ICS 35.240
CCS L 70

中华人民共和国国家标准

GB/T XXXXX—XXXX

数据利用管理技术要求

Technical requirements for data utilization management

(点击此处添加与国际标准一致性程度的标识)

草案版次选择

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国数据标准化技术委员会（SAC/TC609）提出并归口。

本文件起草单位：中国科学院信息工程研究所、中国电子技术标准化研究院、西安电子科技大学、北京大学、中国移动通信集团有限公司、国家信息中心、蚂蚁科技集团股份有限公司、国家计算机网络与信息安全管理中心、中国信息通信研究院、深圳数据交易所有限公司、杭州海康威视数字技术股份有限公司、中国电信集团有限公司、联通数字科技有限公司、航天信息股份有限公司、北京快手科技有限公司、交通银行股份有限公司、中国太平洋保险（集团）股份有限公司、中共廊坊市委网络安全和信息化委员会办公室、公安部第三研究所、工业和信息化部电子第五研究所、中国电子信息产业发展研究院、生态环境部信息中心、农业农村部大数据发展中心、水利部信息中心、北京国际大数据交易所有限责任公司、上海数据交易所有限公司、内蒙古自治区大数据中心、湖北大数据集团数据开发有限公司、天翼云科技有限公司、中移物联网有限公司、中移互联网有限公司、中移动信息技术有限公司、中国移动通信有限公司研究院、中国电力科学研究院有限公司、国网天津市电力公司、国网山东省电力公司、数据空间研究院、蓝象智联（杭州）科技有限公司、华控清交信息科技（北京）有限公司、南京大数据检测技术有限公司、奇安信科技集团股份有限公司、长春吉大正元信息技术股份有限公司、杭州安恒信息技术股份有限公司、北京天融信网络安全技术有限公司、中科信息安全共性技术国家工程研究中心有限公司、中电科网络安全科技股份有限公司、北京计算机技术及应用研究所、上海计算机软件技术开发中心、广州芳禾数据有限公司、翼盾（上海）智能科技有限公司、西安交通大学、电子科技大学、中国质量认证中心、重庆市质量和标准化研究院、浙江大数据交易中心、中移雄安信息通信科技有限公司、联通数据智能有限公司、煤炭科学研究总院有限公司、中国南方航空股份有限公司、中资网络信息安全科技有限公司、国家石油天然气管网集团有限公司、中国科学院计算技术研究所、中国工业互联网研究院、中国交通建设集团有限公司、北京国信新网通讯技术有限公司、北京亿信华辰软件有限责任公司、广州大学、中检集团天帷网络安全技术（合肥）有限公司、浪潮云信息技术股份公司、施耐德电气(中国)有限公司、安徽省征信股份有限公司、安徽省川佰科技有限公司、上海市数字证书认证中心有限公司、北京华宇信息技术有限公司、北京睿数信安科技有限公司、深圳市优必选科技股份有限公司、湖北省标准化与质量研究院、广州地铁集团有限公司、浙江有数数智科技有限公司、浪潮电子信息产业股份有限公司、广电运通集团股份有限公司、讯飞医疗科技股份有限公司、中国汽车工程研究院股份有限公司、暨南大学、缔加数智科技（浙江）有限公司、迪安诊断技术集团股份有限公司、阿里巴巴（中国）有限公司、浙江蚂蚁密算科技有限公司、神州数码融信软件有限公司、西安邮电大学、上海零数众合信息科技有限公司、清华大学、中电科大数据研究院有限公司、洞见科技（雄安）有限公司、苏州数据资产运营有限公司、下一代互联网关键技术和评测北京市工程研究中心有限公司、北京邮电大学、清雁科技（北京）有限公司、中电数据产业集团有限公司、中关村工信二维码技术研究院、海南电网有限责任公司信息通信分公司、北京理工大学、北京交通大学、广东电网有限责任公司、广东电力人工智能试验研究院、南方电网财务有限公司、中国南方电网有限责任公司超高压输电公司、南方电网数据平台与安全（广东）有限公司、广东智转科技有限公司、南航数智科技（广东）股份有限公司、南方电网互联网服务有限公司、机械工业经济管理研究院、北京智网数科技术有限公司、中科斯欧（合肥）科技股份有限公司、贵阳大数据交易所有限责任公司

本文件主要起草人：牛犇、李凤华、范科峰、李晖、王亚沙、茹志强、王鹏彪、韦韬、赵芸伟、袁博、赵婉露、陈加栋、张鑫、房秉毅、张群、李璐璐、落红卫、童蕙、俞斌、刘顺海、刘继顺、魏光辉、

韩冰、黄明祥、哈晓琳、成建国、李振军、吴波、张建军、熊威、杨天路、汤强、黄睿麒、张帆、喻炜、黄秀丽、倪家明、呼海林、林传文、王超、靳晨、陈志洋、安锦程、张念彬、周亚超、王鹏、胡建勋、望娅露、陈志浩、蔡立志、童瑶、朱易翔、王伟、李雄、王锋、姚波、孔俊、钱岭、王静、杨波、武光城、张浩、尹峰、贾蕾、孙毅、张旭、刘学忠、于娜、陈先波、孙哲、刘京、荆潇、曹海霞、杨雪、管松、杨晶、康丽丽、姜玉琳、梁乔玲、李媚婧、温辛妍、梁协君、齐园、金广、程美、蒲云川、李明、邵志鹏、孔睿、李世奇、潘无穷、张琨、陈彦萍、兰春嘉、支婷、李博、杨红、刘东、朱孔林、林杨、顾延甲、牛小兵、王宁、王硕、任爽、陈玥、卢志良、李磊、文星、卢有飞、田志山、陈璟、夏武、杨倩、王为中、赵兴文、赵俊峰、李冠洲、李婷、昌文婷、韩晗、贾轩、许智立、闫皓楠、李锋、李娟、王昕、周晓阳、王磊、孔德智、王超、郝千婷、谢文君、栾明月、崔连伟、沈江涛、王帅、张海涛、周桐、伊然、李征、邵志鹏、王凯、刘荫、赵春玉、张静、伊鹏达、闭珊珊、李朗、姚俊、王晨旭、张源、杜潇霖、龚庆、陈钰炜、王瀚仪、杨佳丽、李阳、张建中、孙颜威、于涛、宋兆雄、祖岩岩、罗海宁、陆禹彤、殷丽华、马英、武建双、聂梦婷、郭猛猛、焦继超、李闻宇、何佳嘉、罗文玲、尤梦祥、吴洁、翁嘉思、张晓蒙、张文华、孙雪华、杨珍、魏勰、张旭东、丁浩、王国仕、贾晓俊、周昉昉、马波勇、温晓君、衣德良、费稼轩、赵梦原、杨波、王继龙、徐周、李崇、刘超、刘紫君、李鹏、宣秀芳、郭军、安俊朋、张幼明、陶衡、李霖泽

引　言

本文件旨在全方位规范数据利用管理流程，保障数据在各关键环节的安全与合规，促进数据的合理高效利用；确保数据利用管理攸关方有序参与数据的收集、存储、使用、加工、传输、提供、公开、销毁等一系列活动，保障数据处理流程的规范与顺畅；提出具体的技术要求和控制措施，提升数据管理的整体效能。本文件通过科学化、规范化和系统化的管理手段，确保数据在全生命周期内的合法性、安全性、可用性和价值最大化，对于推动数据价值释放、助力数字经济和社会发展具有重要意义；能够解决数据利用过程中存在的安全隐患、合规性差、流转不畅等问题，打破数据流通障碍，增强数据的可信度，降低企业数据管理风险。同时，助力企业提升行业整体数据管理水平，为构建健康有序的数据生态环境提供标准化支撑，维护国家数据安全和个人、企业的合法权益，推动数字经济的可持续发展。

数据利用管理技术要求

1 范围

本文件规定了数据利用管理相关的术语和定义、数据利用管理概述，描述数据利用的控制策略要求、数据利用管理主要环节的技术要求，以及相关通用技术要求，提供数据利用管理模型的使用方法。

。

本文件适用于数据基础设施各攸关方规范其在数据利用活动中的行为。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239—2019 信息安全技术　网络安全等级保护基本要求

GB/T 25069—2022 信息安全技术　术语

GB/T 35273—2020 信息安全技术　个人信息安全规范

GB/T 35274-2023 数据安全技术　大数据服务安全能力要求

3 术语和定义

GB/T 22239—2019,GB/T 25069—2022,GB/T 35273—2020以及GB/T 35274-2023界定的以及下列术语和定义适用于本文件。

3.1

原始数据　raw data

初次或源头收集的、未经加工处理的数据。

[来源：国家数据局发布《数据领域常用名词解释》（第一批）第2条]

3.2

数据供给方 data supplier

产生、持有或控制数据，并在流通中出售、提供数据的组织或个人。

注：数据加工处理流通情形可能涉及多个提供方对数据进行联合处理或融合计算，针对非本方提供的数据而言，提供方也属于数据接收方。

3.3

数据服务方　data service provider

提供各类服务的主体，包括数据开发、数据中介、数据托管等类型，提供数据开发应用、交易撮合、托管运营等服务。

3.4

数据需求方 data demander

在数据流通中收集、接收、购买或使用数据的组织或个人。

3.5

数据监测方 data monitoring entity

负责监督和执行系统或生态系统内数据管理实践、政策和法规合规性的权威机构或管理方。

3.6

数据收集 data collection

通过向数据源方收集和捕获信息，以创建数据集或获取关于特定现象的知识的过程。

3.7

数据存储 data storage

将数据用某种结构保存在计算机的物理介质中，以便加工、重用或存档。

3.8

数据使用 data usage

将数据用于各种目的，如分析、决策、研究或问题解决的过程。

3.9

数据加工 data processing

通过数据变换、数据转换、数据编码、数据计算、数据压缩、数据分析等数据操作，生成新数据（集）的数据处理活动。

[来源：GB/T 35274—2023，3.6]

3.10

数据传输 data transmission

数据在不同实体之间进行交换或流动的过程，包括本地网络传输、远程通信等。

3.11

数据提供 data provision

以标准化和可互操作的方式向其他系统、应用程序或实体传输或共享数据的过程。

3.12

数据公开 data disclosure

数据集、研究结果或其他与数据相关的资源提供给更广泛受众的过程。

3.13

数据销毁 data destruction

从存储介质或系统中永久且安全地擦除数据，使其无法恢复，防止未经授权访问的活动。

3.14

场内流通 on-exchange circulation

数据在特定的交易机构或平台内进行的流通行为。

3.15

场外流通 off-exchange circulation

数据供需双方不通过数据交易机构或平台，直接进行数据流通的行为。

4 缩略语

下列缩略语适用于本文件。

DUMM：数据利用管理模型（Data Utilization Management Model）

5 数据利用管理概述

5.1 总体原则

5.1.1 合法性原则

数据利用遵循“来源合法、过程合规、目的正当、权益保障”的总体要求，不侵害数据主体及相关方合法权益。

5.1.2 最小化原则

仅收集和利用实现特定目的所需的最少数据，避免过度采集和冗余存储。数据收集时只获取与目的直接相关的数据，利用时只处理必要的数据，存储时只保留有价值的数据，并及时删除不再需要的数据，以减少数据泄露和滥用的风险。

5.1.3 安全性原则

采取必要的技术和管理措施，确保数据在全生命周期内的保密性、完整性和可用性。

5.1.4 透明性原则

向数据供给方清晰说明数据利用的目的、范围和方式，并取得其授权同意。涉及明确告知数据供给方数据将被用于何种用途、涉及哪些数据以及如何被处理和存储，以确保其知情权和选择权得到充分尊重。

5.1.5 可追溯性原则

建立完整的日志记录机制，确保数据利用过程可审计、可追溯。

5.2 数据利用管理模型

数据利用管理模型（DUMM）的基本架构如图1所示，由以下三个维度构成：

a) 数据利用的攸关方：包括数据的供给方、需求方、服务方、监测方；
b) 数据利用的管理策略：包括策略生成、策略调整、策略传递、策略执行、策略验证；
c) 数据利用的主要环节：包括数据收集、数据存储、数据使用、数据加工、数据传输、数据提供、数据公开、数据销毁。

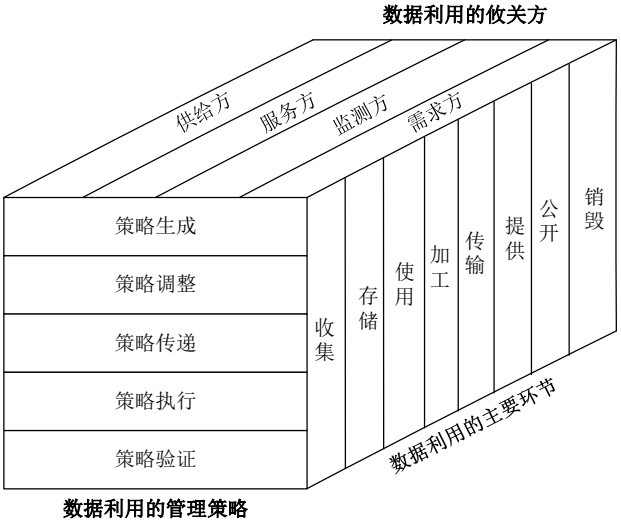

图1 数据利用管理模型

DUMM基本流程如图2所示，具体的使用方法详见附录A。

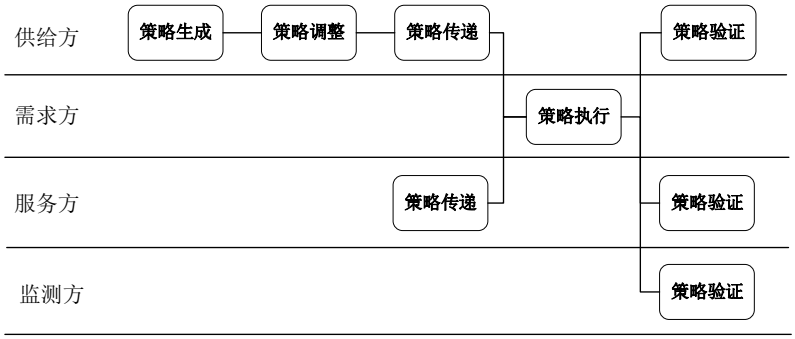

图2　DUMM 的流程示意图

5.3　数据利用管理框架

数据利用管理框架如图3所示。

数据供给方和数据需求方通过数据利用管理的各主要技术环节实现场内流通，也可直接完成场外流通。

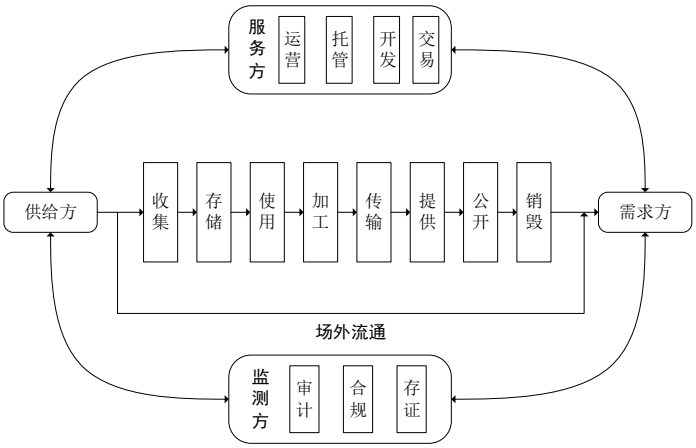

图3　数据利用管理框架

6　数据利用的控制策略要求

6.1　策略生成

对数据利用的控制是将数据供给方和数据需求方之间关于数据如何被利用的条款和条件，保证数据在复杂环境中按约定利用，策略生成方面的要求如下：

a)　数据持有者应在数据收集时生成策略，数据供给者应在数据交易时生成策略；

b)　应考虑利用范围、用途，包括主体、频率、时限、目的、方式、期限，以及是否自用、模型训练、售卖等；

c)　应考虑利用环境，包括设备、运行环境等；

d)　应考虑利用权限，包括自用、所有人、授权的需求方、特定场所等；

e)　应考虑数据传输的要求，包括需求方身份、传输速度、安全性等；

f)　应考虑数据存储的要求，包括存储环境、安全性等；

g)　应考虑数据加工的要求，包括加工用途、加工算法等；

h） 应考虑数据提供的要求，包括提供方式、提供对象、提供数据范围等；
i） 应考虑数据公开的要求，包括公开方式、公开范围、公开对象、公开内容等；
j） 应考虑数据销毁的要求，包括销毁方式、销毁强度、销毁粒度等。

6.2 策略调整

策略调整方面的要求如下：
a） 应由数据供给方调整策略；
b） 应考虑策略调整的合规性，明确策略调整依据，包括对数据攸关方需求、数据利用场景、数据质量等进行重新评估；
c） 应遵循最小权限原则，确保数据供给方调整策略后的权限不能大于数据所有者授予的权限，防止数据被恶意扩权；
d） 数据供给方调整策略时，需及时通知数据需求方，并在双方协商一致或符合约定条件的情况下执行。

6.3 策略传递

策略传递方面的要求如下：
a） 应由数据供给方或服务方传递策略；
b） 应对数据供给方或服务方进行身份验证，保证策略来源的真实性；
c） 应确保策略与数据同步传递，数据需求方接收策略的时间不能晚于接收数据的时间，并确保策略的完整性；
d） 应确保策略的不可抵赖性，避免数据需求方否认其前序数据供给方所生成的控制策略。

6.4 策略执行

策略执行方面的要求如下：
a） 应由数据需求方执行策略；
b） 数据需求方应确保数据利用行为符合策略要求，包括利用用途、利用方式等与策略要求一致；
c） 应采取技术措施，支撑数据供给方对需求方的策略执行的验证，确保策略在需求方被完整执行；
d） 应对策略执行过程进行存证，确保策略执行过程的可追溯性。

6.5 策略验证

策略验证方面的要求如下：
a） 数据供给方应验证需求方的身份、策略是否完整的被需求方接收；
b） 数据需求方应验证供给方身份的真实性，以及策略内容的完整性和真实性；
c） 二次交易或传播时，原始的数据供给方要能验证新的需求方是否接受了完整的策略，并按策略执行。

7 主要环节的技术要求

7.1 数据收集技术要求

数据收集技术要求旨在确保数据收集活动科学、规范、安全地进行，为后续数据处理与应用提供可靠基础，涵盖收集范围、质量、安全及管理等多方面的技术规范。具体要求包括：
a） 应在数据收集前明确数据的所有权；
b） 应考虑数据来源，明确数据源可靠性、真实性、有效性等；

c） 应考虑数据收集范围，包括收集地点、收集方式、收集数据类型等；
d） 应考虑数据收集后的约束条件，包括权限、用途、期限等。

7.2 数据存储技术要求

数据存储技术要求聚焦于保障数据存储的安全、稳定与高效，通过多种技术手段确保数据在存储期间的质量和可访问性，为数据的有效利用提供支撑。具体要求包括：

a） 应按照存储策略进行数据存储，确保存储设备、存储环境、存储期限等与策略保持一致；
b） 应按照策略保护数据的机密性，包括采用加密、访问控制等确保数据的机密性，防止未经授权的访问；
c） 应按照策略保护数据的完整性；
d） 应按照策略保证数据的可用性，包括采用备份等防止数据丢失或损坏；
e） 宜通过数据分类和分级，明确不同级别数据的保护要求，并采取相应的安全措施。

7.3 数据使用技术要求

数据使用是数据利用管理的核心环节，其技术要求旨在规范数据使用行为，确保数据使用合法合规、安全高效、价值最大化。具体要求包括：

a） 数据被使用前应确认数据需求方的身份及其使用权限；
b） 应按照策略使用数据，确保使用目的、使用方式、使用期限等与策略保持一致；
c） 应按照策略保护数据的机密性，包括采用加密等技术，防止数据泄露；
d） 应按照策略保护数据的完整性，包括采用哈希等对数据完整性进行验证；
e） 应按照策略配置使用环境，包括提供隔离的开发测试环境和生产环境，防止数据泄露。

7.4 数据加工技术要求

数据加工技术要求旨在规范数据加工行为，确保数据加工合法合规、安全高效、质量可靠。具体要求包括：

a） 数据加工前应确认数据加工方的身份及其加工权限；
b） 应按照策略进行数据加工，确保加工用途、加工算法等与策略保持一致；
c） 应考虑数据合规性，对于涉及个人隐私等敏感数据，应采用数据脱敏、加密等技术对敏感数据进行保护，防止敏感数据泄露；
d） 应按照策略配置加工环境，包括提供隔离的开发测试环境和生产环境，防止数据泄露；
e） 应考虑数据加工后的衍生数据的控制策略生成；
f） 应明确衍生数据的分类分级标准，且衍生数据的安全等级不应低于其原始数据的安全等级；
g） 应制定衍生数据的控制策略，策略内容需关联原始数据策略，明确衍生数据的存储期限、使用范围、销毁要求，且策略需经数据供给方确认；
h） 应记录衍生数据与原始数据的血缘关系，包括加工算法、加工时间、操作人员等信息，血缘关系记录需与衍生数据同步存储。

7.5 数据传输技术要求

数据传输技术要求旨在规范数据传输行为，确保数据在传输过程中的安全性、完整性和可靠性。具体要求包括：

a） 数据传输前应确认数据供给方和需求方的身份及其权限；
b） 应按照传输策略对数据进行传输，确保时限、可靠性等与策略保持一致；
c） 传输结束后，数据供给方和需求方应验证数据完整性。

7.6 数据提供技术要求

数据提供技术要求旨在数据提供行为，确保数据在提供过程中的合规性、安全性和有效性。具体要求包括：

a) 数据提供前应确认数据发送方和接收方的身份及其权限，其中数据发送方包括数据供给方或服务方，数据接收方包括数据服务方或需求方；
b) 应按照策略对数据进行提供，确保提供方式、提供对象、提供数据范围等与策略保持一致；
c) 应考虑数据质量，包括在数据提供前进行清洗、标准化，确保数据的准确性、一致性和可理解性。

7.7 数据公开技术要求

数据公开技术要求聚焦于保障数据在公开过程中的安全性、合规性和可用性，通过多种技术手段确保数据在公开期间的完整性、可访问性和可控性。具体要求包括：

a) 数据公开前应对数据供给方进行身份认证，确保其是否具备公开权限，涉及个人信息等敏感数据的，还应验证公开范围是否符合数据主体授权及相关法规要求；
b) 应按照公开策略对数据进行公开，确保公开方式、公开范围、公开对象、公开内容等与策略保持一致。

7.8 数据销毁技术要求

数据销毁技术要求旨在规范数据销毁行为，确保数据彻底销毁，无法恢复，并防止数据泄露和滥用，维护数据主体的合法权益。具体要求包括：

a) 应按照销毁策略对数据进行销毁，确保销毁方式、销毁强度、销毁粒度等与策略保持一致；
b) 应支持多种销毁方式，包括物理销毁（如粉碎、消磁、焚烧等物理手段）、逻辑销毁（如格式化、加密擦除、多轮覆写等技术手段），确保数据的不可恢复性；
c) 应支持销毁验证，对销毁效果进行实时或事后验证，确保数据已被有效销毁，向数据提供方提供销毁记录。

8 通用技术要求

8.1 存证与取证技术要求

8.1.1 存证收集

存证收集主要用于收集数据利用管理各核心组件的操作记录，支撑数据基础设施的采集、汇聚、传输、加工、流通、运营、安全等能力，包括但不限于：

a) 存证收集范围，应考虑覆盖数据利用管理的收集、存储、使用、加工、传输、提供、公开、销毁等主要环节。
b) 存证收集内容，应考虑覆盖数据的供给方、需求方、服务方、监测方等攸关方的操作行为等。
c) 存证收集阶段，应考虑覆盖策略生成、调整、传递、执行、验证等。
d) 数据采集能力的相关存证信息收集，具体如下：
    1) 数据来源相关日志信息，包括提供方信息、来源渠道、合法性证明等；
    2) 数据采集过程相关日志信息，包括采集时间与地点、采集方式与工具、采集日志等；
    3) 数据内容相关日志信息，包括数据分类与分级、数据样本、数据量统计等；
    4) 数据采集的合规性相关日志信息，包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；

5) 数据采集的技术保障相关日志信息，包括数据加密证明、数据完整性证明、系统安全性证明等；
6) 数据采集的审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
7) 数据采集的责任与权限相关日志信息，包括采集人员信息、责任分工、权限管理记录等。

e) 数据汇聚能力的相关存证信息收集，具体如下：
1) 数据来源的审计与监控相关日志信息，包括各数据源信息、提供方信息、来源渠道等；
2) 数据汇聚过程的审计与监控相关日志信息，包括汇聚时间与地点、汇聚方式与工具、汇聚日志等；
3) 数据一致性的审计与监控相关日志信息，包括数据校验信息、数据样本、数据量统计等；
4) 数据汇聚合规性的审计与监控相关日志信息，包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
5) 数据汇聚技术保障的审计与监控相关日志信息，包括数据加密证明、数据完整性证明、系统安全性证明等；
6) 数据汇聚审计与监控的审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
7) 数据汇聚的责任与权限相关日志信息，包括汇聚人员信息、责任分工、权限管理记录等。

f) 数据传输能力的相关存证信息收集，具体如下：
1) 数据传输路径相关日志信息，包括传输起点与终点、传输路径、传输渠道等；
2) 数据传输过程相关日志信息，包括传输时间与地点、传输方式与工具、传输日志等；
3) 数据传输安全性相关日志信息,包括数据加密证明、数据完整性证明、传输协议安全性等；
4) 数据传输合规性相关日志信息,包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
5) 数据传输技术保障相关日志信息，包括传输系统的安全性证明、传输效率与可靠性等；
6) 数据传输审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
7) 数据传输责任与权限相关日志信息，包括传输人员信息、责任分工、权限管理记录等。

g) 数据加工能力的相关存证信息收集，具体如下：
1) 数据来源相关日志信息，包括原始数据来源、提供方信息、来源渠道等；
2) 数据加工过程相关日志信息，包括加工时间与地点、加工方式与工具、加工日志等；
3) 数据变更相关日志信息，包括加工前后的数据样本、数据变更记录、数据量统计等；
4) 数据加工合规性相关日志信息,包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
5) 数据加工技术保障相关日志信息，包括数据加密证明、数据完整性证明、系统安全性证明等；
6) 数据加工审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
7) 数据加工责任与权限相关日志信息，包括加工人员信息、责任分工、权限管理记录等。

h) 数据流通能力的相关存证信息收集，具体如下：
1) 数据来源信息相关日志信息，包括数据提供方信息、来源渠道等；
2) 数据流通路径相关日志信息，包括流通起点与终点、流通路径、流通渠道等；
3) 数据流通过程相关日志信息，包括流通时间与地点、流通方式与工具、流通日志等；
4) 数据流通安全性相关日志信息,包括数据加密证明、数据完整性证明、流通协议安全性等；
5) 数据流通合规性相关日志信息,包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
6) 数据流通技术保障相关日志信息，包括流通系统的安全性证明、流通效率与可靠性等；
7) 数据流通审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
8) 数据流通责任与权限相关日志信息，包括流通人员信息、责任分工、权限管理记录等。

i) 数据利用能力的相关存证信息收集，具体如下：

1） 数据来源相关日志信息，包括数据提供方信息、来源渠道等；
2） 数据利用过程相关日志信息，包括利用时间与地点、利用方式与工具、利用日志等；
3） 数据利用合规性相关日志信息,包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
4） 数据利用安全性相关日志信息，包括数据加密证明、数据完整性证明、利用系统的安全性证明等；
5） 数据利用审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
6） 数据利用责任与权限相关日志信息，包括利用人员信息、责任分工、权限管理记录等；
7） 数据利用技术保障相关日志信息，包括数据备份与恢复、数据生命周期管理等；
8） 数据利用结果相关日志信息，包括利用结果样本、利用结果分析、利用结果应用等。

j） 数据运营能力的相关存证信息收集，具体如下：
1） 数据来源相关日志信息，包括数据提供方信息、来源渠道等；
2） 数据存储与管理相关日志信息，包括存储时间与地点、存储方式与工具、存储日志等；
3） 数据运营合规性相关日志信息,包括用户同意证明、隐私政策、数据脱敏与匿名化证明等；
4） 数据运营安全性相关日志信息，包括数据加密证明、数据完整性证明、运营系统的安全性证明等；
5） 数据运营审计与监控相关日志信息，包括审计日志、监控记录、异常事件处理记录等；
6） 数据运营责任与权限相关日志信息，包括运营人员信息、责任分工、权限管理记录等；
7） 数据运营法律与合同相关日志信息，包括合同与协议、法律合规证明等；
8） 数据运营技术保障相关日志信息，包括数据备份与恢复、数据生命周期管理等；
9） 数据运营应用相关日志信息，包括运营结果样本、运营结果分析、运营结果应用等。

k） 数据安全能力的相关存证信息收集，具体如下：
1） 数据安全策略与制度相关日志信息，包括安全策略文件、安全制度文件、策略与制度的执行记录等；
2） 数据访问控制相关日志信息，包括用户身份信息、用户权限信息、访问日志等；
3） 数据加密与脱敏相关日志信息，包括数据加密证明、数据脱敏与匿名化证明等；
4） 数据完整性保护相关日志信息，包括数据完整性校验记录、数据备份与恢复记录等；
5） 数据安全监控与审计相关日志信息，包括监控日志、审计日志、异常事件处理记录等；
6） 数据安全事件应急响应相关日志信息，包括应急预案文件、应急演练记录、安全事件处理记录等；
7） 数据安全责任与权限相关日志信息,包括安全管理人员信息、责任分工、权限管理记录等；
8） 数据安全法律与合同相关日志信息，包括合同与协议、法律合规证明等；
9） 数据安全技术保障相关日志信息，包括安全系统配置信息、安全评估报告、安全培训记录等。

l） 所有存证日志应基于统一且可信的时间源（如国家授时中心）进行记录，以保证时间一致性。

8.1.2 存证存储

存证存储是对收集的存证信息进行高效的组织管理，支撑存证信息的高效检索和充分利用，包括：

a） 存储方式，本地自存证，或第三方存证等存证类型；
b） 存证完整性，保证收集的存证信息齐全，确保存证信息被成功存储，在丢失或损坏存证信息的情况下从原渠道补全对应的存证信息；
c） 存证机密性，采用访问控制技术控制存证信息的访问主体、访问路径、访问时间、访问的信息数量；采用密码技术对存证信息进行加密防止镜像拷贝、拖库等非法获取；
d） 存证可信性，保证存证信息不被篡改、不被随意删除；

e) 存证可靠性，采用RAID技术或双活等机制，实现存证信息的冗余灾备。

8.1.3 证据生成

证据生成是根据证据服务请求对收集到数据利用管理过程中的存证信息进行检索、数据预处理、证据要素封装、证据链构建的过程，支撑对数据利用管理的操作行为进行合规审计、监管、异常事件分析与溯源等，包括：

a) 证据请求响应，接收请求方的证据获取请求，对请求方进行身份验证，解析证据获取事项的要求；
b) 证据完备性，根据证据获取的要求，对各个存证存储系统中的存证信息进行多源证据查找，获取所有相关证据；
c) 多源证据生成，对查找得到的多源存证信息，按照请求事项和时序进行整理并生成证据，采用数字签名技术实现生成证据的不可篡改和不可否认性；如果有机密性要求，采用请求和响应双方预先约定的协议实现密钥协商和传输加密。

8.2 安全技术要求

安全技术要求为数据利用控制技术的实施提供了基本安全保障。

8.2.1 数据分类分级控制

a) 应基于数据敏感性和业务影响，对数据类别进行划分；
b) 宜实施分类分级控制措施，包括加密存储、禁止明文传输、物理隔离。

8.2.2 身份认证与权限管理

a) 应采用强身份认证机制，确保只有经过授权的用户和系统才能访问和处理数据；
b) 应建立权限最小化和职责分离原则，为用户分配适当的访问权限，防止未授权访问和数据泄露；
c) 数据跨域流通过程中，数据流通参与方，数据处理应用及数据提供方提供的数据均应具有唯一标识确定，标识与参与方、数据应用以及数据资源的对应关系不能被篡改、伪造;
d) 宜支持权限审核功能，定期检查和审计用户权限配置，防止权限滥用和权限泄露；
e) 数据的授权应由所属的数据提供方生成或者以数据提供方认可的方式生成；
f) 在数据访问和利用前，应进行鉴权操作。鉴权操作应具有完整的校验链条，包含但不限于被授权方的身份、数据信息、数据提供方签名等，确保授权信息是由真实的数据提供方签发的且数据的请求内容和授权内容是一致的等；当授权、鉴权操作是计算方平台或数据服务方提供时，要保证授权、鉴权操作不能被数据服务方的内容人员伪造、篡改或绕过。

8.2.3 数据加密与传输安全

a) 数据在使用、存储和传输过程中，应采用国家认可的加密算法进行加密保护；
b) 数据传输应使用安全的传输协议，如SSL/TLS等，确保数据在传输过程中的完整性和机密性；
c) 跨境传输通道应部署数据防泄露系统，阻断未申报的敏感数据出境；
d) 进行数据传输之前，应验证数据接收方身份的真实性，仅当真实性验证通过时才传输数据；
e) 进行数据传输之前，应验证数据接收方环境的安全性，仅当安全性验证通过时才传输数据。

8.2.4 数据审计与监控

a) 应具备审计功能，记录关键操作行为，以便在发生安全事件时进行追溯；

b） 应实时监控数据利用情况，发现异常行为及时报警，并采取相应措施。

8.2.5 数据备份与恢复

a） 应定期对数据进行备份，确保数据在遭受破坏时能够及时恢复；
b） 数据备份应采用加密存储，防止备份数据泄露。

8.2.6 安全合规性

a） 应符合国家相关标准和政策要求；
b） 应定期对数据利用控制技术进行安全评估和合规性检查，确保持续满足安全要求；
c） 向境外提供敏感数据时，应通过国家网信部门安全评估，应采用数据安全和隐私保护技术。

8.2.7 数据安全事件应急响应

a）责任与预案：应明确应急响应责任主体，制定涵盖启动条件、处置流程、资源保障的应急预案；
b)分类与分级：应依据事件影响和危害程度对数据安全事件进行分类与分级（如特别重大、重大、一般），以指导差异化响应；
c)监测与报告：应建立事件监测机制，并规定内部与向上级及监管部门的报告流程、时限与内容；
d)处置与恢复：应能迅速采取隔离、抑制、消除影响等措施，并在事后安全恢复数据与业务，全过程需记录留痕；
e)复盘与改进：事件处置后应进行复盘，分析根源并整改，同时定期开展应急演练以持续优化机制。

8.3 运营技术要求

8.3.1 运营分析

a） 应对数据利用管理的运营数据进行分析，包括数据使用量、用户活跃度、服务调用次数等；
b） 宜评估数据利用管理的经济效益和社会效益，为运营决策提供依据；
c） 宜根据经营分析结果优化数据利用管理的技术和流程，提升运营效率和效益。

8.3.2 运营监测

a） 应明确运营监测的主体，包括数据管理部门、业务部门、安全管理部门等；
b） 应对数据利用管理的各个环节进行监测，包括数据质量、数据安全、服务质量、用户满意度等；
c） 应部署实时监控组件，对数据异常利用行为进行告警并记录审计日志；
d） 宜采用技术手段和管理手段相结合的方式，实现对数据利用管理的全方位监测；
e） 宜支持集群资源弹性扩展，节点故障时可自动迁移服务；
f） 可在日常运维中配置多级故障响应机制。

附 录 A
（资料性）
DUMM 利用方法

A.1 概述

本附录给出了数据利用管理模型的一般描述，以及在三种典型场景下的使用方法。

A.1.1 DUMM一般描述

DUMM包含供给方、需求方、监测方和服务方，涉及数据利用管理过程中的收集、存储、使用、加工、传输、提供、公开、销毁等主要环节，并借助数据利用的控制策略生成、调整、传递、执行、验证等步骤予以实现。其一般描述如图4所示。

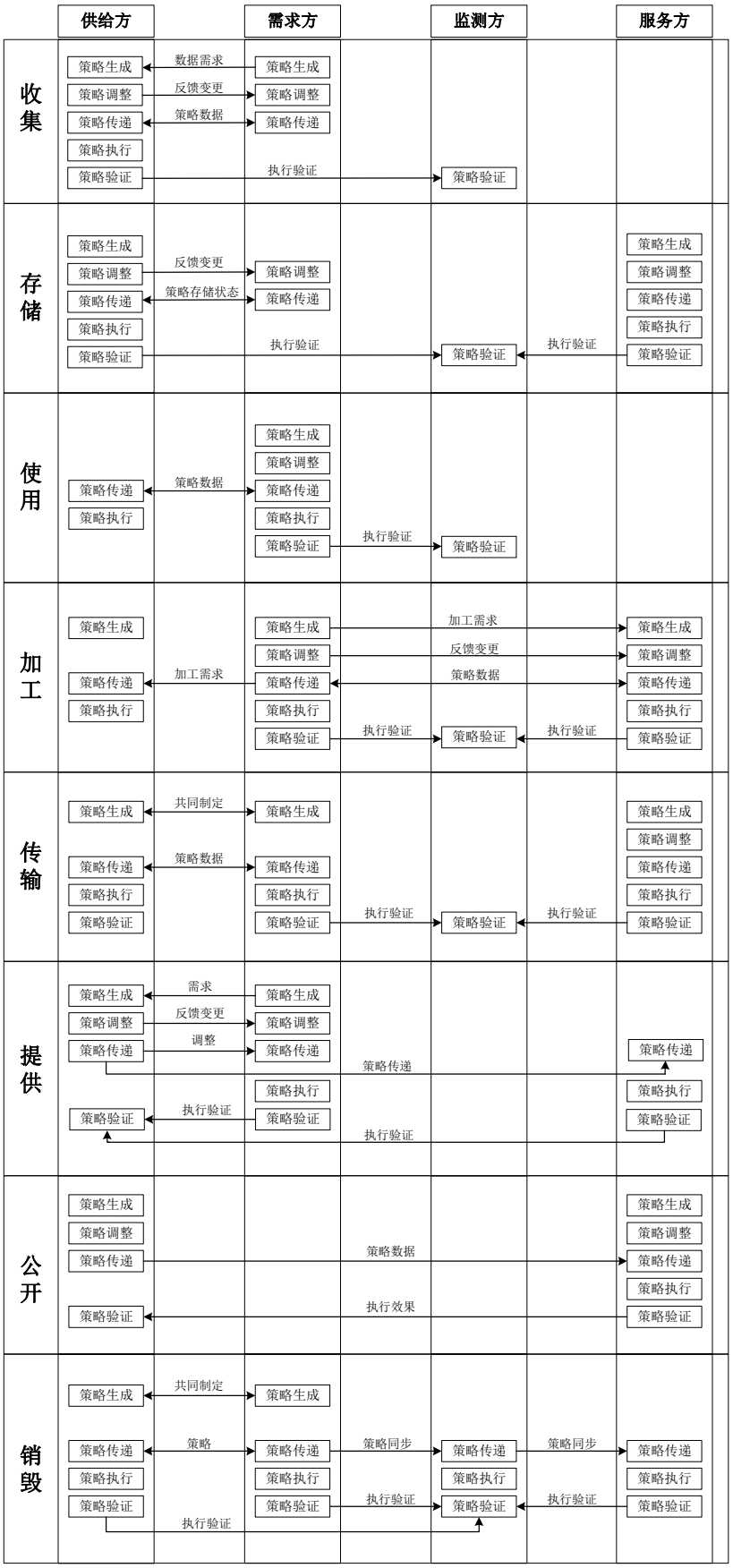

图4　DUMM 的一般描述方法

A.1.2 域内数据利用场景

域内数据利用是指数据供给方在域内完成数据采集、存储、使用、销毁等环节的数据利用场景。部门作为监测方，制定存储安全监测策略，运用工具监测存储设备、加密及期限等情况，验证监测效果。数据服务方为平台内部存储技术团队或外部提供商，基于数据规模、性能与成本生成存储架构、设备选型及备份策略，执行存储架构搭建与数据备份等操作，配合监测方验证以优化服务。

在使用环节，市场部、运营部等数据需求方根据营销活动与商家运营评估需求生成利用策略，组织执行人员合法合规使用数据，通过营销转化率与商家满意度调查验证效果。数据安全与合规部门作为监测方，制定数据使用合规性监测策略，依法规与内部政策调整后传达，监测使用过程，验证监测方法对违规行为的发现能力。数据服务方若为数据分析工具提供商或数据咨询机构，基于平台业务生成工具使用与咨询服务策略，按业务、工具变化或用户反馈调整后传递给需求方与监测方，执行服务操作，配合监测方验证以优化服务。

在加工环节，平台内各业务部门作为数据需求方，基于精准用户画像与准确商家绩效评估需求生成加工策略，画像不准确或绩效评估不符时调整策略并传达给加工执行团队与监测方对比验证加工策略。数据安全部门作为监测方，制定数据加工合规性与质量监测策略，验证监测方法对数据质量问题的发现能力。数据服务方为平台内部数据科学团队或外部加工服务提供商，按技术、业务变化或需求方反馈调整后传递给需求方与监测方，执行数据加工操作，配合监测方验证以改进加工工作。

在提供环节，平台商家作为数据需求方，根据店铺运营需求向平台提出数据需求，参与制定数据提供策略，店铺业务变化时调整需求促使平台调整策略，接收平台传达的策略后按要求获取利用数据，验证数据准确性与完整性。平台内部负责商家服务质量监督的部门作为监测方，制定数据提供合规性与服务质量监测策略。平台内部负责数据报告生成与分发的团队作为数据服务方，基于平台与商家协议、数据存储结构生成数据报告生成、分发及查询接口设计策略，按平台业务、商家需求或技术升级调整后传递给商家与监测方，执行数据报告生成、分发与接口维护操作，配合监测方验证。

在销毁环节，平台内各业务部门作为数据需求方，生成销毁策略，如确定销毁数据范围、方式，随法规或业务调整策略后传达给销毁执行团队与监测方，监督销毁执行，通过数据恢复检测验证销毁效果。数据安全部门作为监测方，制定数据销毁安全与合规监测策略，依法规调整后传达，监测销毁过程，验证监测方法对数据彻底销毁的检测能力。平台内部负责数据销毁的技术团队作为数据服务方，基于平台数据存储情况生成销毁技术方案，按法规、业务变化或需求方反馈调整后传递给需求方与监测方，执行数据销毁操作，配合监测方验证以改进销毁工作。

A.1.3 单向数据流通场景

单向数据流通是指数据供给方仅向数据需求方提供数据的场景。以金融领域为例，数据供给方可能是大型商业银行，拥有海量客户的交易流水、信用评级、资产状况等数据。数据需求方是金融科技公司，专注于开发创新的信贷风险评估模型。银行出于拓展业务合作、优化资源配置等目的，与金融科技公司达成数据交易协议。

在收集环节，银行作为数据供给方，依据金融科技公司构建风险评估模型的需求，生成数据收集策略。确定收集符合特定信用评级范围、一定时间跨度内的客户交易流水及资产信息等数据，以满足模型对数据全面性与准确性的要求。在收集过程中，严格遵循相关金融数据保护法规，确保数据来源合法合规。

在存储环节，银行采用安全可靠的加密存储技术，将收集到的数据存储于专业的金融级存储设备中，设定合理的数据存储期限，既满足业务合作期间的数据利用需求，又符合监管部门对数据留存的规定。当数据需求方，即金融科技公司需要利用数据时，依据双方约定生成策略，明确数据仅用于内部信贷风险评估模型的研发与优化，限定利用人员为模型研发团队成员，并规定数据利用频率，如每周进行一次大规模数据分析。

若数据需要进一步加工，金融科技公司或委托专业的数据服务机构生成加工策略。例如，对原始的客户交易流水数据进行清洗，去除异常值与重复数据，构建复杂的风险评估模型框架，确定模型参数与算法流程等。在数据传输过程中，银行与金融科技公司共同制定传输策略，采用加密性能卓越的传输协议，如 SSL/TLS 协议，选择安全稳定的网络传输路径，确保数据在传输过程中的保密性、完整性与可用性，防止数据被窃取或篡改。

当银行按照约定时间、格式，如以 CSV 格式按时向金融科技公司提供数据时，严格执行提供策略。在整个数据交易流程中，数据监测方，如金融监管部门下属的数据监管机构，密切关注各环节策略的执行情况。从数据收集的范围合规性，到存储的安全性、利用的合法性、加工的规范性、传输的安全性以及提供的准确性等方面，进行全方位的验证。确保数据供给方与需求方的交易活动符合金融行业的数据管理规范与法律法规要求，维护金融市场的数据安全与稳定秩序。

在传输环节，银行与金融科技公司会进一步细化策略。传输前，双方共同评估数据体量与紧急程度，若数据量庞大且对时效性要求高，可选择带宽充足、稳定性强的专线网络作为传输路径，同时配置高性能的网络传输设备，确保数据能够快速传输。银行会对要传输的数据进行预处理，添加数字签名，以便金融科技公司接收数据后进行完整性校验。

在销毁环节，银行与金融科技公司依据相关金融法规和双方协议，确定销毁时间。银行针对存储数据的金融级存储设备，采用专业的数据销毁软件，按照多次覆写、随机填充等安全算法对数据进行销毁操作，确保数据无法恢复。金融科技公司则对其接收并利用过数据的本地存储设备和工作电脑进行同样严谨的销毁处理。销毁完成后，双方各自留存详细的销毁记录，包括销毁时间、操作人员、销毁设备型号以及数据销毁软件的操作日志等。数据监测方会对销毁过程进行严格审查，通过专业的数据恢复工具对双方销毁后的存储介质进行检测，确认数据已被彻底销毁，以保障金融数据的安全性与合规性，维护金融市场的稳定运行。

A.1.4 多方联合利用场景

多方联合利用是指多个参与方既作为数据供给者提供原始数据，又作为数据需求者使用联合利用结果的场景。以联邦学习场景为例，数据利用管理的技术要求涉及多个环节，包括数据收集、存储、使用、加工、传输、提供和销毁。该场景下涉及多个参与方，每个参与方在不同的环节下所属的角色不同。以金融领域风险评估为例，各个银行作为参与方，拥有海量客户的交易流水、信用评级、资产状况等数据。其希望在已有数据不出域的前提下，基于各个单位的数据共同构建更准确的风险评估模型。

在收集环节，金融监管部门作为监测方，各个银行作为数据供给方，依据联邦学习模型的需求，银行生成数据收集策略。收集策略包括但不限于：收集数据的类型、范围和格式等。在收集过程中，各参与方需严格遵循数据保护等法规，确保数据来源合法合规，并采用差分隐私技术对敏感数据进行匿名化处理，以保护用户隐私。

在存储环节，金融监管部门作为监测方，各个银行作为数据供给方，依据国家和监管部门的数据存储要求，银行生成数据存储策略。存储策略包括但不限于：数据存储的位置、存储方式、存储期限、存储时的安全措施、备份策略等。银行执行存储策略，并进行策略验证。金融监管部门对银行的数据存储行为进行存证。

在使用环节，金融监管部门作为监测方，各个银行作为数据供给方，同时也是数据需求方，依据国家和监管部门的数据利用要求，生成数据利用策略。利用策略包括但不限于：使用的数据范围、期限、目的、方式、频率、人员、安全性要求等。银行利用本地存储的数据，在本地模型进行训练，执行策略。例如，对原始数据进行清洗、去重、归一化等预处理操作，并将处理后的数据作为模型的输入，进行模型训练。金融监管部门对银行的数据利用行为进行存证。

在加工环节，各个银行作为数据供给方，某算力平台作为服务方，金融监管部门作为监测方。各个银行依据国家和监管部门的数据加工要求，生成数据加工策略。加工策略包括但不限于：需求方、加工

需求、范围、方式、期限、用途。并将生成的策略传递至算力平台进行确认，经过策略调整后生成最终的策略。算力平台执行策略，对数据进行加工。金融监管部门对算力平台的数据加工行为进行存证。

在传输环节，某算力平台作为数据供给方，主要涉及模型参数的传输，各个银行作为数据需求方，金融监管部门作为监测方。算力平台生成数据传输策略，该策略包括但不限于：传输数据、带宽、协议、方式、时间、路径、接收方等。金融监管部门对算力平台的数据加工行为进行存证。

在提供环节，各个银行作为数据供给方，主要涉及提供更新后的模型参数，某算力平台作为服务方，金融监管部门作为监测方。银行依据国家和金融监管部门的数据提供要求，生成数据提供策略。提供策略包括但不限于：提供数据的范围、方式、时间、用途等。银行执行策略。算力平台对策略进行验证。金融监管部门对银行的提供行为进行存证。

在销毁环节，各个银行作为数据供给方，某算力平台作为服务方，金融监管部门作为监测方。银行生成数据销毁策略，销毁策略包括但不限于：数据销毁的范围、时间、方式等。算力平台执行销毁策略，并由银行进行策略验证。金融监管部门对算力平台的销毁过程进行存证。

附 录 B
（资料性）
国家数据基础设施相关业务功能与本文件各环节的关系

《国家数据基础设施建设指引》（后续简称《指引》）明确了国家数据基础设施具备数据采集、汇聚、传输、加工、流通、运营、安全等能力，这些能力在推动数据的有效管理与利用中发挥着关键作用。以下是对相关能力的详细阐述：

a） 数据采集：主要通过传感器、业务系统等多样化手段，实现对相关数据的采集工作，为后续的数据处理提供基础来源。

b） 数据汇聚：借助标识编码解析、数据目录等技术，实现对数据的高效接入、合理编目，达成数据的广泛汇聚、存储以及发布，提升数据的组织与管理效率。

c） 数据传输：具备支持节点即时组网和数据高效传输的能力，保障数据在不同节点间的顺畅流转。

d） 数据加工：为参与方提供高效便捷且安全可靠的数据清洗、计算服务，同时建立数据质量控制和评估机制，显著提高数据处理环节的效率和质量。

e） 数据流通：运用数据分类分级策略，实现数据的共享、交易等流通功能，为不同行业、地区和机构营造可信的流通环境。

f） 数据运营：涵盖数据登记、监督管理、数据认证、合规保障等功能，有力支撑全国一体化数据市场的有序运行。

g） 数据安全：提供动态全过程的数据安全服务，包括防窃取、防泄露、防滥用、防破坏等，确保数据在全生命周期内的安全性。

《指引》中的业务功能	对应本文件的数据利用环节	关联解释
采集	收集	《指引》中的数据采集环节，与本文件的数据收集环节相对应。二者均聚焦于从各类数据源获取数据，在实际操作中，数据采集环节获取的数据为数据收集提供了原始素材，而本文件的数据收集在此基础上，更强调依据业务需求、法律法规等进行科学规范的收集，确保收集范围的精准性、数据质量的可靠性以及收集过程的安全性
汇聚	存储	数据汇聚主要负责将采集到的数据进行整合、编目和存储，本文件的数据存储环节则在此基础上，进一步强调存储的安全性、稳定性和高效性。通过实施严格的访问控制策略、采用安全的存储介质和备份策略等措施，保障数据在存储期间的质量和可访问性，为数据的有效利用提供坚实支撑
传输	传输	《指引》中的数据传输与本文件的数据传输环节高度契合，均致力于确保数据在不同设备或系统之间的高效、安全传输。在实际应用中，二者都需采用标准化传输协议、保障数据的完整性和可用性，并不断优化传输效率，以满足数据快速流通的需求
加工	加工	数据加工环节，二者都强调为参与方提供数据处理服务，提升数据质量和价值。《指引》侧重于提供高效的计算服务和质量控制能力，本文件则从加工流程、算法、验证等

		多方面进行规范，确保数据加工合法合规、安全高效、质量可靠，使加工后的数据能够更好地满足业务需求
流通	使用、提供、公开	《指引》的数据流通功能通过分类分级策略实现数据共享、交易，而本文件的数据使用、提供和公开环节则是数据流通的具体体现形式。数据使用强调在本地使用数据时的合规性、安全性和有效性，数据提供强调向其他系统、应用程序或实体传输数据时的合规性、安全性和有效性，数据公开则侧重于保障数据在公开过程中的安全性、合规性和可用性
运营	收集、存储、加工、使用、传输、提供、公开、销毁	数据运营功能广泛涉及数据管理的各个方面，与本文件的多个环节密切相关。在数据收集、存储、加工、使用、传输、提供、公开、销毁等环节中，运营通过数据登记、监督管理、数据认证、合规保障等措施，确保各环节有序进行，有效支撑全国一体化数据市场的有序运行，保障数据处理活动的合规性和可持续性
安全	收集、存储、加工、使用、传输、提供、公开、销毁	数据安全贯穿于数据利用的全过程，在数据收集、存储、加工、使用、传输、提供、公开、销毁等各个环节，都需要采取相应的安全措施，如数据加密、访问控制、审计监控等，防止数据被窃取、泄露、滥用和破坏，确保数据在全生命周期内的安全性，维护数据主体的合法权益

通过明确《指引》中的业务功能与本文件各环节的对应关系，有助于各相关方更好地理解和应用国家数据基础设施的能力，在遵循本文件的基础上，实现数据的科学管理与高效利用，推动数字经济的健康发展。

参 考 文 献

[1]中华人民共和国数据安全法（2021年6月10日第十三届全国人民代表大会常务委员会第二十九次会议通过）

[2]中华人民共和国网络安全法（2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过）

[3]中华人民共和国个人信息保护法（2021年8月20日十三届全国人大常委会第三十次会议通过）

[4]国家数据基础设施建设指引（2024年12月31日，国家发展改革委、国家数据局、工业和信息化部联合发布）

[5] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

[6] GB/T 35273—2020 信息安全技术 个人信息安全规范

[7] 李凤华,李晖,牛犇,等.数据要素流通与安全的研究范畴与未来发展趋势[J].通信学报,2024,45(05):1-11.

[8] “国家数据局发布《数据领域常用名词解释》（第一批）”