附件

绍兴市公共数据授权运营管理实施细则（试行）（征求意见稿）

为规范绍兴市公共数据授权运营管理，促进公共数据有序开发利用，加快培育数据要素市场，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》《浙江省公共数据条例》《浙江省公共数据授权运营管理办法》（试行）等有关法律法规，结合本市实际，制定本细则。

一、总则

（一）总体要求

公共数据授权运营坚持中国共产党的领导，遵循依法合规、安全可控、统筹规划、稳慎有序的原则，按照“原始数据不出域、数据可用不可见”的要求，在保护个人信息、商业秘密、保密商务信息和确保公共安全的前提下，向社会提供数据产品和服务。优先支持与民生紧密相关、行业发展潜力显著和产业战略意义重大的领域开展公共数据授权运营。禁止开放的公共数据不得授权运营。

（二）适用范围

本市行政区域内公共数据授权运营相关的授权、加工、经营、安全监管等数据活动，适用本细则。

（三）术语定义

本细则中下列术语的定义：

公共数据授权运营（以下简称授权运营），是指县级以上人民政府按程序依法授权法人或者非法人组织（以下简称授权运营单位），对授权的公共数据进行加工处理，开发形成数据产品和服务，并向社会提供的行为。

授权运营协议，是指县级以上政府与授权运营单位就公共数据授权运营达成的书面协议，明确双方权利义务、授权运营范围、运营期限、合理收益的测算方法、数据安全要求、期限届满后资产处置、退出机制和违约责任等。

授权运营域，是指由公共数据主管部门依托一体化智能化公共数据平台（以下简称公共数据平台）组织建设和运维的，为授权运营单位提供加工处理授权运营公共数据服务的特定安全域，具备安全脱敏、访问控制、算法建模、监管溯源、接口生成、封存销毁等功能。

数据产品和服务，是指利用公共数据加工形成的数据包、数据模型、数据接口、数据服务、数据报告、业务服务等。

二、职责分工

（一）协调机制

建立绍兴市市级公共数据授权运营管理工作协调机制（以下简称协调机制），具体由市公共数据、网信、发展改革、经信、公安 、国家安全、司法行政、财政、市场监管等市级单位组成。协调机制的主要职责：负责统筹推进本市行政区域内授权运营管理工作；建立健全授权运营相关制度规范和工作机制；审议给予授权、终止或撤销授权等重大事项；授权运营的安全监管

和监督评价；组建市公共数据授权运营专家组；统筹协调解决授权运营工作中遇到的重大问题。

区、县（市）政府建立本级协调机制，负责本行政区域内授权运营工作的统筹管理、安全监管、监督评价，审议给予、终止或撤销本级授权运营等重大事项，根据需要组建县级专家组，统筹协调解决本级授权运营工作中的重大问题。

（二）职责分工

市、县两级相关部门在各自职责范围内积极配合协调小组的公共数据授权运营指导与监督工作。

公共数据主管部门负责落实协调机制确定的工作任务，承担协调机制日常工作，研究提出推进授权运营的政策建议，指导开展授权运营工作。本级政府设置公共数据授权运营合同专用章，由公共数据主管部门管理使用。

公共管理和服务机构做好本领域公共数据的编目、归集、治理、申请审核和安全监管等授权运营相关工作。未经本级政府批准，不得与任何第三方签订公共数据运营协议，不得以合作开发、委托开发等方式交由第三方承建相关信息系统而使其直接获取数据运营权。

发展改革、经信、财政、市场监管等单位按照各自职责，做好数据产品和服务流通交易的监督管理工作。完善数据产品和服务的市场化运营管理制度。对违反反垄断、反不正当竞争、消费者权益保护等法律法规规定的，由有关单位按照职责依法处置，相关不良信息依法记入其信用档案。

市场监管会同发展改革、经信、司法行政等单位建立数据

知识产权保护制度，推进数据知识产权保护和运用。

网信、密码管理、保密行政管理、公安、国家安全等单位按照各自职责，做好授权运营的安全监管工作。

专家组负责提供授权运营相关业务和技术咨询。协调机制有关单位可委托专家对授权运营申请单位进行综合评审，辅助决策。

三、授权申请程序

（一）发布公告

公共数据主管部门发布重点领域开展授权运营的公告，明确申报条件。公告内容包括申请条件、授权运营具体工作要求，所需提交材料、申请方式、申请时间等。

授权运营单位应当在公告规定的时间内提交申请，申请时应当提交下列材料：

1.授权运营申请表（见附件 1）；

2.最近一年的第三方审计报告和财务会计报告；

3.数据安全承诺书；

4.安全风险自评报告；

5.授权运营单位资格证明佐证材料；

6.公共数据主管部门要求提供的其他材料。

对于曾经签订授权运营协议的单位，还应提交历年的公共数据授权年度运营报告、评估报告等材料。

（二）资格审查

公共数据主管部门对授权运营单位提交的资料进行初步审

查，提交材料不齐全或者不符合形式要求的申请单位应当在规定时间内补交相关材料。初审通过后，协调机制有关单位组织召开专家论证会，专家组对授权运营单位的资质实力、安全条件、信用条件等进行综合评审，出具论证评审意见。资格条件审查内容包括：

1.基本条件审查：经营状况良好，具备授权运营领域所需的专业资质、知识人才积累和生产服务能力；企业及其法定代表人无重大违法记录。企业及其法定代表人未被列入失信被执行人名单、重大税收违法案件当事人名单、严重失信名单。

2.技术安全条件审查：落实数据安全负责人和管理部门，建立授权运营内部管理和安全保障制度；具有符合网络安全等级保护三级标准和商用密码安全性评估的系统开发和运维实践经验；具备成熟的数据管理能力和数据安全保障能力；近3年未发生网络安全或数据安全事件。

3.应用场景审查：应用场景明确，具有重大经济价值或社会价值，并设置数据安全保障措施；应用场景具有较强的可实施性，在授权运营期限内有明确的目标和计划，能够取得显著成效；按照应用场景申请使用公共数据，坚持最小必要的原则。

4.重点领域具体安全要求审查：由公共数据主管部门会同相关领域主管部门研究确定。

（三）授权备案

市、县两级协调机制有关单位综合专家组评审结果，将拟授权运营单位名单上报本级人民政府。区、县（市）政府坚持

总量控制、因地制宜、公平竞争的原则，结合具体应用场景确定授权运营领域与授权运营单位，报市政府审核备案。备案材料包括：备案文件、授权运营协议、专家论证意见、本级协调机制审议记录等。

（四）社会公开

协调机制有关单位负责向社会公开授权运营单位名单等信息，公示期为7天，期间若有异议，需对异议在五个工作日内进行答复和处理。

（五）签订协议

由市、县（市、区）人民政府委托公共数据主管部门，与公示通过的授权运营单位签订授权运营协议，协议中应明确授权运营范围、授权运营期限、授权方式等。若涉及公共数据有偿使用的，还应明确收益方式、违约责任等，其他细节事项由授权运营单位与公共数据主管部门双方商议决定后在协议中体现（详见附件2）。

（六）期满重新申请

授权运营期限由授权运营单位和公共数据主管部门协商确定，一般不超过3年。在期限届满6个月前，需要继续开展授权运营的，授权运营单位应按程序重新申请公共数据授权运营。

四、运营实施

（一）建立平台

市级公共数据主管部门应当依托本级公共数据平台建设授权运营域，为授权运营活动提供支撑平台，区、县（市）应当

依托市级授权运营域开展授权运营工作。授权运营域的建设需按照省公共数据主管部门制定的建设标准进行，并提交省公共数据主管部门验收。

授权运营域应满足以下条件：遵循已有的公共数据平台标准规范体系，复用统一用户认证组件、用户授权服务等公共数据平台能力；实现网络隔离、租户隔离、开发与生产环境隔离，具备数据脱敏处理、数据产品和服务出域审核等功能，确保全流程操作可追踪，数据可溯源；满足政府监管需求，支持集成外部数据，具备分布式隐私计算能力；满足授权运营单位的基本数据加工需求。

（二）运营要求

授权运营单位应当依法合规开展公共数据运营，在实施过程中应遵循下列要求：

1.不得泄露、窃取、篡改、毁损、丢失、不当利用公共数据，不得将授权运营的公共数据提供给第三方；

2.相关管理人员、技术人员应当通过省公共数据主管部门组织的授权运营岗前培训；

3.定期报告运营情况，接受公共数据主管部门对授权运营涉及的业务和信息系统、数据使用情况、安全保障能力等方面的监督检查；

4.严格执行数据产品和服务定价、合理收益有关规定。完善公共数据安全制度，建立健全高效的技术防护和运行管理体系，确保公共数据安全，切实保护个人信息；

5.应当承担授权运营成本，以及授权运营域加工其所用数据产生的损耗和成本。

（三）数据申请

授权运营单位通过一体化数字资源系统提交公共数据需求清单，经公共数据主管部门会同数源单位审核通过后获取。申请省回流市、县（市、区）数据的，应经省公共数据主管部门同意后获取。涉及个人信息、商业秘密、保密商务信息的公共数据，应当经脱敏、脱密处理后，或经相关数据所指向的特定自然人、法人或者非法人组织依法授权同意后获取。相关数据不得以“一揽子授权”、强制同意等方式获取。

（四）数据加工

获取公共数据后，授权运营单位应当在授权运营域内对公共数据进行加工处理，形成数据产品和服务。公共数据加工处理应符合下列要求：

1.授权运营单位所有参与数据加工处理的人员须经实名认证、备案与审查，签订保密协议，操作行为应做到有记录、可审查。保密协议应明确保密期限和违约责任。

2.原始数据对数据加工人员不可见。授权运营单位使用经抽样、脱敏后公共数据进行数据产品和服务的模型训练与验证；

3.经本级公共数据主管部门审核批准后，授权运营单位可以将依法合规获取的社会数据导入授权运营域，与授权运营的公共数据进行融合计算。

授权运营单位在数据加工处理或提供服务过程中发现公共

数据质量问题的，可向本级公共数据主管部门提出数据治理需求。需求合理的，公共数据主管部门应督促数据提供单位在规定期限内完成数据治理。

授权运营单位在开展公共数据运营过程中，因数据汇聚、关联分析等原因发现数据间隐含关系与规律，并危害国家安全、公共利益，或侵犯个人信息、商业秘密、保密商务信息的，应立即停止相应的数据处理活动，及时向公共数据主管部门报告数据风险情况。

（五）数据导出

授权运营单位加工形成的数据产品和服务在导出授权运营域前，应向本级公共数据主管部门提交导出申请，审核通过后方可导出。原始数据包不得导出授权运营域。通过可逆模型或算法还原出原始数据包的数据产品和服务，不得导出授权运营域。

经公共数据主管部门审核批准后导出授权运营域的数据产品和服务，不得用于或变相用于未经审批的应用场景，不得以直接或者间接方式将数据产品和服务交由第三方使用。

数据产品和服务应按照国家和省、市有关数据要素市场规则流通交易。

（六）授权收益

推动用于公共治理、公益事业的公共数据采用有条件无偿使用方式进行授权；探索用于产业发展、行业发展的公共数据可在价值评估的基础上探索采用有条件有偿使用方式进行授权，并在授权运营协议中予以约定。

授权运营单位应当遵循依法合规、普惠公平、收益合理的原则，严格执行公共数据产品定价和合理收益有关规定，对加工形成的公共数据产品和服务确定价格，并依据授权协议在公共数据授权运营参与方之间进行合理的利益分配。鼓励多方合作开展数据产品和服务市场化运营，探索成本分摊、利润分成、股权参股、知识产权共享等多元化利益分配机制。

（七）运营报告

授权运营单位在运营期限内，应当向本级公共数据主管部门提交公共数据授权运营年度运营报告，报告内容包括：本单位与授权运营相关的数据产品和服务存储、加工处理、分析利用、安全管理及市场运营情况等。

（八）运营评估

公共数据主管部门会同有关单位或委托第三方机构，对本级授权运营单位开展授权运营情况年度评估，对授权运营单位实行动态管理，评估结果作为再次申请授权运营的重要依据。

评估结果分为通过、未通过和限期整改。通过评估的授权运营单位，可继续承担公共数据授权运营工作。限期整改的授权运营单位应当制定整改方案，30 日内整改完成，报本级公共数据主管部门再次评估。未通过或限期整改后仍未通过的，由公共数据主管部门向人民政府反馈评估结果，终止其授权运营工作，并重新发布信息，审核符合条件的授权运营单位承担此授权运营工作。

五、授权终止

（一）终止情形

授权运营终止分为授权运营单位主动退出和被动退出两种情形。主动退出包括授权运营协议期满退出和提前终止协议。确需提前终止协议的授权运营单位，应提前6个月向市公共数据主管部门提出主动退出申请，提交授权运营提前终止申请书，并做好退出工作和数据处置工作。

授权运营单位有以下情形之一的，公共数据主管部门应当按照协议约定责令其改正，并暂时关闭其授权运营域使用权限；授权运营单位应当在规定期限内完成整改，并反馈改正情况；未按照要求改正或情节严重的，公共数据主管部门有权终止其相关公共数据的授权，运营协议自动失效。

1.未履行公共数据安全管理义务的；

2.违规使用公共数据并造成损失的；

3.授权运营活动存在较大安全风险的；

4.违反规定利用公共数据或擅自更改应用场景的；

5.对于授权运营评估结果为限期整改，拒不整改或整改未通过的；

6.违反本细则规定及其相关法律法规的其他行为。

（二）退出审查

授权运营协议终止或撤销的，本级公共数据主管部门应当及时撤销授权运营单位的授权运营域使用权限，及时删除授权运营域内留存的相关数据，并按照规定留存相关网络日志不少于6个月。

协调机制有关单位应对授权运营单位的退出条件进行审查，

防止出现授权运营工作不合规、数据安全漏洞、数据泄露等安全隐患，若审查结果不通过，授权运营单位有义务完成整改工作。

六、安全监管

（一）安全原则

公共数据授权运营坚持统筹发展和安全的原则，按照“公共数据分类分级”要求，加强公共数据全生命周期安全和合法利用管理，确保数据来源可溯、去向可查，行为留痕、责任可究。

（二）政府监管

市、县（市、区）公共数据主管部门应当履行下列公共数据安全管理职责：

1.建立健全授权运营安全防护技术标准和规范，落实安全审查、风险评估、监测预警等管理机制，明确各管理机制对应的负责部门，定期开展公共数据安全培训，培训主题与内容应针对培训对象进行具体调整；

2.实施数据产品和服务的安全合规管理，对授权运营域的操作人员进行认证、授权和访问控制，记录数据来源、产品加工和数据调用等全流程日志信息；

3.建立健全公共数据授权运营安全监督检查机制，做好针对授权运营行为中所产生数据信息的监督检查追踪工作，定期开展安全监督检查工作成果检查和安全检查系统技术升级。在安全监督检查中，发现授权运营单位存在较大安全风险的，可依法依规对授权运营单位进行约谈，并要求其采取相应的安全措

施进行整改消除隐患；

4.会同网信、密码管理、保密行政管理、公安、国家安全等单位，按照“一授权一预案”要求，结合公共数据授权运营的应用场景制定应急预案，并定期组织应急演练。发生数据安全事件时，公共数据主管部门应按照应急预案启动应急响应，采取相应的应急处置措施，防止危害扩大，消除安全隐患；

5.监督授权运营单位落实公共数据开发利用与安全管理责任，定期委托第三方机构，根据法律、法规等有关规定，对授权运营单位开展数据安全检测评估，并根据评估意见采取相应的安全措施。

（三）单位职责

授权运营单位应当履行下列公共数据安全管理职责：

1.建立完善的数据安全管理制度。实行“谁运营谁负责、谁使用谁负责”的责任制，明确授权运营单位的主要负责人是授权运营公共数据安全的第一责任人。

2.配合公共数据主管部门完成各类安全审查、信息登记、检测评估和培训演练工作，对于评估工作，应如实提供有关资料，不得拒绝、隐匿、瞒报。

3.建立健全公共数据开发利用日常监测、安全测评、风险评估、安全审查等机制，确保各参与主体在公共数据管理、需求审核、开发利用、技术支撑等全流程安全可控。

4.建立安全事件应急预案，发生数据泄露、毁损、丢失等数据安全事件或重大风险时，应立即启动授权运营安全应急处置预

案，并及时向公共数据主管部门汇报情况。

5.在数据授权运营过程中，授权运营单位如发现存在数据安全隐患或其它不安全因素，应第一时间向本级公共数据主管部门上报，并密切配合本级公共数据主管部门做好数据安全事件的处置及调查工作，积极采取措施消除安全隐患。

6.一旦发现可能或已经发生数据泄露等数据安全事件的，应立即通知本级公共数据主管部门，调查事件发生原因，积极采取补救措施，并承担相应法律责任。

（四）社会监督

社会公众有权对公共数据授权运营相关活动进行监督，认为存在违法违规行为的，可以向公共数据主管部门进行投诉或举报，公共数据主管部门应会同相关部门及时调查处理，并为举报人保密。

（五）法律责任

授权运营单位及相关人员存在违反国家相关法律法规的，依法承担相应的法律责任，侵犯他人商业秘密、个人隐私等合法权益或造成财产损失的，应由授权运营单位直接承担。

授权运营单位违反授权运营协议，属于违反网络安全、数据安全、个人信息保护有关法律法规规定的，由网信、公安等单位按照职责依法予以查处，相关不良信息依法记入其信用档案。

七、附则

本细则自2023年X月X日起施行。国家和省对公共数据授权运营管理有新规定的，从其规定。

附件：1.授权运营申请表；

2.授权运营协议模板。