公共数据分类分级及应用实践研究

何正庆[1]，吴善鹏[1]，刘超[1]，白惠文[2]，李安伦[2]，吴志刚[2]
1. 江苏省大数据管理中心，江苏 南京 210036；
2. 中国软件评测中心，北京 100048

摘要
公共数据分类分级制度是数据基础制度的重要部分，其有力有序的应用实施对数据要素的体系供给、高效流通和安全治理具有重要支撑保障作用。根据江苏省相关部门及设区市分类分级试点情况，提出可行的公共数据分类分级闭环管理方法，并针对不同敏感级别的数据建立分类分级管控体系，在保障数据安全的前提下，优化数据资源配置，促进数据共享开放和授权运营，提高数据流通交易的安全性和透明度，以推动数据要素价值有效释放。

关键词
公共数据；数据要素；安全治理；分类分级闭环管理；分类分级管控体系

中图分类号：TP309 文献标志码：A doi：10.11959/j.issn.2096–0271.2025032

Research on public data classification and grading and application practice

HE Zhengqing[1], WU Shanpeng[1], LIU Chao[1], BAI Huiwen[2], LI Anlun[2], WU Zhigang[2]
1. Jiangsu Province Big Data Management Center, Nanjing 210036, China
2. China Software Testing Center, Beijing 100048, China

Abstract
The public data classification and grading system is an important part of the data foundation system. Its strong and orderly application and implementation of data elements of the system supply, efficient circulation and security governance has an important role in supporting and guaranteeing. This paper proposes a feasible closed-loop management method for public data classification and grading based on the pilot situation of classification and grading of relevant departments and cities in Jiangsu Province. We establish a classification and grading control system for data of different sensitive levels. Under the premise of safeguarding data security, we optimize the allocation of data resources, promote data sharing and opening and authorized operation, and improve the security and transparency of data circulation and transaction, so as to promote the effective release of the value of data elements.

Key words
public data, data element, security governance, classification and grading closed-loop management, classification and grading control system

0 引言

数据作为新型生产要素，是数字化、网络化、智能化的基础，已快速融入生产、分配、流通、消费和社会服务管理等各个环节，深刻改变着生产方式、生活方式和社会治理方式。党中央高度重视发挥数据要素作用和完善数据基础制度。早在2015年，党的十八届五中全会就首次提出国家大数据战略，发布《促进大数据发展行动纲要》。2019年，党的十九届四中全会首次明确数据作为生产要素，可以按贡献参与分配。2020年，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，将数据、土地、劳动力、资本、技术并列为五大生产要素，要求加快培育数据要素市场。2022年，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》（简称“数据二十条”），要求加快构建数据基础制度体系。2023年新一轮机构改革中国家数据局成立，着力推动数据要素市场化配置改革，统筹数字中国、数字经济和数字社会规划和建设，加快发展新质生产力，加快推进实体经济和数字经济深度融合，加快培育全国一体化数据市场。2023年，国家数据局与中央网信办、科技部等17部门联合发布了《“数据要素×”三年行动计划（2024—2026年）》，部署了工业制造、现代农业等12个围绕数据要素应用的行动，发挥数据要素的放大、叠加、倍增作用，构建以数据为关键要素的数字经济[1]。

“数据二十条”聚焦数据产权、流通交易、收益分配和安全治理，提出了20条政策举措，科学搭建了我国数据基础制度的“四梁八柱”，要求在国家数据分类分级保护制度下，推进公共数据、企业数据、个人数据等分类分级确权授权使用和市场化流通交易，健全数据要素权益保护制度；结合数据流通范围、影响程度、潜在风险，区分使用场景和用途用量，建立数据分类分级授权使用规范[2]。数据的可复制性、非竞争性、非排他性、非耗竭性等特性，使数据的获取和利用难以通过物理方法简单化处理；同时，为充分释放要素价值，又要求让数据高效合规流动。因此，分类分级是数据要素流通交易的基础性工作，成为数据开发利用和安全保护的基准规则。

1 公共数据分类分级体系研究现状

鉴于各地区、各部门的定位不同、方案各异，公共数据分类分级的深化推进工作仍存在一系列挑战[3]。当前，公共数据领域主要存在3种分级框架体系，且相互之间并不兼容统一，是数据分级管理的难点重点。

第一种为政务数据分级框架体系。国务院办公厅秘书局发布的《政务数据资源目录编制规范》对公共数据提供了一种4级分级框架，国内多数地方政府部门的公共数据按照此方法定级。例如，浙江省《数字化改革 公共数据分类分级指南》、《安徽省政务数据分类分级指南（试行）》、《重庆市公共数据分类分级指南（试行）》、北京市《政务数据分级与安全保护规范》等地方标准将公共数据遭到破坏后的影响对象和影响程度作为定级要素。

第二种为一般数据、重要数据、核心数据分级框架体系。根据《中华人民共和国数据安全法》（简称《数据安全法》）的相关要求，按照数据对国家安全、公共利益或者个人、组织合法权益的影响和重要程度，将

数据分为一般数据、重要数据、核心数据。《网络安全标准实践指南——网络数据分类分级指引》《数据安全技术 数据分类分级规则》应用此类框架体系，后者根据数据在经济社会发展中的重要程度，以及一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益造成的危害程度，将数据从高到低分为核心数据、重要数据、一般数据3个级别。

第三种为网络安全等级保护分级框架体系。根据《网络安全等级保护基本要求》中所提的等级保护对象在国家安全、经济建设、社会生活中的重要程度，遭到破坏后对国家安全、社会秩序、公共利益以及公民、法人和其他组织的合法权益的危害程度等，由低到高被划分为5个保护等级。

从一些省级部门和设区市公共数据分类分级试点的探索情况看，当前多套数据分级框架同时存在，无法较好地使用统一标准开展数据分级。这给数据管理工作造成“一致性”困扰，难以明确公共数据的共享和开放属性，影响后续的数据使用和价值释放。因此，亟须探索一种能够兼容多种分级框架体系的分级方法。

此外，当前公共数据领域缺乏统一的分类分级保护体系，不同地区间的公共数据分级管控要求不尽一致，北京[4]、浙江[5]、重庆[6]、深圳[7]等地分别提出了分级保护要求，但是现有标准对于同一等级数据的保护要求存在明显差异，因此在可否共享或开放方面存在分歧，导致公共数据流通不畅。国务院新闻办公室新闻发布会称，截至2024年6月全国已上线226个地方数据开放门户，但从整体社会感知而言，数据开放工作仍存在数据种类少、数据更新慢等问题[8]。同样针对公共数据的最低敏感等级共享，《政务数据分级与安全保护规范》（北京）要求根据共享交换设置共享规则[4]，《公共数据安全要求》（深圳）则要求：公共数据提供部门应与公共数据使用部门签署相关协议，明确数据使用目的、供应方式、保密约定、数据共享范围、数据安全保护要求等内容；公共数据提供部门应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性等要求。

总体上，相关地区已经探索开展公共数据分类分级工作，取得了一定成效，但是仍然存在以下问题。一是分类分级的方法缺乏统一性，根据调研统计和地方试点情况分析，至少存在3种分级框架，不同分级方法对数据管理工作造成“一致性”困扰，影响数据流通应用。二是分级管控的方法缺乏系统性，一方面多数标准或规则未能明确不同等级公共数据的管控措施，所提到的管控措施难以区分管理措施和技术措施等不同维度，给数据分级保护落地执行造成困扰。另外，在针对共享开放等数据要素开发利用和流通的重点环节缺乏安全基线，导致对不同级别数据管控的程度区分不清楚。

公共数据属于高使用价值又无法替代的数据[9]，其有效应用服务意义重大，因此有必要明确公共数据分类分级方法以及相应安全管控措施。

2 公共数据分类分级闭环管理方法

2.1 江苏省公共数据分类分级试点总结

《江苏省公共数据管理办法》要求公共数据主管部门会同有关主管部门结合数据应用需求、数据安全和个人信息保护和数据应用需求等因素，根据国家分类分级保护制度要求，推动制定本省公共数据分类分级具体规则[10]。江苏省于2022年开展公

共数据分类分级试点工作，在试点过程中，发现的典型问题有以下4个方面。

• 数据分级的敏感级别定级比较困难，敏感级别高影响应用服务，敏感级别低影响风险防控，应用与安全的平衡点较难把握，阻碍了数据要素的有序流通。

• 部分行业已存在国家部委制定的数据分类分级标准规范，在制定省级公共数据分类分级指南的过程中要充分兼容行业已有标准规范，在数据共享开放过程中与行业标准保持相应的协调性。

• 部门单位风险管控能力基础不同，数据管理周期涉及汇聚（采集）、传输、存储、加工处理、共享、开放、销毁等多个环节，全环节实现统一管控比较困难，部分管控措施难以实现。此外，关于信息系统的等级保护要求，试点单位分级管控要求与等级保护要求之间要对应。

• 对行业数据分类分级情况，需要通过实际工作验证相关方法和规则的科学性、合理性。另外，辅助分类分级的技术手段相对缺乏，难以支撑数据的精准管理。

为了做好公共数据分类分级，一是需要制定更加精细、合理的定级原则和方法，平衡好定级细分颗粒度和执行难度之间的矛盾，设计兼容性更好的分级体系，尽可能兼容协调国办电子政务目录分级、网信部门网络数据分级方法、公安部门等级保护方法等不同的标准规范体系。二是在分级管控方面，需结合各省份、重点行业已有的数据分级管控策略，以及江苏省试点经验，创新和细化分级管控策略，明确管理措施、技术措施，并对数据生命周期各环节制定通用性要求、个性化要求，随着数据敏感级别增高，管控措施要求严格度依次递增。三是研究制定分类分级工作落实成效评价方法及量化评分算法，从数据目录分类分级标识设置情况、数据分类分级的合理度、分类分级更新及时性、共享和开放属性设置是否符合对应敏感级别的要求、分级管控措施是否达到要求等方面对分类分级工作进行量化评分，提供工作评价参考依据，从而形成闭环管理，达到优化升级的目的。

2.2 公共数据分类分级闭环管理

本文提出一种公共数据分类分级管理体系，总体思路如**图1**所示，通过数据资产梳理、数据分类、数据分级、标识审核、分级管控、成效评价和动态更新7个步骤，实现公共数据分类分级的闭环管理。

首先对数据资产进行全面梳理，明确数据资产基本信息和相关方，形成数据资产目录，包括以物理或电子形式记录的数据库表、数据文件以及其他结构化和非结构化数据资产；然后结合自身业务，按照主题、行业、对象等维度划分大类、中类和小类，以及按照业务特点进行更细粒度的划分；再结合自身业务特点，根据数据重要性、影响范围、影响程度等，综合考虑数据规模、领域、精度等因素，对公共数据进行分级。公共数据定级方法和规则见**表1**。

本文所提方法对现有3种分级框架体系的兼容情况见**表2**。其基本能够兼容《政务数据资源目录编制规范》，同时可以兼容《网络安全标准实践指南——网络数据分类分级指引》和《数据安全技术 数据分类分级规则》中对重要数据和核心数据的划分，《网络安全等级保护基本要求》等级划分规则整体高于本文方法，但本文后续通过数据分级管控要求进一步对应到相应保护等级。

公共数据分类分级实施主体应对分类分级标识结果进行自主检查，公共数据分类分级审核方对通过自主检查的分类分级

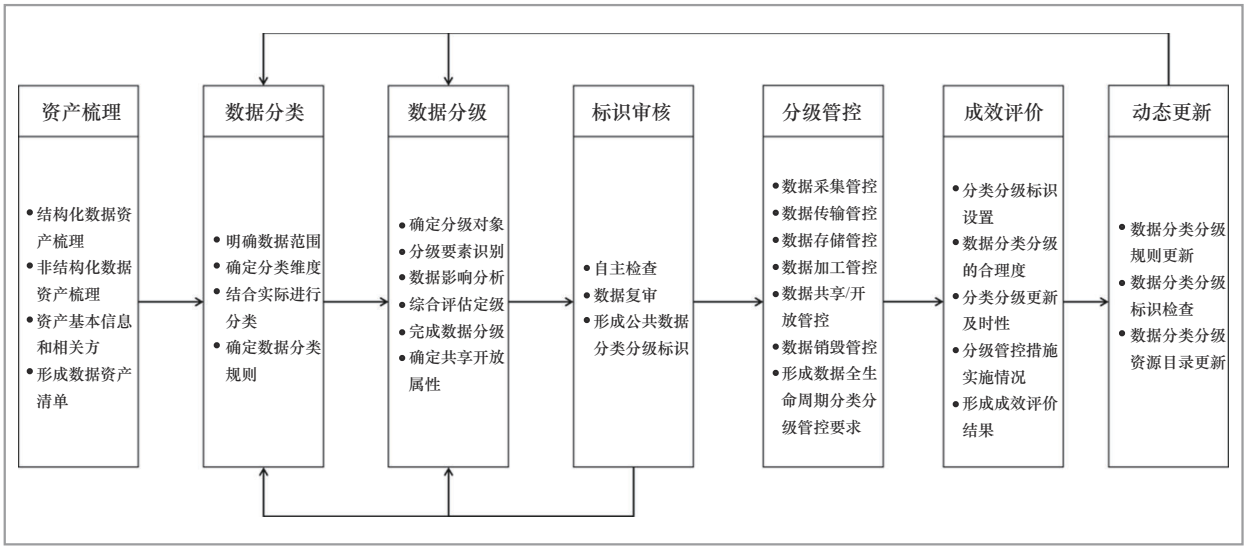

图1 公共数据分类分级管理体系

表1 数据级别和影响对象、影响程度的映射规则

细分级别	敏感程度	影响对象				
		国家安全	经济运行	社会稳定	公共利益	个人/组织合法权益
更高级	极敏感数据	特别严重危害、严重危害	特别严重危害	特别严重危害	特别严重危害	特别严重危害
四级	高敏感数据	一般危害	严重危害	严重危害	严重危害	特别严重危害
三级	敏感数据	轻微危害	一般危害	一般危害	一般危害	严重危害
二级	低敏感数据	无危害	轻微危害	轻微危害	轻微危害	一般危害、轻微危害
一级	不敏感数据		无危害	无危害	无危害	无危害

表2 本文方法对不同分级框架体系规则的兼容性说明

本文方法兼容情况	《政务数据资源目录编制规范》	《网络安全标准实践指南——网络数据分类分级指引》	《数据安全技术 数据分类分级规则》	《网络安全等级保护基本要求》
一级	兼容一级数据	兼容一般数据	兼容一般数据	等保中不存在无危害情况
二级	兼容二级数据			兼容一级和部分二级定级规则
三级	兼容三级数据			兼容部分二级和三级定级规则
四级	兼容四级数据	兼容重要数据	兼容重要数据	兼容四级定级规则
更高级	为公共数据定级留出备用级别，后续按照国家相关法律法规等要求，极其重要的数据定为更高级别（五~六级）	兼容核心数据	兼容核心数据	高于四级定级规则

结果进行复审，主要检查分类分级标识是否完善、共享/开放属性设置是否合理等。审核发现明显错误的应退至分类分级标识主体并提示修改；未发现错误的予以通过。数据审核通过后，分类分级主体应进行确认，形成分类分级标识结果，并按管控要求进行共享开放。

为了促进分类分级有效落地执行，要对分类分级成效进行科学评估，完成优化更新和闭环管理。以数据目录为最小评估颗粒度，设置分类标识设置及合理程度、分级标识设置及合理程度、共享和开放属性的设置及合理程度、全生命周期管控措施等指标项。此外，还需根据实际业务情况，以及数据重要程度和可能造成的危害程度变化，对数据分类分级规则、数据分类分级标识和资源目录等进行动态更新。

3 多维度公共数据分类分级管控体系构建

本文所提公共数据分类分级管控体系如**图2**所示，首先对公共数据进行分类，再对每个类别的公共数据进行分级，最后针对不同级别的公共数据实施分级管控，从而落实分类分级保护制度。

按照《数据安全法》、“数据二十条”等文件要求，数据开发利用需要在分类分级保护下有序开展。本文提出一种多维度的分类分级管控体系。管控体系由管理措施和技术措施两部分组成：管理措施提出全生命周期的组织保障、制度流程、人员能力等方面的要求；技术措施针对数据收集、存储、加工等各个阶段使用的平台和工具等提出要求，如访问控制、权限管理、加密算法、脱敏工具等。管理措施和技术措施相互配合，可以有效提升管控体系的保护能力。

为了制定有效的分级管控细则条款，本文充分借鉴了现有网络等保相关要求[11]，金融、电信等行业经验[12-15]，以及现有公共数据标准中的分级管控要求等[4,16]，并结合江苏省分类分级试点的实践经验，提出了数据全生命周期通用要求和

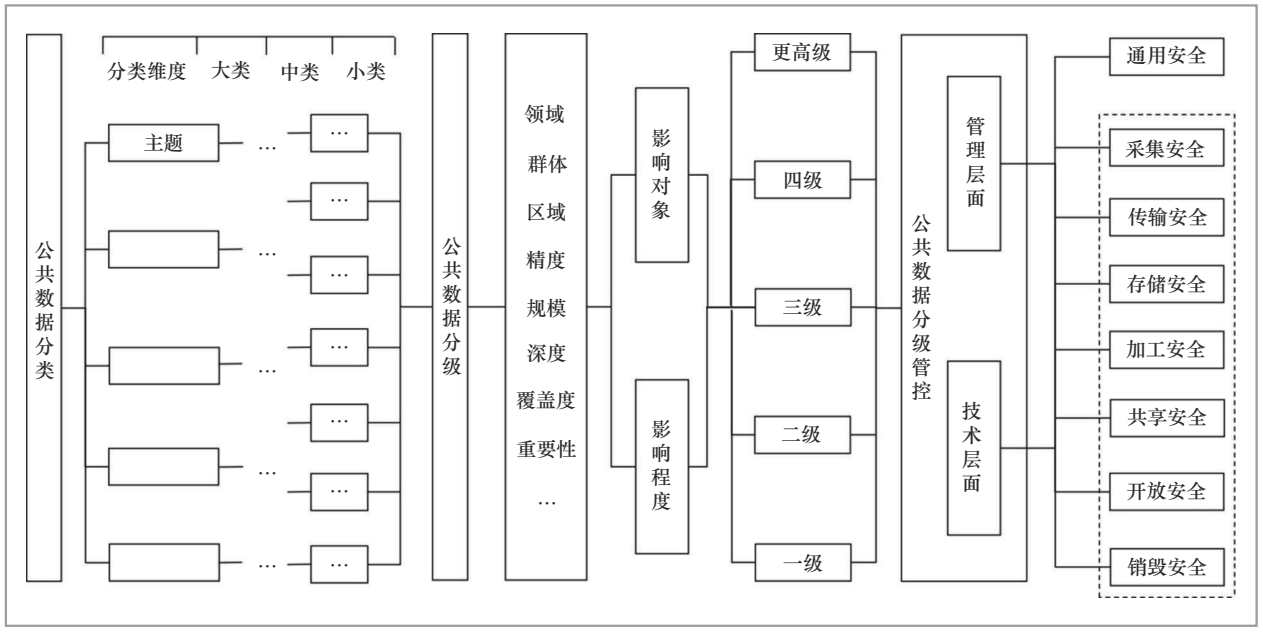

图2 公共数据分类分级管控体系框架

数据采集、传输、存储等各个环节特定的要求，并分别制定符合不同敏感级别公共数据的管控措施。例如，针对数据全生命周期各个阶段，均需采用口令认证等方式进行身份鉴别和授权处理，设置访问控制规则等，且对高敏感级别数据，还需进一步明确使用范围并设置限定条件，特定情况需进行“一事一议”。针对加工、共享析等促进数据流通的重点环节，制定的管控措施见**表3**和**表4**。建立管理措施和技术措

表3 数据加工安全措施

措施	第一级数据	第二级数据	第三级数据	第四级数据	更高级
管理措施	1.建立数据加工审核管理机制，明确数据加工处理的目的、操作人员、数据获取方式、权限范围、授权机制、预计产生的新数据等信息，经审批授权后方可开展相关工作；对数据操作行为进行全流程记录，相关信息保存时长不低于6个月，并进行定期审计和检查 2.开展数据加工活动过程中，可能危害国家安全、公共安全、经济安全和社会稳定的，立即停止加工活动 3.建立身份鉴别与访问控制机制，防止非授权数据加工 4.对数据加工结果进行评估，如产生新数据，对新数据进行安全审核、合规风险评估和数据使用授权流程，确保新数据不存在数据泄露风险。对加工、分析产生的新数据设置级别标签	在满足一级管控要求基础上，还应采取： 1.在数据加工之前进行数据风险评估，并制定约束机制 2.对数据进行脱敏后再进行加工、分析，确需直接对其进行非脱敏的加工、分析时，经审核批准后进行 3.对数据本地下载等敏感操作行为进行监控，并进行二次审批操作 4.建立数据风险应急预案，明确启动预案的条件、应急处理流程、应急资源保障等。应定期对应急预案重新评估，修订完善；相关人员应定期参加应急处理技能培训，并通过考核 5.获得数据加工授权的人员签署保密协议，不应进行非授权操作，不应复制和泄露任何信息 6.如涉及数据加密(或脱敏)，加工执行方和加密(或脱敏)方由不同人员分别实施	在满足二级管控要求基础上，还应采取： 1.严格限制数据加工的组织、企业和个人范围，限定数据加工使用的目的和范围；对加工超过100万条数据的人员进行登记备案管理，应审核其个人身份信息、工作单位资质和信誉；对曾经出现过数据安全事件的个人和组织，禁止其参与数据加工 2.建立数据加工风险监测管理机制，明确威胁行为、风险内容、处理要求等相关措施 3.数据加工操作由多人多级分权审核管理，确保单人无法拥有数据的完整操作权限	在满足三级管控要求基础上，还应采取： 1.一般情况不允许加工若需加工时，遵循“一事一议、一事一审核”原则，经审核批准后，进行脱敏降级后予以加工 2.对加工数据加密时，相关密码至少由两人管理	不允许加工
技术措施	1.依据权限最小化原则分配账号权限，通过管控技术手段统一实现账号认证和权限分配；不同用户只能访问与其权限对应的数据 2.采用口令认证等方式进行身份鉴别和授权处理，设置访问控制规则，依据权限合理调配数据，防止非授权的加工、分析操作 3.对系统间和后台数据的导出进行监控，通过技术手段予以严格控制 4.远程加工、分析数据时，严格限制数据加工、分析终端的外部接入IP数量和地址	在满足一级管控要求基础上，还应采取： 1.采用可靠技术手段对数据进行加密或脱敏处理，防止数据加工过程中的数据泄露。若必须使用原始数据，需提供必要性说明，经审批授权后方可使用原始数据进行加工处理，并对数据操作行为进行每日审计监管 2.仅在内部环境进行数据加工、分析操作，并采取技术措施禁止远程加工、分析数据 3.定期进行应急演练	在满足二级管控要求基础上，还应采取： 1.采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现 2.对加工处理产生的新数据进行加密保护 3.建设数据加工风险监测预警系统，对数据加工的全过程进行监测、记录、审计，对异常数据操作行为及时预警、处置，对违规行为及时阻断	在满足三级管控要求基础上，还应采取： 对数据加工过程进行实时风险监控，并进行持续动态认证和授权	

表4 数据共享安全措施

措施	第一级数据	第二级数据	第三级数据	第四级数据	更高级
管理措施	1.建立数据共享目录，明确数据共享范围和使用属性 2.无条件共享 3.数据共享实施报备登记管理，并留存相关共享记录，相关信息保存时长不低于6个月，并进行定期审计和检查	在满足一级管控要求基础上，还应采取： 1.建立数据共享的审核批准机制，有条件共享，明确数据共享目的、申请方、范围（应细化到数据项）、期限、频次等内容，对数据共享申请应进行严格审批和授权，经审核批准后，予以共享 2.针对数据共享，事前开展数据风险评估，并制定约束机制 3.建立数据风险应急预案，明确启动预案的条件、应急处理流程、应急资源保障等；定期对数据风险应急预案进行重新评估、修订完善；相关人员定期参加应急处理技能培训，并通过考核	在满足二级管控要求基础上，还应采取： 1.明确数据共享限定的组织范围，限定使用目的和范围 2.对数据共享申请方的数据安全保护能力进行评估，确保其具备足够的数据安全保护能力 3.建立数据共享风险监测管理机制，明确威胁行为、风险内容、处理要求等相关措施 4.采取多人分级分权形式对数据共享进行审批、监督、执行、归档等管理	在满足三级管控要求基础上，还应采取： 1.一般情况不予共享，若需共享时，遵循“一事一议、一事一审核”原则，经审核批准后，进行脱敏降级后予以共享 2.若需提供密钥给数据共享申请方，密钥至少由其两人管理	不允许共享
技术措施	1.采用口令认证等方式，进行身份鉴别和授权处理，设置访问控制规则，依据权限合理调配数据 2.采取可靠技术手段，保证共享数据的完整性、一致性，防止数据的篡改、丢失及滥用	在满足一级管控要求基础上，还应采取： 1.定义数据共享的数据项（字段）、数据资源类型、传输方式、更新频率等信息，并对数据共享过程进行记录和审计 2.建立可靠的数据共享通道，如VPN、专线等 3.定期进行应急演练	在满足二级管控要求基础上，还应采取： 1.采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术进行身份鉴别，且其中一种鉴别技术至少使用密码技术来实现 2.对共享场景进行评估，可以满足需求的情况下，采用数据可用不可见的方式提供数据共享，如对数据进行加密或脱敏处理；若共享场景必需明文数据，对不同的数据共享申请方提供不同的密钥或将数据解密后提供 3.建设数据共享风险监测预警系统，对数据共享的全过程进行监测、记录、审计，对异常数据操作行为及时预警、处置，对违规行为及时阻断，必要时切断数据共享	在满足三级管控要求基础上，还应采取： 1.对共享的数据采取数字水印等技术，确保共享数据可溯源 2.宜采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性	

施相结合的分类分级管控体系，可以有效实施公共数据的精细化管理，从而平衡数据的开发利用和安全保障，有利于公共数据要素流通。

4 分类分级促进公共数据有序流通

按照“数据二十条”、《国务院关于加强数字政府建设的指导意见》、《国务院办公厅关于印发全国一体化政务大数据体系建设指南的通知》等国家顶层设计要求，江苏省全面推进数字政府建设，加快数字化转型，促进公共数据共享开放，印发省政府规章《江苏省公共数据管理办法》和《江苏省“十四五”数字政府建设规划》《省政府关于加快统筹推进数字政府高质量建设的实施意见》等政策文件，并加快贯

彻落实。为保障超大规模数据应用服务安全有序开展，江苏省发布了地方标准《公共数据管理规范 第1部分：数据分类分级》和《公共数据管理规范 第2部分：数据共享交换》，落实公共数据分类分级制度，促进公共数据有序流通和开发利用，在数据要素流通价值链[17]中发挥重要作用。

2023年，江苏省在无锡、徐州、苏州、南通、淮安、泰州等地开展了公共数据授权运营试点工作，试点地区制定了公共数据分类分级管理、授权运营管理等文件，促进公共数据开放和授权运营。公共数据分类分级作为前置动作，明确数据属性和用途，帮助数据授权运营更具针对性和可操作性，优化数据授权运营的流程和模式，提高数据处理的效率和准确性，从而实现数据的精准利用。

淮安市建设市公共数据开放与运营管理平台，在金融、医疗等领域开展数据授权运营，推出“淮数易贷”“惠民就医”等应用场景；通过公共数据资源的整合共享和开发利用，为金融机构提供精准数据服务支持，从而降低金融机构的获客成本和信贷风险；细化数据分类，筛选出符合金融机构需求的数据目录，金融机构通过联合建模、可用不可见方式在公共数据中查询与企业信用、经营状况、行业信息等相关的子类数据，精准获取数据服务，避免超范围使用等问题；通过明确数据分级，确定数据安全使用要求，金融机构同步明确接收数据结果后的防护措施，制定更加合理的数据结果使用策略，提升数据资产整体价值。此外，公共数据分级管控措施中要求，对数据挖掘分析过程中产生的新数据，按照数据分级相应的保护要求进行防护。综上所述，公共数据的分类分级管理保障了数据的合规流通，提高了信贷审批效率和准确性。随着数字经济不断发展，相关金融服务创新举措将会越来越依赖于高质量的公共数据资源供给，而公共数据分类分级则是确保上述数据资源有效利用的基础和前提。

2023年，宿迁市发布数据产品“企业近一年行政处罚可视化分析数据”，进入数据交易场所挂牌并成功交易，实现了数据要素市场流通[18]。在这个过程中，公共数据分类分级有效厘清了从数据资源化到要素化的发展演变。数据分类分级进一步明确了数据的价值，合规界定不同类别和级别的数据在市场上的价值差异，通过合理的分类分级确保评估结果的公正性和准确性。在数据产品审查过程中，需要对数据产品的安全性、合规性进行审查，数据分类分级帮助审查机构快速识别出可能涉及敏感信息或需要特殊保护的数据类别，从而采取相应的审查措施。通过数据分类分级，相关部门可以明确哪些数据适合进行交易，哪些数据需要限制交易或采取特殊保护措施，有助于降低数据交易的风险，提高交易的效率和成功率。数据分类分级为该类数据产品交易的顺利进行提供了保障。

为了深入推进数字经济和实体经济融合发展，江苏省连续多年举办省级数据开发与应用的相关赛事活动，围绕医疗卫生、智慧交通、智慧康养、新能源等赛道探寻创新解决之道，助推江苏数字经济高质量发展。通过数据分类分级，数据开发应用能够根据数据敏感级别设置更加合理的模型算法、风险防控措施，在发挥数据价值的同时兼顾数据安全，参赛者更加深入地挖掘数据的潜在价值，发现新的应用场景和解决方案，从而深化数据管理开发利用，推进数据资源的高效率配置、高质量供给，强化公共数据与行业数据深度融合，以业

务需求为牵引积极打造应用场景，提升政府治理能力和公共服务水平。

从上述实例可以看出，公共数据分类分级在明确数据所有权和使用权、优化数据资源配置、促进数据共享和开放、提高数据交易的安全性和透明度、保障数据安全、推动数据市场的健康发展等方面都发挥了重要作用，为数据要素的有序流通和开发利用提供了有力支持。

5 结束语

数据分类分级有利于更加有效地管理数据，推动数据开放共享和流通。本文构建了一种公共数据分类分级闭环管理框架，并建立分类分级管控体系，在公共数据管理中进行实践并取得良好成效。一方面，数据流通过程涉及多个环节且每个环节的主体不同，分类分级有助于明确各环节各主体的使用范围和使用边界，消除公共数据、企业数据和个人数据的开放共享顾虑，进而提高数据要素市场供给；另一方面，分类分级有效促进了对数据的挖掘利用，在保障安全的前提下，推动数据处理者依法依规对原始数据进行开发利用，有利于数据处理者行使数据应用相关权利，促进数据使用价值复用与充分利用，进一步推动了数据使用权交换和市场化流通。

参考文献：

[1] “数据要素×”三年行动计划(2024—2026年)[EB]. 2024.
Three-year action plan for “data elements ×”(2024-2026)[EB]. 2024.

[2] 中华人民共和国中央人民政府. 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[EB]. 2022.
The Central People’s Government of the People’s Republic of China. Opinions of the Central Committee of the Communist Party of China and the State Council on establishing the fundamental data system to better leverage the role of data elements[EB]. 2022.

[3] 王跃, 苏娜. 我国政务数据分类分级实施关键问题与实践研究[J]. 大数据, 2024, 10(3): 16-26.
WANG Y, SU N. Research and practice on key issues in the implementation of government data classification and grading in China[J]. Big Data Research, 2024, 10(3): 16-26.

[4] 北京市市场监督管理局. 政务数据分级与安全保护规范[EB]. 2022.
Beijing Municipal Administration for Market Regulation. Specifications for classification and security protection of government data[EB]. 2022.

[5] 浙江省市场监督管理局. 数字化改革 公共数据分类分级指南[EB]. 2021.
Zhejiang Provincial Administration for Market Regulation. Guidelines for public data classification and categorization in digital reform[EB]. 2021.

[6] 重庆市大数据应用发展管理局. 重庆市公共数据分类分级指南(试行)[EB]. 2021.
Chongqing Municipal Administration of Big Data Application and Development. Guidelines for public data classification and categorization (Trial)[EB]. 2021.

[7] 深圳市政务服务数据管理局. 公共数据安全要求[EB]. 2022.
Shenzhen Municipal Administration of Government Service and Data Management. Security requirements for public data[EB]. 2022.

[8] 高丰. 厘清公共数据授权运营: 定位与内涵[J]. 大数据, 2023, 9(2): 16-32.
GAO F. Investigation into authorized

public data operation: its positioning and nature[J]. Big Data Research, 2023, 9(2): 16-32.

[9] 朱扬勇. 依照数据用途界定公共数据[J]. 大数据, 2024, 10(3): 163-167.
ZHU Y Y. On public data[J]. Big Data Research, 2024, 10(3): 163-167.

[10] 江苏省公共数据管理办法[EB]. 2021.
Management measures for public data of Jiangsu Province[EB]. 2021.

[11] 全国信息安全标准化技术委员会.信息安全技术 网络安全等级保护基本要求[EB]. 2019.
National Information Security Standardization Technical Committee. Information security technology—baseline for classified protection of cybersecurity [EB]. 2019.

[12] 全国金融标准化技术委员会. 金融数据安全 数据安全分级指南[EB]. 2020.
National Financial Standardization Technical Committee. Financial data security—data security classification guidelines[EB/OL]. 2020.

[13] 中国证券监督管理委员会. 证券期货业数据分类分级指引[EB]. 2018.
China Securities Regulatory Commission. Guidelines for data classification and categorization in the securities and futures industry[EB]. 2018.

[14] 全国信息安全标准化技术委员会. 信息安全技术 健康医疗数据安全指南[EB]. 2020.
National Information Security Standardization Technical Committee. Information security technology—guidelines for health and medical data security[EB]. 2020.

[15] 王健, 周磊, 刘欣, 等. 电力行业数据安全防护思路研究[J]. 网络空间安全, 2021, 12(5): 17-22.
WANG J, ZHOU L, LIU X, et al. Application and research of cyber security insurance on industrial control system[J]. Cyberspace Security, 2021, 12(5): 17-22.

[16] 江苏省市场监督管理局. 公共数据管理规范 第1部分:数据分类分级[EB]. 2023.
Jiangsu Provincial Administration for Market Regulation. Specification for the management of public data—Part 1: data classification and grading[EB]. 2023.

[17] 黄丽华, 杜万里, 吴蔽余. 基于数据要素流通价值链的数据产权结构性分置[J]. 大数据, 2023, 9(2): 3-15.
HUANG L H, DU W L, WU B Y. Structural separation of data property rights based on data factor circulation value chain[J]. Big Data Research, 2023, 9(2): 3-15.

[18] 叶雅珍, 朱扬勇. 数据知识产权:一种可流通交易的数据权[J]. 大数据, 2024, 10(2): 192-195.
YE Y Z, ZHU Y Y. Data intellectual property is a negotiable and tradable data property[J]. Big Data Research, 2024, 10(2): 192-195.

作者简介

何正庆（1977– ），男，江苏省大数据管理中心副主任，主要研究方向为数据资源管理、数据要素市场化等。

吴善鹏（1979– ），男，江苏省大数据管理中心处长、高级工程师，主要研究方向为数据资源管理、数据要素市场化、数据安全等。

刘超（1987– ），男，江苏省大数据管理中心高级工程师，主要研究方向为数据资源管理、数据要素市场化、人工智能等。

白惠文（1992– ），男，博士，中国软件评测中心工程师，主要研究方向为数据安全治理、数据空间、网络流量分析、云计算安全、人工智能等。

李安伦（1986– ），男，中国软件评测中心高级工程师，主要研究方向为数据治理、数据要素、云计算安全等。

吴志刚（1969– ），男，中国软件评测中心副主任、高级工程师，主要研究方向为数据要素、数据治理、电子政务、智慧城市等。

收稿日期: 2024-09-26