ICS 35.080
CCS L 77

DB52

贵 州 省 地 方 标 准

DB52/T 1557—2021

大数据开放共享安全管理规范

Security management specification for opening and sharing of big data

2021－01－14 发布　　2021－05－01 实施

贵州省市场监督管理局　　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。

本文件由贵州航天计量测试技术研究所提出。

本文件由贵州省大数据标准化技术委员会归口。

本文件起草单位：贵州航天计量测试技术研究所、贵州大学、贵州省机械电子产品质量监督检验院、贵州财经大学、贵州省保密技术检查中心、贵州医科大学附属医院、贵州中软云上数据技术服务有限公司。

本文件主要起草人：潘积文、陈永久、杨玉龙、彭长根、丁红发、郑少波、朱义杰、田有亮、李明贵、禹忠、邓迪、杨大刚、姜龙、李帅、冯迪、黄克敏、魏自强、关艳梅、韦超。

大数据开放共享安全管理规范

1 范围

本文件规定了大数据开放共享安全管理总体要求、数据流通过程、数据开放安全管理和数据共享安全管理。

本文件适用于大数据开放共享的安全管理。

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（包括所有的修订单）适用于本文件。

GB/T 22239 信息安全技术 网络安全等级保护基本要求

GB/T 35295 信息技术 大数据 术语

3 术语和定义

GB/T 35295 界定的以及下列术语和定义适用于本文件。

3.1

数据资源 data source

数据提供方在履行职责、业务处理、日常管理等过程中依法采集、生成、存储、管理的各类不宜公开的数据，不含涉密数据和公开数据。

3.2

数据开放 data open

数据提供方在安全保密、公共利益导向前提下，面向数据接收方以非排他形式提供数据资源的行为。

3.3

数据共享 data share

数据提供方因履行职责、公共利益需要，经与数据接收方磋商，向数据接收方提供数据资源的行为。

3.4

数据提供方 data provider

基于数据流通平台，向其他政府部门、团体机构、企事业单位或公众提供数据资源的实体。

注：包括政府部门、团体机构、企事业单位或公众。

3.5

数据接收方 data receiver

使用数据资源的实体。

注：包括政府部门、团体机构、企事业单位或公众。

3.6

数据流通 data flow

参与开放、共享的数据资源作为流通对象，按照一定的规则从数据提供方传递到数据接收方的过程。

3.7

数据流通平台 data flow platform

用于数据流通的信息管理服务平台，包含承载数据资源的各业务系统。

3.8

数据流通服务机构 data flow service

负责数据流通的日常管理、业务流转、运行维护等经营活动的组织。

4 总体要求

4.1 安全原则

数据流通应遵循以下原则：

a) 责任共担原则：数据流通服务机构、数据提供方、数据接收方对数据流通过程及结果负责，共同确保数据流通的安全。
b) 合法合规原则：数据流通应遵从数据安全管理的相关法律法规、合同、标准等，遵守社会公德，不得损害国家利益、社会公共利益和他人合法权益。
c) 责任权属原则：数据提供方对数据负责，数据流通过程中，责任不随数据转移而转移。
d) 最小授权原则：在保证数据流通完整实现的基础上，数据流通过程中各参与方具备最小操作权限，确保非法用户或异常操作所造成的损失最小。
e) 数据安全原则：数据流通服务机构应确保数据流通平台的安全控制措施和策略有效，保护数据生命周期的安全。
f) 安全审计原则：对数据流通平台的每次数据流通行为进行记录，确保可追溯可审查。

4.2 机构要求

数据流通服务机构应满足以下要求：

a) 为无违法违规记录的境内合法组织机构；
b) 得到相关行政或主管部门的授权或许可；
c) 具备承担数据流通服务相对应的安全保障能力；
d) 将从事境内数据流通服务的数据流通平台部署在我国境内；

e） 数据流通服务机构职责：组织、协调和指导数据流通平台的建设、使用和开发工作；组织对数据流通平台的安全检查和风险评估；监督和指导数据流通的日常管理、业务流转、运行维护等经营活动；对数据流通参与方的注册信息进行审核；审查和确定数据流通平台用户的行为和权限；建立和执行针对数据流通各参与方的安全监管、审计制度和流程；建立和执行针对数据销毁的安全监管、审计制度和流程。

4.3 人员要求

数据流通服务机构应满足以下要求：

a） 建立数据流通安全领导小组，由机构最高管理者或授权代表担任组长；
b） 建立数据流通安全管理职能部门，设立安全管理负责人岗位，明确安全责任；
c） 设立数据流通系统管理员、安全管理员、安全审计员等岗位，明确各岗位的安全职责；
d） 对数据流通重要岗位人员进行安全审查和技术考核，确保无违法违规记录；
e） 对数据流通重要岗位人员签署安全保密协议，与重要岗位人员签署岗位责任协议；
f） 对数据流通各类岗位人员制定和实施培训计划，培训内容包括安全意识、专项技能等，具备与岗位要求相适应的安全管理知识和专业技术水平；
g） 对第三方人员进行安全管理，对于可能接触流通数据的第三方人员，签署安全保密协议。

4.4 制度要求

数据流通服务机构应满足以下要求：

a） 根据数据流通的安全需求和安全目标，结合自身实际情况，制定明确的数据流通安全管理策略；
b） 建立和执行安全责任制度，实行领导责任制，明确各岗位应承担的责任和义务；
c） 建立和执行安全工作制度，包括人员、物理设施与环境、运行与开发、数据安全和个人信息安全保护等；
d） 为数据流通管理人员或操作人员执行的管理或业务操作建立操作规程；
e） 定期对数据流通服务安全管理策略、制度和规程进行评审，并及时进行更新。

5 数据流通

5.1 数据开放

数据开放服务参考框架如图1所示。数据开放涉及到数据提供方、数据接收方和数据流通服务机构。数据流通服务机构依托数据流通平台，制定数据流通安全管理保障措施，为数据提供方、数据接收方提供数据开放服务。数据开放包括数据准备、数据发布和开放结束。

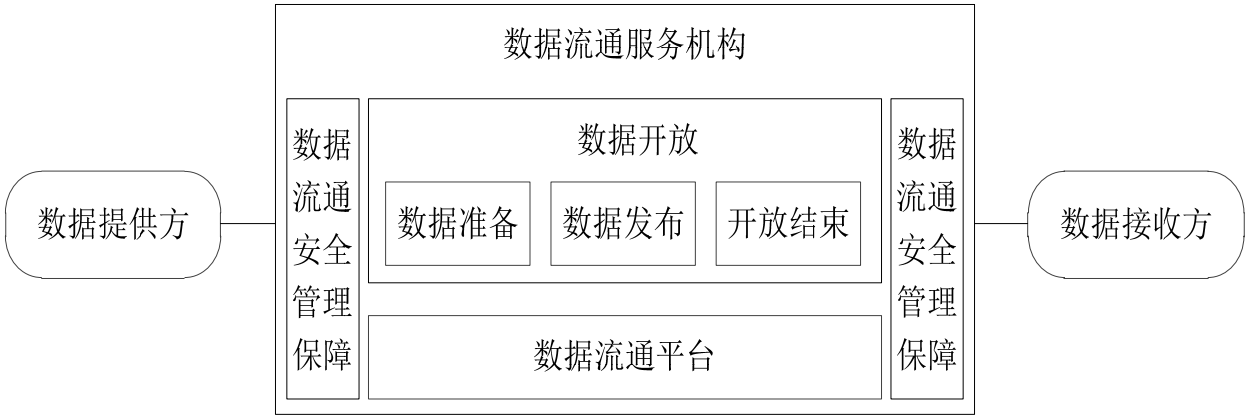

图 1　数据开放服务参考框架

5.2　数据共享

数据共享服务参考框架如图2所示。数据共享涉及到数据提供方、数据接收方和数据流通服务机构。数据流通服务机构依托数据流通平台，制定数据流通安全管理保障措施，为数据提供方、数据接收方提供数据共享服务。数据共享包括数据准备、共享磋商、共享实施和共享结束。

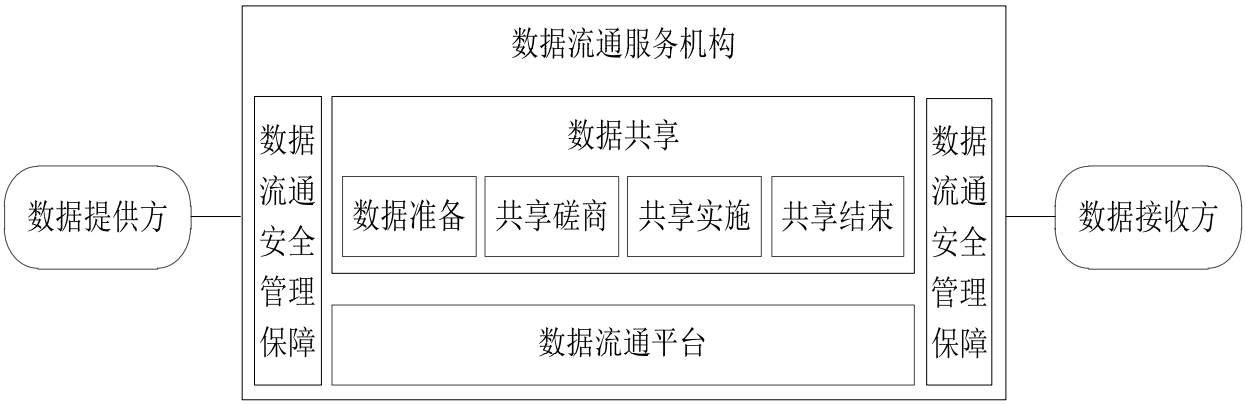

图 2　数据共享服务参考框架

6　数据开放安全管理

6.1　数据准备

6.1.1　数据提供方要求

数据提供方应满足以下要求：

a)　为无违法犯罪记录的境内合法组织或自然人；

b)　完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；

c)　遵守数据流通服务机构的安全管理制度和流程。

6.1.2　数据安全

6.1.2.1 数据安全要求

参与开放的数据应满足以下要求：

a) 应确保通过合同或其他诸如强制的内部策略等明确界定数据接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平；
b) 应采用防计算机病毒系统对数据进行安全性扫描，确保数据的安全可靠；
c) 应是真实可靠的数据，不应有蓄意伪造、篡改等造成数据污染的行为；
d) 不应携带涉密、商业秘密、隐私等敏感信息及违法信息。

6.1.2.2 数据分类要求

应对开放数据进行分类，数据分类应满足以下要求：

a) 数据分类应易于理解；
b) 应形成文档化的数据分类条目，便于查询。

6.1.3 访问控制策略

6.1.3.1 策略制定

应根据数据提供方数据开放的需求和目标，结合数据接收方的实际需求，按照最小授权原则，制定明确的数据开放访问控制策略。

6.1.3.2 策略更新

应根据数据提供方数据开放的需求和目标、数据接收方的需求、数据流通平台的变化情况，及时调整现有的访问控制策略，动态保障数据流通平台的访问权限。

6.1.4 方案设计要求

数据流通服务机构进行数据开放应制定详细方案，方案设计应满足以下要求：

a) 方案设计前应进行安全性及数据泄露风险评估，根据评估结果确定应采取的保护措施；
b) 应自行或组织具有相应能力的承建单位承担数据开放方案的设计；
c) 应联合数据提供方对设计方案进行审查论证。

6.2 数据发布安全

6.2.1 数据流通平台安全

数据流通平台应满足以下要求：

a) 符合 GB/T 22239 中第 3 级的相关安全要求；
b) 采用的密码技术应遵循相关国家标准和行业标准。

6.2.2 数据传输安全

数据传输应满足以下要求：

a) 应对数据接收方进行身份鉴别；
b) 应采用密码技术进行数据传输保护，采用的密码技术应遵循相关国家标准和行业标准。

6.2.3 数据安全审计

数据开放过程应满足以下安全审计要求：

a) 应制定文档化的明确的数据发布安全审计策略，策略应根据数据发布的变化情况动态更新；
b) 安全审计应与数据安全、访问控制等安全功能的设计紧密结合，针对数据开放过程中的可审计事件产生审计记录；
c) 审计记录应包括以下内容：事件发生的时间、地点、类型、主体、客体和结果（成功或失败）；
d) 应对已存储的审计记录进行保护，能检测或防止对审计记录的修改和伪造；
e) 审计记录应长期保存；
f) 应定期对审计记录进行审查或分析，调查可疑行为及违规操作，采取相应的措施，并及时报告。

6.2.4 数据权属明确

数据开放过程中，应明确数据权属不变，仍为数据提供方所有，数据转移过程中应遵循责任权属原则。

6.2.5 数据开放期限

数据流通服务机构与数据提供方应约定数据开放期限。

6.3 开放结束

6.3.1 数据接收方要求

数据接收方应满足以下要求：
a) 应为无违法犯罪记录的境内合法组织或自然人；
b) 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；
c) 应证明其具备对开放数据实施安全保护的能力；
d) 应提供书面的数据开放和使用安全承诺，内容包括但不限于：遵守数据开放安全原则，愿意接受数据流通服务机构安全监督，遵从数据提供方提出的数据安全要求，对所持有数据提供充分的安全保护，未经明确授权不公开或转交数据给第三方，未经明确授权不应转移或携带数据出境，不用于违法犯罪用途等。

6.3.2 数据销毁要求

数据销毁应满足以下要求：
a) 数据流通平台在按照数据开放规则完成数据开放后，应及时销毁开放数据；
b) 数据流通平台应长期保留数据开放日志记录，以备数据溯源。

7 数据共享安全管理

7.1 数据准备

7.1.1 数据提供方要求

数据提供方应满足以下要求：
a) 为无违法犯罪记录的境内合法组织或自然人；
b) 完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；
c) 遵守数据流通服务机构的安全管理制度和流程。

7.1.2 数据安全

7.1.2.1 数据安全要求

参与共享的数据应满足以下要求：

a) 应确保通过合同或其他诸如强制的内部策略等明确界定数据接收方接收的数据范围和要求，确保其提供同等或更高的数据保护水平；
b) 应采用防计算机病毒系统对数据进行安全性扫描，确保数据的安全可靠；
c) 应是真实可靠的数据，不应有蓄意伪造、篡改等造成数据污染的行为；
d) 不应携带涉密、商业秘密、隐私等敏感信息及违法信息。

7.1.2.2 数据分类要求

应对共享数据进行分类，数据分类应满足以下要求：

a) 数据分类应易于理解；
b) 应形成文档化的数据分类条目，便于查询。

7.1.3 访问控制策略

7.1.3.1 策略制定

应根据数据提供方数据共享的需求和目标，结合数据接收方的实际需求，按照最小授权原则，制定明确的数据共享访问控制策略。

7.1.3.2 策略更新

应根据数据提供方数据共享的需求和目标、数据接收方的需求、数据流通平台的变化情况，及时调整现有的访问控制策略，动态保障数据流通平台的访问权限。

7.1.4 方案设计要求

数据流通服务机构进行数据开放应制定详细方案，方案设计应满足以下要求：

a) 方案设计前应进行安全性及数据泄露风险评估，根据评估结果确定应采取的保护措施；
b) 应自行或组织具有相应能力的承建单位承担数据共享方案的设计；
c) 应联合数据提供方对设计方案进行审查论证。

7.2 数据共享磋商

7.2.1 共享磋商要求

数据共享磋商应满足以下要求：

a) 数据提供方、数据接收方应对共享数据的用途、使用范围、共享方式和使用期限等协商和约定，形成共享合同；
b) 数据流通服务机构应对共享合同从数据流通安全、个人信息保护安全等方面进行审核，确保满足合规性要求，撤销不符合要求的共享合同；
c) 数据流通服务机构应对审核通过的合同进行登记备案，并对数据提供方、数据接收方发出合同确认通知。

7.2.2 数据共享承诺

数据共享承诺应满足以下要求：

a) 数据提供方、数据流通服务机构、数据接收方在启动数据共享流程前应签订书面的数据共享和使用安全承诺；
b) 安全承诺内容包括但不限于：遵守数据共享安全原则，数据流通服务机构愿意接受数据提供方的安全监督，数据接收方愿意接受数据流通服务机构安全监督，遵守数据提供方提出的数据安全要求，对所持有数据提供充分的安全保护，未经明确授权不公开或转交数据给第三方，未经明确授权不应转移或携带数据出境，不用于违法犯罪用途等。

7.3 数据共享安全

7.3.1 数据流通平台安全

数据流通平台应满足以下要求：
a) 符合 GB/T 22239 中第 3 级的相关安全要求；
b) 采用的密码技术应遵循相关国家标准和行业标准。

7.3.2 数据传输安全

数据传输应满足以下要求：
a) 应对数据接收方进行身份鉴别；
b) 应采用密码技术进行数据传输保护，采用的密码技术应遵循相关国家标准和行业标准。

7.3.3 数据安全审计

数据共享过程应满足以下安全审计要求：
a) 应制定文档化的明确的数据共享安全审计策略，策略应根据数据共享的变化情况动态更新；
b) 安全审计应与数据安全、访问控制等安全功能的设计紧密结合，针对数据共享过程中的可审计事件产生审计记录；
c) 审计记录应包括以下内容：事件发生的时间、地点、类型、主体、客体和结果（成功或失败）；
d) 应对已存储的审计记录进行保护，能检测或防止对审计记录的修改和伪造；
e) 审计记录应长期保存；
f) 应定期对审计记录进行审查或分析，调查可疑行为及违规操作，采取相应的措施，并及时报告。

7.3.4 数据权属明确

数据共享过程中，应明确数据权属不变，仍为数据提供方所有，数据转移过程中应遵循责任权属原则。

7.4 共享结束

7.4.1 数据接收方要求

数据接收方应满足以下要求：
a) 应为无违法犯罪记录的境内合法组织或自然人；
b) 应完成在数据流通服务机构的注册，并经数据流通服务机构审核通过；
c) 应证明其具备对共享数据实施安全保护的能力；
d) 在按照数据共享规则完成数据使用后，应及时销毁共享数据。

7.4.2 数据销毁要求

数据销毁应满足以下要求：

a） 数据流通平台在按照数据共享规则完成数据共享后，应及时销毁共享数据；
b） 数据流通平台应长期保留数据共享日志记录，以备数据溯源。

参 考 文 献

[1] GB/T 25070—2019 信息安全技术 网络安全等级保护安全设计技术要求

[2] GB/T 37932—2019 信息安全技术 数据交易服务安全要求

[3] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[4] 《中华人民共和国网络安全法》中华人民共和国主席令第五十三号

[5] 《关于加强国家网络安全标准化工作的若干意见》中网办发文〔2016〕5 号

[6] 《国务院关于印发促进大数据发展行动纲要的通知》国发〔2015〕50 号