

# 中国（北京）自由贸易试验区数据出境 负面清单管理办法（试行）

## 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，提升中国（北京）自由贸易试验区（以下简称北京自贸试验区）数据出境管理能力及便利化程度，促进数据高效便利安全跨境流动，根据《数据安全法》关于数据分类分级保护制度规定、国家互联网信息办公室《促进和规范数据跨境流动规定》、北京市《中国（北京）自由贸易试验区条例》等要求，制定本办法。

第二条 北京自贸试验区内开展数据出境负面清单制定审批和使用管理等活动，适用本办法。

第三条 负面清单管理应坚持以下原则：

（一）坚持安全底线。负面清单管理应当遵守法律法规有关规定，建立健全安全管理机制和技术保障能力，在保障数据安全的前提下，推动数据依法有序流动。

（二）助力产业发展。充分考虑数据处理者数据出境实际需求，科学合理制定须纳入负面清单的数据范围，最大程度便利数据出境活动，促进跨境业务发展。

(三)分批分类管理。负面清单按照行业、领域分批次制定。负面清单中的数据项应采取分类管理，按照敏感程度可分为适用数据出境安全评估的数据、适用个人信息出境标准合同备案或个人信息保护认证的数据。

## 第二章 职责及分工

第四条 按照国家数据跨境传输安全管理制度要求，北京市互联网信息办公室、北京市商务局、北京市政务服务和数据管理局统称市级管理部门，负责建立北京自贸试验区数据出境负面清单管理体系并统筹协调相关事宜，指导并监督北京自贸试验区数据跨境流动活动，分行业、分领域、分批次组织开展负面清单制定工作，履行报审及备案流程，建立负面清单动态管理机制等。

第五条 本市朝阳、海淀、昌平、通州、顺义、大兴、亦庄北京自贸试验区组团的管理部门及属地相关职能部门统称各自贸组团，负责组织指导本组团内数据处理者合规使用负面清单，制定出台负面清单配套实施指南、明确负面清单使用对象及申报流程、指导数据处理者开展使用申请和备案工作、加强数据出境活动的跟踪监督、形成事中存证与事后监管能力等。

第六条 本办法所称数据处理者，是指北京自贸试验区内登记注册、开展数据跨境流动等相关活动的企业、事业单位、机构、团体或其他组织。

数据处理者应当按照相关规定识别、申报重要数据。按照各自贸组团相关要求开展数据出境活动，并配合市级管理部门、各自贸组团开展跟踪核验和监督检查等工作。

### 第三章 负面清单制定及管理

第七条 负面清单制定主要包括以下工作流程：

（一）需求调研。聚焦北京自贸试验区产业发展和数据处理者实际需求，遴选重点行业、领域组织开展调研，从业务场景、类别、量级、字段等方面摸排掌握出境数据情况，作为负面清单制定依据。

（二）重要数据识别。在本市数据安全工作协调机制的统筹协调下，市级管理部门依据《数据安全法》及相关法律、法规和规定，明确重要数据识别标准，对数据进行分类分级，形成北京自贸试验区重要数据目录，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（北京）自由贸易试验区数据分类分级参考规则》识别重要数据。

（三）业务场景分析。结合调研结果及重要数据识别结果，选取数据出境需求迫切、流动频繁的业务场景，对数据出境的规模、范围和频率进行分析，为风险可控的数据出境业务场景合理设置数据项及数据量级。

（四）论证与征求意见。邀请行业、法律、数据安全等领域专家开展评审论证，并征求市级行业主管部门、有关职能部门意见，进一步修订完善。

（五）履行审批报备流程。负面清单应经北京市数据安全工作协调机制审核通过后，报市委网络安全和信息化委员会批准，由北京市互联网信息办公室、北京市政务服务和数据管理局联合报国家网信部门、国家数据管理部门备案。

第八条 负面清单应至少包含以下两方面：

（一）需要通过数据出境安全评估的数据清单，主要包括：

1. 关键信息基础设施运营者向境外提供个人信息或者重要数据；

2. 关键信息基础设施运营者以外的数据处理者向境外提供重要数据，或者向境外提供达到负面清单要求申报数据出境安全评估的个人信息。

（二）需要通过个人信息出境标准合同备案、个人信息保护认证出境的数据清单，主要包括：

关键信息基础设施运营者以外的数据处理者向境外提供达到负面清单要求订立个人信息出境标准合同或者通过个人信息保护认证的个人信息。

第九条 负面清单实行动态管理。市级管理部门对于已出台的负面清单，跟踪评估实施情况和安全风险，统筹开展负面清单修订工作。对于尚未出台负面清单的行业、领域，及时研判数据

出境实际需求，研究制定相应行业、领域负面清单，不断完善北京自贸试验区数据跨境流动管理政策体系。

## 第四章 负面清单实施

第十条 数据处理者使用负面清单出境数据，遵循以下主要流程：

（一）提交申请。数据处理者按照所在自贸组团负面清单配套实施指南要求，向相应的自贸组团提交申请，申请材料包括注册所在地、所属行业、经营情况、近2年在业务经营活动中受到行政处罚和有关主管监管部门调查及整改情况等。

（二）提交备案。通过审核的数据处理者应按照配套实施指南开展负面清单使用备案。备案材料包括数据出境业务场景、出境数据目录、出境数据规模、境外接收方、出境数据适用负面清单的理由及适用负面清单中的数据子类等。

（三）合规出境。完成备案的数据处理者，可按照各自自贸组团出具的研判意见开展数据出境活动，配合市级管理部门、各自自贸组团开展监督、核验等工作。数据出境情况发生变化时，及时向各自自贸组团更新备案。

第十一条 各自自贸组团重点开展以下工作：

（一）各自自贸组团依据配套实施指南对数据处理者提交的申请材料进行审核，审核结果应在5个工作日内书面告知数据处理者，并协助通过审核的数据处理者开展负面清单使用备案。

(二) 各自贸组团应在数据处理者提交备案材料后，于5个工作日内提出出境数据是否适用负面清单的初步意见，报北京自贸试验区管理机构确认后，向数据处理者反馈。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，明确告知数据处理者可按照负面清单配套实施指南要求安全有序自由流动；出境数据不适用负面清单的，按照现行法律法规执行。

(三) 各自贸组团应与使用负面清单的数据处理者建立对接服务机制，动态搜集掌握数据处理者数据出境诉求，听取对负面清单使用的意见建议，结合数据跨境流动总体态势情况，不断优化和改进本区域内数据出境便利化服务举措。

## 第五章 监督管理

第十二条 市级管理部门应严格落实国家及行业数据安全管理工作要求，加强对北京自贸试验区数据出境活动的指导监督，建立数据出境活动风险研判、安全事件发现通报机制，统筹开展安全风险监测预警能力建设，强化负面清单使用过程中事前事中事后全链条全领域综合监管。

第十三条 数据处理者在数据出境活动中，应及时备案，各自贸组团应组织专业技术机构就数据实际出境情况与备案材料进行一致性抽验，对于数据处理者在数据出境活动中未严格履行相

关承诺，或出现瞒报、虚报、故意造成实际出境数据与备案数据不一致等违规行为的，各自贸组团可责令其暂停数据出境活动，要求限期整改，整改完成后重新履行负面清单申请、备案程序；情节严重的，终止其数据出境活动，对其采取重点监管措施，并及时向市级管理部门上报有关情况。

**第十四条** 市级管理部门联合行业主管部门定期对各自贸组团、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。

**第十五条** 数据处理者违反有关法律法规，拒不改正或者造成严重后果的，依法追究其法律责任。

## 第六章 附 则

**第十六条** 关系国家安全、国民经济命脉、重要民生、重大公共利益等数据属于国家核心数据，实行更加严格的管理制度，不纳入负面清单管理。

**第十七条** 本办法由北京市互联网信息办公室会同北京市商务局、北京市政务服务和数据管理局负责解释。

**第十八条** 本办法未涉及的行业、领域的数据分类分级参考规则，按照有关规定和标准执行。

**第十九条** 出境数据属负面清单外的行业、领域，按《数据出境安全评估办法》《个人信息出境标准合同办法》《促进和规范数据跨境流动规定》等国家相关规定执行。

第二十条 本办法自发布之日起施行。

附件：中国（北京）自由贸易试验区数据分类分级参考规则

## 附件

# 中国（北京）自由贸易试验区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.北京自贸试验区企业掌握的 1000 万人以上个人信息（不含敏感个人信息）；100 万人以上敏感个人信息；10 万人以上且包含个人银行账户、个人保险账户、个人注册账户、个人诊疗数据等的个人敏感信息。
- 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.北京自贸试验区企业在研发设计过程、生产制造过程、经营管理过程中收集和产生的与行业竞争力、行业生产安全相关的高价值敏感数据；涉及国家安全的企业供应链相关数据。
- 5.北京自贸试验区企业掌握的关系国计民生领域的自动控制系统参数以及控制、运行维护、测试数据。

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、国土空间规划、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。不宜公开发布的具有军事价值的海洋环境监测数据、灾害防御数据等。能够反映水旱灾情、工程险情、综合分析评价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、数字孪生水利地理空间数据等，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、河湖保护、节约用水、移民等水利业务数据，数字孪生水利地理空间数据等。	
(三)工业类	8. 钢铁、有色金属	包括储量、产量、冶炼装备、采购量等数据，国际合作数据、国际贸易数据等。	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	包括储量与开采数据、行业使用数据、出口数据等。	
	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	包括生产作业场所和运输信息、生产销售信息、制作方法信息，民用爆炸物品行业相关数据信息。	
	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	包括基础电子信息产品（关键芯片、操作系统、大型软件等）参数，源代码、集成电路布图等数据，产品测试数据，产品面向国防军工、政务等领域销售和服务情况。	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。
	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	包括工业装备研发、应用、生产、销售、运维、管理数据。	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。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	汽车关键零部件研发和生产数据，用于研发生产的智能网联汽车自动驾驶模型训练数据。	
	17. 其他	包括工业互联网的网络、平台、安全保障相关数据，工业控制系统的参数、控制、运行维护、测试数据。	
(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	包括网络规划运维数据、安全保障数据、经济运行与业务发展数据、关键技术成果数据等。	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) 广播电视和网络视听类	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，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。
	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。	
(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	银行、保险、证券期货及融资租赁领域的机构安保信息，

		统运行和安全管理数据等。	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的控制类数据、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. 服务外包	包括境外客户委托境内企业提供服务过程中收集、产生的数据或与重要服务客户有关的数据。开展数字贸易、跨境电商业务中收集、产生的数据或与重要服务客户有关的数据。	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. 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。	
	37. 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	38. 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》有关数据。
	39. 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	40. 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、生物等安全,符合重要数据定义的数据。
	41. 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、生物等安全的数据。		