中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据出境负面清单管理办法（试行）

第一章 总 则

第一条 为保障国家数据安全，保护个人信息权益，复制推广中国（上海）自由贸易试验区及临港新片区数据出境管理成熟经验，进一步促进和规范数据依法有序出境，全面对接国际高标准经贸规则，打造国家制度型开放示范区，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》《促进和规范数据跨境流动规定》等法律法规和规章规定，以及商务部《上海市服务业扩大开放综合试点总体方案》《关于复制推广新一批服务业扩大开放综合试点示范经验的通知》等相关要求，制定本办法。

第二条 在上海市注册且在上海市开展数据出境活动的数据处理者，以及相关促进、保障、监管工作，适用本办法。根据《个人信息保护合规审计管理办法》，向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息，不适用于本办法。法律、行政法规或者国家网信部门、行业主管部门另有规定的，依照其规定执行。

第三条 坚持统筹发展和安全，建立负面清单和操作指引相结合的数

据安全合规出境模式，鼓励数据处理者依法依规开展数据出境业务，提升数据出境便利性。

第四条 按照包容审慎、创新容错、促进发展、保障权益的原则，推动上海市数据出境便利化。

第二章 工作机制与职责

第五条 在上海市数据安全工作协调机制的统筹协调下，上海市互联网信息办公室、上海市数据局及各市级行业主管监管部门依据《中华人民共和国数据安全法》及相关法律、法规和规定，按照相关重要数据识别标准，组织行业数据处理者开展数据分类分级，形成重要数据目录，并按程序向国家数据安全工作协调机制办公室备案。

行业主管部门已公开发布或已在行业内部发布本行业、本领域数据分类分级标准规范的，优先按照其规定识别重要数据。行业主管部门未明确判定标准的，按照《中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据分类分级参考规则》识别重要数据。

第六条 按照国家数据出境传输安全管理制度要求，聚焦“五个中心”建设，上海市互联网信息办公室、上海市数据局、上海市公安局负责统筹协调上海市数据出境负面清单相关事宜，建立负面清单数据安全风险评估

机制，定期开展成效评估与风险防控工作，并将评估结果作为优化清单管理的重要依据，同时联合各市级行业主管监管部门指导并监督数据出境活动。

上海市国家安全局依照有关法律、行政法规和本办法的规定，在职责范围内承担数据出境安全监督管理职责。

各区负责组织指导本区域内数据处理者使用负面清单开展数据出境活动，持续开展事前事中事后管理等。

上海自贸试验区管委会和临港新片区管委会在各自职责范围内，积极探索构建数据跨境管理新模式，推动数据跨境流动机制创新以及便利化举措落地，提升数据跨境服务中心服务效能。

第七条 上海市互联网信息办公室、上海市数据局会同各市级行业主管监管部门按照数据分类分级保护制度，主要负责上海市数据出境负面清单和操作指引的编制和更新、解决数据处理者开展数据出境活动存在的问题等工作事项，做好上海市数据出境信息共享，通报负面清单和操作指引实施情况及具体问题解决方案，做到信息互通。

第三章 负面清单实施与管理

第八条 数据出境负面清单经市委网络安全和信息化委员会批准后，由上海市互联网信息办公室、上海市数据局联合报国家互联网信息办公

室、国家数据局备案。

第九条 在上海市注册的数据处理者，属于已公布负面清单的行业、领域，向境外提供负面清单外的数据可以免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证。

第十条 如相关行业、领域已发布操作指引，有出境需求的数据处理者可按照操作指引开展数据出境活动。操作指引与负面清单不一致的地方，以负面清单为准。国家法律法规对数据出境另有规定的，依照其规定执行。

第十一条 数据处理者使用负面清单开展数据出境活动，遵循以下流程:

（一）提交备案申请。数据处理者按照负面清单配套实施指南要求，向所在区提交备案申请。

（二）开展合规出境。完成备案的数据处理者，应按照所在区要求开展数据出境活动。数据出境情况发生变化时，及时向所在区更新备案。

数据处理者向境外传输重要数据和个人信息，应当按照国家有关法律法规和配套政策标准，履行数据安全保护义务，采取技术措施和其他必要措施，增强数据安全保障能力，保障数据出境安全，并留存有关数据出境日志。发生数据出境安全事件或者发现数据出境安全风险的，应当采取补救措施，并及时向上海市互联网信息办公室、上海市数据局、上海市公安局、上海市国家安全局、所在区报告。

第十二条 各区应对外公开发布受理渠道，在收到数据处理者提交的备案材料后，提出出境数据是否适用负面清单的初审意见，报上海市互联网信息办公室、上海市数据局审核后，向数据处理者反馈备案审核结果。出境数据在负面清单内的，指导数据处理者申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证；出境数据在负面清单外的，告知数据处理者可依法有序自由流动；出境数据不适用负面清单的，按照现行法律法规执行。

鼓励各区设立数据跨境服务中心，开展数据出境负面清单适用咨询服务，帮助数据处理者高效便利安全开展数据出境活动。

第十三条 上海市互联网信息办公室、上海市数据局组织对区提出的初审意见及数据处理者提交的申请材料进行数据出境负面清单适用性和风险研判审核。对于情况复杂的，可联合相关行业主管监管部门进行审核。必要时，可召开专题会商会或专家论证会，形成审核意见。

第四章 监督管理

第十四条 上海市互联网信息办公室、上海市数据局、上海市公安局联合各市级行业主管监管部门会同相关职能部门通过定期检查和双随机抽查等方式，对负面清单的落实情况和数据处理者的数据出境活动进行监督检查。

第十五条 上海市互联网信息办公室、上海市数据局、上海市公安局联合各市级行业主管监管部门定期对上海市数据处理者落实本办法要求情况进行检查评估。发现数据处理活动存在较大安全风险的，应当立即采取补救措施，消除隐患，对影响或可能影响国家安全的出境数据，及时更新纳入负面清单。发现涉嫌违法犯罪线索的，应当及时通报上海市公安局、上海市国家安全局，上海市公安局、上海市国家安全局依照有关法律、行政法规，在各自职责范围内依法防范和打击危害数据出境安全的违法犯罪活动。

第十六条 各区应对负面清单的落实情况和本区域内数据出境情况进行跟踪监督，强化事前事中事后监管，提升数据出境安全风险发现和预警能力。

各区应当于每年年底前将本区内使用负面清单出境数据的数据处理者当年度数据出境总体情况向上海市互联网信息办公室、上海市数据局、上海市公安局报告，重要情况及时报告，相关情况汇总后报送上海市数据安全工作协调机制办公室，并向国家互联网信息办公室、国家数据局报告。

第十七条 数据处理者违反本办法和国家数据出境安全管理有关规定，存在违规出境数据行为的，由有关主管部门依照《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规依法追究其法律责任。

第十八条 参与数据出境负面清单管理的人员对在履行职责中知悉的

国家秘密、个人隐私、个人信息、商业秘密、保密商务信息等数据应当依法予以保密，不得泄露或者非法向他人提供、非法使用。违反者按照相关法律法规进行惩处。

第五章 附 则

第十九条 负面清单和操作指引未涉及的行业、领域的数据分类分级参考规则，按照有关规定和标准执行。

第二十条 负面清单和操作指引涉及的行业、领域中，如涉及《中华人民共和国出口管制法》规定的管制物项相关技术资料或《中华人民共和国对外贸易法》规定的技术出口管理事项等数据出境的，按照《中华人民共和国出口管制法》《中华人民共和国对外贸易法》等法律法规、规章规定执行。

负面清单和操作指引未涉及的行业、领域数据，按《网络数据安全管理条例》《数据出境安全评估办法》《个人信息出境标准合同办法》《个人信息出境认证办法》《促进和规范数据跨境流动规定》等相关法律法规、规章规定执行。

全国其他省市自由贸易试验区、自由贸易港、改革开放先行区、国家服务业扩大开放综合试点示范地区正式发布的数据出境负面清单，上海市可参照执行。

本办法中未明确规定的，若法律、行政法规或者国家互联网信息办公室、各行业主管监管部门等有关部门出台新的规定，从其规定。

第二十一条 本办法由上海市互联网信息办公室、上海市数据局负责解释。

本办法自发布之日起施行，原《中国（上海）自由贸易试验区及临港新片区数据出境负面清单管理办法（试行）》《中国（上海）自由贸易试验区及临港新片区数据出境管理清单（负面清单）（2024版）》同步废止。本办法施行前，数据处理者已依据《中国（上海）自由贸易试验区及临港新片区数据出境负面清单管理办法（试行）》开展数据出境活动的，继续有效。

中国（上海）自由贸易试验区及临港新片区、国家服务业扩大开放综合试点地区（上海）数据分类分级参考规则

重要数据统一识别参考规则:

1.本参考规则适用于非涉密数据，涉密数据按相关规定执行。

2.上海市企业掌握的1000万人以上个人信息（不含敏感个人信息）；100万人以上敏感个人信息；10万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的敏感个人信息。

3.被国家认定为关键信息基础设施的运营者掌握的10万人以上个人信息。

4.上海市企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据；涉及国家安全的企业供应链相关数据。

5.上海市企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。

一级类别	二级类别	数据基本信息描述	重要数据识别参考规则（示例）
（一）战略物资和大宗商品类	1.石油、石化和天然气	包括存储与交易数据、国际贸易数据等。	石油、石化、天然气领域可能推算出涉及国家重大战略的重要领域运行状况、发展态势、增长速度等的产品产量数据、国际贸易数据等。粮食、棉花、食用植物油、食糖、肉类、乳制品等大宗农产品战略储备数据以及未公开的国际合作数据、国际贸易数据，涉及农作物、畜禽、水产珍稀濒危种质资源（含基因）类别、数量等方面的可能影响生物安全的数据，未公开的农业农村统计数据、检验监测数据、防疫检疫数据，达到一定精度或者未公开的地理信息数据。
	2.农产品	包括种质资源数据、国际合作数据、国际贸易数据、战略储备数据等。	

（二）自然资源和环境类	3.地理信息	包括基础地理信息数据，可细分为定位基础数据、地名地址数据、地形地貌数据、基础地理实体数据，其他基础地理信息数据；遥感影像数据，可细分为原始影像数据、影像产品数据和其他遥感影像数据等；专题地理信息数据，可细分为自然资源、生态环境等领域的专题地理信息。	达到国家规定的覆盖度、精度和尺度等，或表现敏感区域和目标的基础地理信息数据和遥感影像数据。服务军事、国防科研、高科技领域的各类气象监测数据。不宜公开发布或具有军事价值的海洋生态环境监测数据、灾害防御数据等。能够反映水旱灾情、工程险情等水旱灾害防御业务数据，险工险段等水利基础数据，不宜公开的国家水资源、水环境基础数据、水情信息、水文观测数据等，满足一定精度要求的遥感影像、数字孪生水利数据等，重点水利工程物理安全保护情况等。
	4.气象	包括气象监测数据、空间大气监测数据、气象保障数据、区域气象数据、雷达基数据、气象台站元数据等。	
	5.海洋	包括海洋生态环境数据、海洋资源数据。	
	6.环保	包括反映污染物排放水平的自行监测、接受行政处罚或其他污染物排放等数据。	
	7.水利	包括江河湖泊、水利工程、监测站等水利基础数据，水旱灾害防御、水资源、水文、水环境、节约用水、移民等水利业务数据，数字孪生水利数据等。	
（三）工业类	8.钢铁、有色金属	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	具有重要军用、民用价值的有色金属储量、产量、采购量等数据，国家钢铁、有色金属战略储备数据或战略性有色金属矿床的重要地质数据，富含重要伴生矿资源的矿区数据。我国独特掌握的稀土开采、冶炼等生产技术数据。大宗原材料信息，以及能够左右原材料采购定价权的数据。
	9.稀土	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	
	10.其他矿产	包括储量数据、国际合作数据、国际贸易谈判数据、与矿产有关的产业发展布局情况。	

	11.化学工业	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	上海市企业掌握的重点危险化学品检测监控、关键工艺、设备运行、产量储量等数据。民用核设施领域科研试验数据，运行监控数据等。电子信息行业先进技术、集成电路先进设计和制造技术、重大计算装备设计数据、算法和软硬件架构以及重要电子元器件设备国产化率等信息。
	12.电力	包括发电厂生产数据、输配电数据、建设运维数据。	
	13.电子信息	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	
	14.民用核设施	包括民用核设施科研中的试验或测试数据，核设施相关设计和制造工艺信息，核设施运行监控数据。	
	15.工业装备	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	关系我国科技实力、影响我国国际竞争力的汽车关键零部件研发和生产数据，如车身稳定控制系统、主动减震器系统相关研发数据。用于研发生产的智能网联汽车自动驾驶模型训练数据。车辆及路侧设备联网运行过程中，收集和产生达到一定精度、一定规模、覆盖特定区域的时空数据。规上工业企业使用的工业互联网或工业控制系统安全运行保障数据。
	16.智能网联汽车	参照《工业领域重要数据识别指南》（YD/T4981-2024）《汽车数据出境安全指引》（2026版）识别。	
	17.其他	参照《工业领域重要数据识别指南》（YD/T4981-2024）识别。	
（四）国防科技工业类	18.国防科技工业类	包括经营管理、研发设计、生产制造、试验验证、维修保障等数据。	与国家军事、经济、科技、网络安全相关的数据，综合反映国防科技工业重要企事业单位科研与生产能力的数据，汇总后能反映国防科技工业整体情况的数据，国防科技工业领域相关特色重要数据。
（五）电信类	19.电信	参照《电信领域重要数据识别指南》（YD/T3867-2024）识别。	重要网络设施和信息系统建设规划数据、性能参数数据、监测分析数据、运行维护数据、统计分析数据等。
（六）广播电视和	20.广播电视	包括广播电视节目采集拍摄、制作播出、传输覆盖、分发服务、监测监管等环节处理的数据。	未公开的视听创作内容，被滥用可能导致意识形态安全、公共安全的视听内容，省级及以上广电机构传输覆盖数据

网络视听类	21.网络视听	包括网络视听节目采集拍摄、制作播出、分发服务、监测监管等环节处理的数据。	，广电视听监测监管数据，以及广播电视行业关键信息基础设施、重要网络和信息系统规划建设数据、运行维护数据、关键资源、安全保障数据等。
（七）金融类	22.银行	包括银行客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。	银行、保险、证券期货、融资租赁、支付清算领域的机构安保信息，以及其处理的重要企事业单位业务数据，包括国防军工企业、关系国家安全企业的相关信息。
	23.保险	包括保险机构客户数据、业务数据、经营管理数据、系统运行和安全管理数据等。	
	24.证券期货	包括投资者类数据、技术类数据、业务类数据等。	
	25.融资租赁	包括客户数据、企业交易数据、经营管理数据等。	
（八）交通运输类	26.交通	包括铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空、邮政管理、综合管理等数据。	铁路交通、公路交通、道路运输、城市交通、水路交通、民用航空、邮政管理等领域影响生产安全、供应链安全的数据、施工建设过程中获取的自然资源类数据、未公开的线路图、关键站点等数据，以及被泄露、篡改可能造成重大交通事故的数据。
（九）卫生健康和食品药品类	27.遗传资源	包括自然人基因数据、人类遗传资源信息等与种族、群体健康相关的数据。	反映种族整体情况或关系生物安全的遗传资源数据，关系国家安全、生命安全、人类自身安全的食品、药品、生物安全和疾控数据。特定领域、特定群体、特定区域或达到一定精度和规模的涉及人民群众生命健康和安全的医疗领域诊疗数据。
	28.健康医疗	包括医疗服务、电子病历、电子健康档案、医学研究等各类数据，健康数据、医疗救援保障数据、特定药品实验数据等，或对患者健康医疗数据的开发利用结果。	
	29.食品	包括食品安全溯源标识数据，食品生产中自动控制系统的参数和控制类数据。	

	30.药品	包括药品供应、药品审批过程中提交的实验数据，以及与药品生产流程、生产设施有关的试验数据。	
	31.生物安全	包括病毒研究或生物实验室相关数据。	
	32.疾控数据	包括突发公共卫生事件及与传染病相关的疫情、治疗、疫苗、死因等数据。	
（十）公共安全类	33.物理安全	包括建筑基础数据、安保装备数据等。	一旦遭到非法利用，可能给社会稳定造成严重危害的重要目标基础数据、安保装备数据、敏感场所安保部署数据；关键信息基础设施或重要网络规划、安全运行数据。
	34.网络安全	包括自贸试验区企业信息系统设计运行数据、网络设施拓扑架构数据、安全保障数据等。	
（十一）互联网服务和电子商务类	35.互联网平台服务	包括提供互联网服务过程中产生的各类数据。	在提供互联网服务过程中产生的可用来实施社会动员的数据，相关退伍人员等敏感人群数字画像数据，对军工、政府类客户记录和跟踪的数据。可能影响国家安全和社会公共利益的人工智能训练数据、算法源代码、关键组件数据、控制程序等数据。
	36.人工智能服务	包括人工智能训练数据、算法源代码、关键组件数据、控制程序等数据。	
（十二）科学技术类	37.知识产权和重大发现	包括涉及国防、国家安全或其他非公开的知识产权，其他能显著提升国家安全能力或直接影响国家安全的科研论文、观测数据、产业化成果等。	涉及国防、国家安全的知识产权数据。

（十二）科学技术类	37.知识产权和重大发现	包括涉及国防、国家安全或其他非公开的知识产权，其他能显著提升国家安全能力或直接影响国家安全的科研论文、观测数据、产业化成果等。	涉及国防、国家安全的知识产权数据。被列入《中国禁止出口限制出口技术目录》所列技术有关的数据。
	38.禁止出口限制出口技术	包括《中国禁止出口限制出口技术目录》所列技术有关的数据。	
（十三）其他数据类	39.属于出口管制法管制的相关数据	包括列入国家出口管制清单的相关物项数据。	与国家安全和利益、履行防扩散等国际义务相关属于出口管制法管制的数据。其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、低空、生物等安全，符合重要数据定义的数据。
	40.其他可能影响国家政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益、太空、极地、深海、低空、生物等安全的数据。		