中诚信征信有限公司	中诚信征信,成立于2005年，致力于以独立第三方数据信用服务商的身份，为数据要素市场提供一站式的数据信用和数据科技整体解决方案,帮助金融及大型机构进一步提高信用风险管理的质量及效率。是国内首家企业征信业务的持牌机构，也是国内首家个人征信业务持牌机构“百行征信”的发起股东之一。

<p>中国 电 信 股 份 有 限 公 司 研 究 院</p>	<p>中国电信股份有限公司研究院负责前瞻基础与决策研究、应用研究，开展关键核心技术研究验证、面向企业战略与技术方向的决策支持和应用创新等工作。其主要研发领域包括云网融合、5G/6G 网络与终端、MEC 边缘服务、大数据与 AI、网络与信息安全防护、基础运营技术研究以及企业战略与决策科学等。</p>
<p>中 国 政 法 大 学</p>	<p>中国政法大学是一所以法学学科为特色和优势，兼有政治学、经济学、管理学、文学、历史学、哲学、教育学、理学、工学等学科的“211 工程”重点建设大学，“‘985 工程’优势学科创新平台”“2011 计划”和“111 计划”（高校学科创新引智计划）重点建设高校，国家“双一流”建设高校。</p>



扫码关注官方公众号



扫码加入社区



联易融官方公众号



深圳数据交易所官方公众号

chenxi@linklogis.com



Open Islands