

DB4403

深圳市地方标准

DB4403/T XXX—XXXX

智慧城市数据账户资源共享应用规范

Application specification for resource sharing of data account for smart
city

(送审稿)

XXXX-XX-XX 发布

XXXX-XX-XX 实施

深圳市市场监督管理局 发布

目 次

前言	II
引言	III
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 数据账户资源应用框架	3
5 数据账户相关方及业务活动	5
6 数据账户关键业务流程	13
7 数据账户资源共享应用要求	15
8 安全要求	19

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。

本文件由深圳市政务服务和数据管理局提出并归口。

本文件起草单位：深圳市政务服务和数据管理局、深圳市龙华区政务服务和数据管理局、深圳市标准技术研究院、深圳市智慧城市科技发展集团有限公司、深圳市腾讯计算机系统有限公司、深圳市华傲数据技术有限公司、平安科技（深圳）有限公司、深圳市安证企业合规管理（集团）有限公司、深圳市前海数据服务有限公司、深圳莱拉科技有限公司、华为技术有限公司、深圳市聚龙智慧城市研究院、深圳市三希软件科技有限公司、腾讯云计算（北京）有限责任公司。

本文件主要起草人：张永昌、胥少卿、高杰、杜佳、杨舸、王刚、伍可、胡瀛、吴仪、王永霞、代威、何旭珩、孙汀、江鑫、蔡玉娟、刘国光、崔昊、吕令广、杨在文、胡林红、辛鹏。

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，为充分发挥海量数据规模和丰富应用场景优势，为智慧城市提供合规、安全、可信、可追溯的数据应用服务，本文件以公共基础信息库、数据共享平台、数据开放平台、数据授权运营平台等作为数据来源，以公共机构、企业、个人等为实体构建公共机构数据账户、企业数据账户、个人数据账户等类型数据账户，将公共数据、企业数据、个人数据经过归集融合形成数据账户资源，在数据账户平台提供的用户管理、权限管理、资源管理、授权管理、场景和供需管理、安全合规管理等功能模块支撑下，为智慧城市应用场景提供高效、安全、有序、精准的数据共享、开放、运营、交易等的应用服务。

智慧城市数据账户资源共享应用规范

1 范围

本文件规定了智慧城市中数据账户资源应用框架、数据账户相关方及业务活动、数据账户关键业务流程、数据账户资源共享应用要求及安全要求。

本文件适用于在智慧城市中以公共机构、企业、个人为实体的数据账户及其相关业务活动、管理及共享应用。其他类型数据账户可参考使用。

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 34960.5 信息技术服务 治理 第5部分：数据治理规范
 GB/T 35273 信息安全技术 个人信息安全规范
 GB/T 35274 数据安全技术 大数据服务安全能力要求
 GB/T 37973 信息安全技术 大数据安全管理指南
 GB/T 39477 信息安全技术 政务信息共享 数据安全技术要求
 GB/T 37988 信息安全技术 数据安全能力成熟度模型
 GB/T 41479 信息安全技术 网络数据处理安全要求
 GB/T 43697 数据安全技术 数据分类分级规则
 SF/Z JD0400001 电子数据司法鉴定通用实施规范
 DB44/T 2133 政务公开 目录编制指南
 DB4403/T 271 公共数据安全要求
 DB4403/T 278 公共基础信息数据元规范
 GDZW 0031 广东省政务信息资源目录编制指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

公共机构 public institutions

全部或者部分使用财政性资金的国家机关、事业单位和团体组织。

[GB/T 36674—2018, 3.1]

3.2

企业 enterprise

共同承担确定使命、目标和目的，以提供产品或服务输出中的一个或多个组织。

注：包括诸如广义企业、虚拟企业等相关概念。

[来源：GB/T 20529.1—2006, 3.1]

3.3

个人 personal

以电子或者其他方式记录的已识别或者可识别的自然人。

注：包括中国境外、中国境内、中国国籍、非中国国籍等各类自然人。

3.4

数据账户 data account

智慧城市中以公共机构（3.1）、企业（3.2）、个人（3.3）等为实体对象，按业务视角分类方式归集目录和数据，为政府、企业和社会公众等的应用场景提供数据服务，所形成的全生命周期、全视角范围内数据和信息的集合。

3.5

公共机构数据账户 public institutions data account

以公共机构（3.1）为实体的数据账户（3.4），在公共管理和服务机构依法履职或提供公共服务过程中产生、处理的公共机构全生命周期、全视角范围内数据和信息的集合。

3.6

企业数据账户 enterprise data account

以企业（3.2）为实体的数据账户（3.4），在企业、经营、注销、信用、专利、著作、社保缴纳、公积金缴纳、纳税、商业行为等（且不限于上述事项）企业全生命周期、全视角范围内所形成的数据和信息的集合。

3.7

个人数据账户 personal data account

以个人（3.3）为实体的数据账户（3.4），在出生、教育、就业、婚姻、购房、购车、投资、公积金、保险、生育、医疗、退休、养老、离世等（且不限于上述事项）个人全生命周期、全视角范围内所形成的数据和信息的集合。

3.8

其他类型数据账户 other data account

除公共机构数据账户（3.5）、企业数据账户（3.6）、个人数据账户（3.7）之外，以其他类型实体为对象构建的数据账户。

3.9

数据资源 data resource

作为资源看待的，具有业务属性，用于支持实现数据账户各相关方业务目标，服务于业务场景的数据。

[来源：GB/T 42450—2023，3.1，有修改]

3.10

数据账户主体 data account subject

开设或入驻数据账户（3.4）后，享有数据被保护的权力，可对自己的数据进行访问、更正、删除、拒绝、限制等活动的相关方。

3.11

数据提供方 data provider

大数据参考体系结构中的一种逻辑功能构件，它将新的数据或信息引入大数据系统。

注：数据提供方一般包括公共机构、企业、个人、电子政务、公共事业、互联网等。

3.12

数据应用方 data user

执行数据生命周期相关的数据采集、数据传输、数据存储、数据处理（如计算、分析、可视化等）、数据交换、数据销毁等数据活动，运行在数据账户平台，并提供数据服务的相关方。

3.13

数据账户管理方 data account manager

对数据账户（3.4）中数据的共享、开放、运营、交易等数据流通过程进行资源整合、确权及授权，为数据账户提供数据的核验、治理等服务的相关方。

3.14

数据知识产权 data intellectual property

数据处理者对其依法依规获取的，经过一定规则处理形成的，具有实用价值和智力成果属性的数据集合所享有的权益。

4 数据账户资源应用框架

4.1 概述

数据账户资源应用框架模型如图1所示。数据账户由公共机构、企业、个人或其他类型实体根据需求开设，公共数据、企业数据、个人数据经授权、核验或认证以及治理后进入数据账户，形成包括基础、业务和管理等信息的数据账户资源；数据账户平台提供用户管理、权限管理、资源管理、授权管理、场景和供需管理、安全合规管理等功能模块，为智慧城市中无偿的数据共享和数据开放应用场景，以及有偿的数据授权运营和数据交易应用场景提供合规、安全、可信、可追溯的技术支撑。

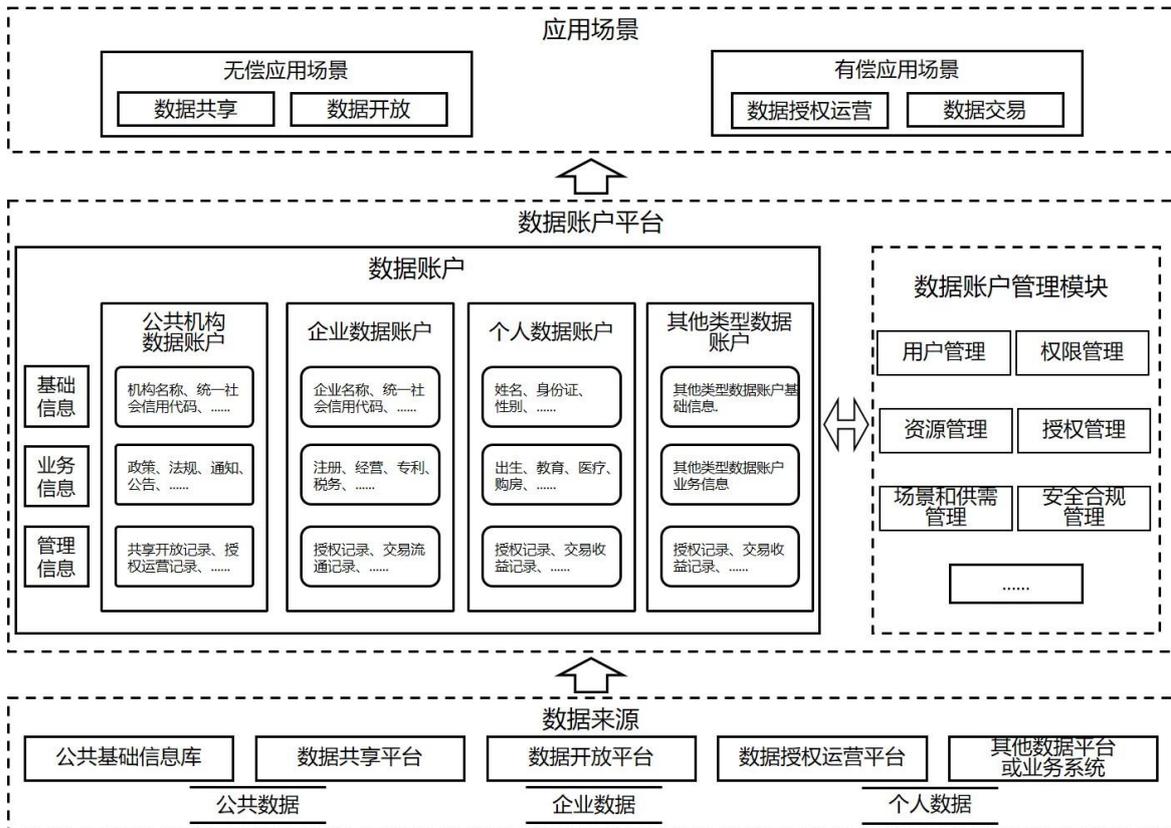


图1 数据账户资源应用框架模型

4.2 数据来源

DB4403/T XX-202X

数据来源中的数据可包括公共数据、企业数据、个人数据等。数据来源于公共基础信息库、数据共享平台、数据开放平台、数据授权运营平台和其他数据平台或业务系统。数据来源满足以下要求：

- a) 公共基础信息库应符合 DB4403/T 278 中的规定；
- b) 数据共享、开放平台、授权运营、交易等相关平台的目录资源编制宜符合 DB44/T 2133 和 GDZW 0031 中的规定；
- c) 其他数据平台或业务系统宜具备提供结构化数据的能力。

4.3 数据账户

4.3.1 概述

数据账户可包括公共机构数据账户、企业数据账户、个人数据账户和其他类型数据账户，每类数据账户包括基础信息、业务信息和数据授权应用等关键管理信息的数据账户资源。

4.3.2 公共机构数据账户资源

公共机构数据账户资源包括机构名称、统一社会信用代码等基础信息，以公共管理和服务机构依法履职或提供公共服务过程中产生、处理的公共数据为主的业务信息，以及共享开放、授权运营等过程中的审批、授权记录等管理信息。

4.3.3 企业数据账户资源

企业数据账户资源包括企业名称、统一社会信用代码等基础信息，注册、经营、注销、信用、专利、著作、社保缴纳、公积金缴纳、纳税、商业行为等业务信息以及授权记录、交易流通记录等管理信息。

4.3.4 个人数据账户资源

个人数据账户资源包括姓名、身份证、性别等基础信息，出生、教育、就业、婚姻、购房、购车、投资、公积金、保险、生育、医疗、退休、养老、离世等业务信息以及授权记录、交易收益记录等管理信息。

4.3.5 其他类型数据账户资源

其他类型数据账户资源包括社会团体、民办非企业单位和基金会等其他实体对象所构建数据账户的基础信息、业务信息以及授权记录、交易流通记录等管理信息。

4.4 数据账户管理

4.4.1 概述

数据账户管理为数据账户资源的形成及对外的数据应用服务提供支撑，包括用户管理、权限管理、资源管理、授权管理、场景和供需管理及安全合规管理等。

4.4.2 用户管理

用户管理是为数据账户用户分配不同类型的角色和不同层级的用户，每个用户可被分配一个或多个角色，不同角色和用户可具有不同的操作权限。

4.4.3 权限管理

权限管理是对数据账户中不同角色和不同层级的用户权限进行划分和管理，实现对数据的有效性访问控制和权限控制。

4.4.4 资源管理

资源管理是对数据账户的目录、数据等进行管理，实现数据账户资源的归集与融合。

4.4.5 授权管理

授权管理是对数据进入数据账户以及数据与场景的结合应用进行授权，并按数据授权申请、权限审批、数据访问控制、数据监控和追溯等流程进行管理。

4.4.6 场景和供需管理

应用场景和供需管理是对数据账户应用场景需求报送、需求评审、需求响应、统筹协调、数据服务及成效评价等过程进行管理。

4.4.7 安全合规管理

安全合规管理是通过采取必要措施，确保数据处于有效保护和合法利用的状态，并具备保障持续安全状态的能力，以及对数据账户主体合规、数据内容合规、数据来源合规、数据全生命周期合规等进行管理。

4.5 应用场景

应用场景是指数据账户主体根据业务需求，基于数据账户平台功能支撑，提供无偿的数据共享和数据开放，以及有偿的数据授权运营和数据交易等服务。

5 数据账户相关方及业务活动

5.1 概述

数据账户相关方及业务框架模型如图2所示。数据账户的相关方包括数据提供方、数据账户主体、数据账户管理方及数据应用方，各相关方在数据账户业务过程中采用如区块链等技术，保证数据的可信、完整性和质量等要求，并结合公证、鉴定、数据知识产权登记等方式，对数据账户业务过程进行监督管理和安全管理。

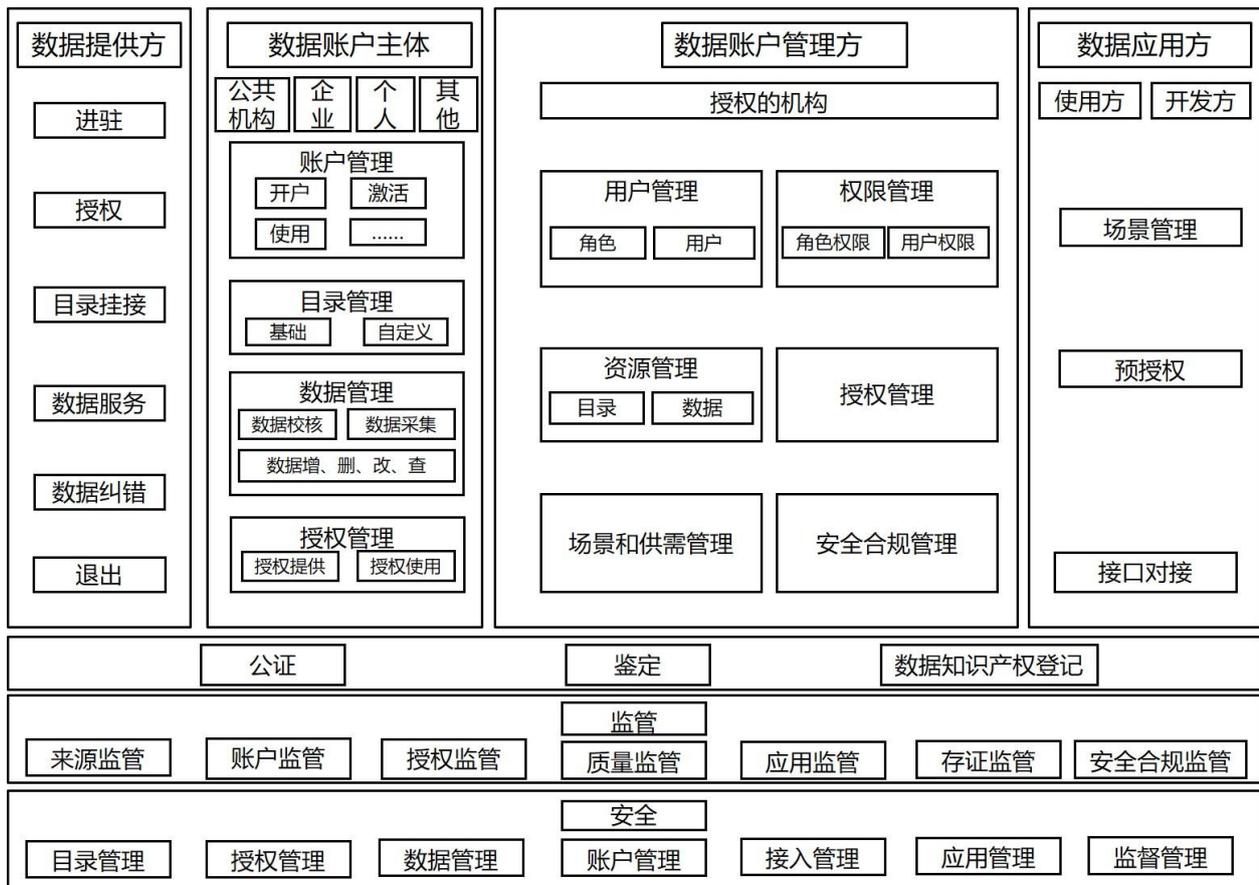


图 2 数据账户相关方及业务框架模型

5.2 数据提供方业务活动

5.2.1 概述

数据提供方的业务活动包括数据账户的进驻、授权、目录挂接、数据服务、数据纠错以及退出。

5.2.2 进驻

数据提供方向数据账户提供数据前应在数据账户平台进行注册并进驻数据账户。

5.2.3 授权

数据提供方在进驻数据账户和为数据账户进行数据接入时应获得数据账户管理方的授权。

5.2.4 目录挂接

数据提供方提供的目录应与数据账户的标准数据目录进行目录对齐和挂接。

5.2.5 数据服务

数据提供方应通过接口等方式提供数据的抽取、清洗、转换和加载等接入服务，并满足数据的时效性、一致性、规范性、可访问性等质量要求。

5.2.6 数据纠错

数据提供方应根据数据账户其他相关方提出的数据错误等情况进行数据纠错处理。

5.2.7 退出

当数据提供方不再为数据账户提供数据时宜及时退出数据账户。

5.2.8 提供数据要求

数据提供方提供数据时应满足以下要求：

- a) 提供格式规范、内容完整的数据；
- b) 对数据进行有效性验证；
- c) 对数据进行数据知识产权登记；
- d) 所提供的数据可追溯；
- e) 对数据进行加密传输；
- f) 对所提供的数据业务场景根据要求进行补充。

5.3 数据账户主体业务活动

5.3.1 概述

数据账户主体包括公共机构、企业、个人和其他类型数据账户，通过账户管理、目录管理、数据管理以及授权管理等方式对各项业务活动进行管理。

5.3.2 账户管理

数据账户主体应对数据账户的创建、开户、激活、使用、维护、冻结、注销、关闭等全生命周期活动进行管理，并可管理数据账户的身份信息，包括但不限于个人联系方式、密码、绑定的证件信息等。

5.3.3 目录管理

5.3.3.1 概述

数据账户目录由基础目录和自定义目录组成，基础目录是数据账户自身具有、已经规范并发布的目录，自定义目录是数据账户相关方根据业务及场景需求自行定义的目录。基础目录涵盖数据目录、权限目录和应用目录，自定义目录涵盖数据目录、应用目录。

5.3.3.2 基础目录

数据账户主体可创建、修改自身账户中的基础目录，并设定基础目录的可见性。对于设置不可见的目录，对数据账户管理方和数据应用方不可见，且无法对数据应用方进行使用授权。

5.3.3.3 自定义目录

数据账户主体可创建自定义目录，并应满足以下要求：

- a) 数据账户主体能对自定义目录进行编辑、删除和可见性设置；
- b) 数据账户主体能对自定义目录进行数据使用授权；
- c) 数据账户主体维护自定义目录中对应的数据；
- d) 自定义目录中元数据的数据结构与标准数据目录中的元数据保持一致。

5.3.4 数据管理

数据账户主体应对数据账户中数据的收集、存储、使用、加工、传输、交换、处理、提供、公开、开放、删除等进行管理，并满足以下要求：

- a) 数据管理工具应由数据账户管理方提供和运维，数据账户主体应使用数据账户管理方提供的工具进行数据管理操作；
- b) 在数据账户主体进行数据维护操作前，数据账户管理方应对操作人进行身份验证并确定其为数据账户主体合法操作人；
- c) 数据账户主体能对数据账户中的数据进行查看、修改、删除等操作，其中修改、删除等编辑性操作应形成数据变更记录和日志，数据账户管理方、数据应用方可查询相关记录和日志；
- d) 数据账户主体能对数据账户进行数据备份，备份数据由数据账户管理方保存并做冗余存储和完整性检测和校验，数据账户主体可从数据账户管理方获取备份数据的副本；
- e) 数据账户主体能使用备份数据恢复或覆盖数据账户中现有数据，如恢复后的数据与恢复前的数据不同，则差异信息应对数据账户管理方、数据应用方可见；在进行数据恢复操作前，数据账户管理方应对用于恢复操作的备份文件做完整性或是否被篡改等的安全性校验。

5.3.5 授权管理

数据账户主体面向数据提供方、数据应用方、数据账户管理方在数据账户平台中进行授权，并应满足以下要求：

- a) 数据接入授权：数据账户主体对数据提供方进行授权，授权内容包括数据提供范围、数据提供服务起止时间等；
- b) 数据使用授权：数据账户主体对数据应用方进行数据使用授权，授权内容包含数据项和应用场景、使用期限、使用主体范围、使用环境等；
- c) 数据账户管理授权：数据账户主体对数据账户管理方进行数据管理操作授权，授权内容包含可管理的数据项和操作权限范围等；
- d) 其他要求：
 - 1) 授权协议：数据账户主体根据数据应用方发起的授权请求查看授权详情，同时确定应用场景中数据应用方提供的服务及调用数据的范围、用途、时限、安全措施等信息后，与数据应用方签署数据授权使用协议；
 - 2) 授权记录：数据账户相关方能查看数据授权使用的审核记录。

5.4 数据账户管理方业务活动

5.4.1 概述

数据账户管理方应获得相关机构授权后对数据账户进行账户管理、权限管理、资源管理、授权管理、场景和供需管理、安全合规管理。

5.4.2 用户管理

数据账户管理方应对数据账户的角色和使用者进行管理，针对不同角色和数据的分类分级情况设置不同权限级别的账户权限，实现对不同账户主体的身份认证，账户权限的划分、管理及监控，支撑对数据的有效性访问控制和权限控制。数据的分类分级应符合GB/T 43697中的规定。

5.4.3 权限管理

权限管理应符合以下要求：

- a) 支持用户的创建与管理，包括：
 - 1) 用户列表和检索；

- 2) 用户信息详情及新增与编辑;
- 3) 用户的启用、禁用及删除。
- b) 支持角色管理, 包括:
 - 1) 角色的列表和检索;
 - 2) 角色详情及新增、编辑与删除;
 - 3) 角色的启用、禁用及删除。
- c) 支持数据分类分级的管理, 包括:
 - 1) 数据分类分级规则配置和管理;
 - 2) 根据核心数据、重要数据、一般数据的分级进行相应的安全管理;
 - 3) 敏感数据、重要数据识别以及对数据的脱敏脱密;
 - 4) 数据自动和人工分类和分级;
 - 5) 数据分类分级检索及新增、编辑与删除。
- d) 支持权限配置, 包括:
 - 1) 权限的列表和检索;
 - 2) 权限的新增、编辑及删除;
 - 3) 权限多维配置。

5.4.4 资源管理

数据账户资源管理具有账户目录管理、账户数据整体管理、账户数据治理、数据服务管理、数据分析管理等功能, 并符合以下要求:

- a) 账户目录管理。维护并管理数据账户目录资源, 应具备账户目录资源编制、目录资源发布、策略(共享策略、更新策略等)管理等功能;
- b) 账户数据整体管理。管理数据账户数据资源, 应具备账户数据查询、数据纠偏申请、数据来源管理、数据接入管理、数据更新管理、数据量管理等功能;
- c) 账户数据治理。根据数据目录体系要求对账户资源进行全生命周期的数据治理, 应具备数据标准管理、数据模型管理、元数据管理、主数据管理、数据质量管理、数据安全等功能, 并符合 GB/T 34960.5 中的规定;
- d) 数据服务管理。管理基于数据资源提供的基础数据服务, 应具备数据服务查询、数据服务订阅、数据服务审核、数据服务管理、数据服务统计、数据服务授权、数据服务认证、数据地图等功能;
- e) 数据分析管理。基于数据服务的分析, 应具备数据账户数据分析和资源分析的能力;
- f) 数据可视化管理。对于数据质量、数据血缘调度关系及结果可视化展示, 异常任务可视化展示及报警通知, 以及对应的报警工作单处理过程可视化展示、数据调用频率等价值权重可视化展示, 并能识别关键价值数据。

5.4.5 授权管理

数据账户管理方围绕应用场景授权管理, 基于合法合规、隐私保护、公平合理、最小化、谁授权谁使用谁负责等原则, 面向数据账户各相关方, 建立监督和管理机制, 提供数据授权申请、权限审批、数据访问控制、数据监控和追溯等能力支持, 并应符合以下要求:

- a) 用户具有对已申请数据账户所必需的最小访问权限;
- b) 数据账户管理方及时撤销用户不必要的访问权限;
- c) 数据账户管理方按统一的授权流程进行授权;

- d) 数据账户管理方对授权进行定期检查，对所有授权访问进行记录，并定期回溯被授权数据的指标内容和数据周期；
- e) 数据账户管理方定期审计授权情况并生成授权审计报告，授权审计报告包括已授权用户列表、权限级别和访问日志等信息。

5.4.6 场景和供需管理

5.4.6.1 需求管理

数据账户管理方应提供线上、线下等不同应用场景及相关数据需求申报方式和统一的需求申报接口。

5.4.6.2 需求评审

数据账户管理方对应用场景及相关数据需求进行评审，评审包括需求目的、交付标准、交付时效等内容，必要时补充数据登记信息。应用场景及相关数据的需求评审不通过时由数据账户管理方将结果反馈至需求方进行处理。应用场景需求内容包括数据产品、数据服务、数据工具等。

5.4.6.3 需求响应

数据账户管理方应要求数据提供方针对通过评审的应用场景及相关数据需求进行响应，并做如下处理：

- a) 无数据时增补相关数据；
- b) 无法提供数据时应反馈给需求方理由；
- c) 可提供数据时，反馈相关数据需求响应清单（包括数据供给清单、数据供给计划、数据供给说明书等）给需求方，同时对所提供的数据进行预处理。

5.4.6.4 统筹协调

数据账户管理方针对需求响应后的反馈意见进行复核，确认数据供需双方的需求有效且一致，并发布相关数据需求响应复核清单。

5.4.6.5 数据提供

数据账户管理方应要求数据提供方按数据需求响应复核清单以数据共享、数据开放、数据授权运营等方式向数据应用方提供相关数据，并按相关规定进行数据应用登记备案。

5.4.6.6 数据交易

当场景应用涉及数据交易时，应由相关方进行交易定价约定并履约实施交易，需要时对交易纠纷进行处理。

5.4.6.7 成效评价及改进

数据账户管理方可自行或委托第三方对应用场景及数据的全流程进行评价，并按需针对所提供的的数据质量，数据共享、数据开放、数据授权运营、数据交易等数据服务效率和质量等进行持续改进。

5.4.7 安全合规管理

5.4.7.1 安全管理

数据账户管理方应按GB/T 37973、GB/T 37988、GB/T 39477、GB/T 41479及DB4403/T 271等标准的要求进行数据账户的安全管理。

5.4.7.2 合规管理

数据账户管理方应按以下内容进行合规管理：

- a) 设置数据账户合规管理组织架构，并明确合规管理的部门和责任人；
- b) 建立数据账户合规管理制度，包括但不限于数据分级分类保护制度、数据全生命周期管理制度、数据安全事件应急预案制度、数据合规风险评估制度等；
- c) 组织开展数据合规管理培训；
- d) 开展合规管理体系实施评估，并根据评估情况进行持续改进。

5.5 数据应用方业务活动

5.5.1 概述

数据应用方包括数据使用方和数据开发方，能通过软硬件设备和系统实现数据采集、数据整理、数据分析、数据检索、数据可视化等功能，基于数据账户数据提供数据使用场景、进行应用开发和提供数据服务，具有提供数据库、数据报表、数据报告、数据订阅、API接口等多种方式的数据应用能力，在数据账户中提供统一服务入口，并进行场景申请、预授权、接口对接等管理。

5.5.2 相关方要求

5.5.2.1 数据使用方

数据使用方是已进驻数据账户，为数据账户主体提供专业服务，对数据有使用需求的相关方，应满足以下要求：

- a) 具有对所申请或使用数据的安全保障能力；
- b) 按数据使用的最小必要需求进行申请及使用；
- c) 具有明确的数据使用目的。

5.5.2.2 数据开发方

数据开发方是接受数据账户管理方委托，基于数据账户数据，为数据账户管理方开发软件或者接口服务的相关方。数据开发方在数据开发全流程中各环节应符合数据账户管理方在运行环境、人员变更、代码变更、部署运维、数据存取等方面的监管要求，并能提供审计数据给数据账户管理方。

5.5.3 场景管理

数据使用方应对应用场景的申报、评审状态、上下架、渠道管理、场景使用调用情况进行管理，并向数据账户主体提供包括手机APP、服务接口、应用软件、委托代理服务数据应用和服务，并满足以下要求：

- a) 可通过查询检索，比对订阅、自助分析、标签取数、模型推荐、指标服务等方式获取数据应用场景；
- b) 建立数据场景适配流程，能将场景与应用进行一对一适配；
- c) 对数据按场景授权进行应用；
- d) 对数据在应用场景中的应用流向信息进行完整记录；
- e) 建立场景访问日志并确保可追溯、可审计；
- f) 建立数据应用场景评价机制，对场景的应用成效进行量化评价。

5.5.4 预授权

数据账户平台应支持使用方对用户的注册、授权、修改、注销等管理，并能对使用方进行权限控制，提供基于角色的授权管理策略，支持用户名密码、数字证书、动态口令等多种身份认证方式。数据开发方使用数据时应向数据账户主体申请数据使用预授权，获取脱敏样本数据后用于相关应用场景的开发测试，并在数据账户管理方允许的网络和硬件资源上使用数据。

5.5.5 接口对接

数据使用方和数据开发方应能通过多种存储设备和传输协议的服务进行接口对接，并满足实时和非实时接入数据的需求。

5.6 公证

应由第三方机构对数据账户相关方和数据的可信性、合规性，以及数据授权和使用等过程进行认证公证并提供权威报告。

5.7 鉴定

应由第三方机构对电子数据的完整性、唯一性及数据质量等进行评价，对电子数据的检验鉴定应符合SF/Z JD0400001中的相关规定，并能提供权威意见。

5.8 数据知识产权登记

数据账户相关方对符合数据知识产权登记条件的数据向主管部门指定的机构申请登记，获取数据知识产权登记证书。

5.9 监管

5.9.1 概述

监管应由政府相关部门依职责或按需引入第三方机构开展。包括对数据来源、账户、授权、数据质量、应用、存证、安全合规等全生命周期、全视角范围的监管。

5.9.2 来源监管

来源监管包括对数据提供方等数据来源机构的资质、信用等的监管。

5.9.3 账户监管

账户监管包括对数据账户的开设、入驻、退出等全生命周期过程的监管。

5.9.4 授权监管

授权监管包括对数据账户的开设、入驻、开发、共享应用等过程中涉及的授权等的监管。

5.9.5 质量监管

质量监管包括对数据的规范性、完整性、准确性、一致性、时效性等数据质量的监管。

5.9.6 应用监管

应用监管包括对数据应用的场景申请、预授权、接口对接等的监管。

5.9.7 存证监管

存证监管包括对数据账户的主体存证、关系存证、资产存证以及活动存证等的监管。

5.9.8 安全合规监管

安全监管包括对数据账户数据安全、网络安全、系统安全、应用安全、用户安全等的监管，以及数据应用服务的技术和管理措施等的监管。合规监管包括对数据账户主体合规、数据内容合规、数据来源合规、数据全生命周期合规等的监管。

6 数据账户关键业务流程

6.1 业务活动总体要求

数据账户关键业务流程是指数据账户的开设/入驻、数据资源目录创建、数据供给及数据资源目录挂接、数据应用、数据账户注销等全生命周期的业务活动，如图3所示。数据账户业务活动应满足以下要求：

- a) 数据账户的开设/入驻：基于数据账户主体的自愿和授权，数据账户主体有权选择是否开通数据账户，以及选择数据账户的类型、范围和内容；
- b) 数据账户数据资源目录创建：应基于业务需求和应用场景进行；
- c) 数据账户数据供给：满足完整性、准确性和时效性等数据质量要求；数据账户主体具有查看、修改、删除、补充和更新数据账户中数据的权限，并可对数据进行备份和恢复；
- d) 数据资源目录挂接：供给的数据与数据账户中的标准数据目录进行对齐匹配，形成分类对应关系；
- e) 数据账户数据应用：遵守数据账户的授权规则，数据账户主体有权控制数据账户中数据的访问、使用、共享和交易，以及撤销、变更和终止等的授权；
- f) 数据账户注销：不再使用的数据账户及时进行清理和销毁，数据账户主体有权申请注销数据账户并选择数据账户的注销方式和范围。

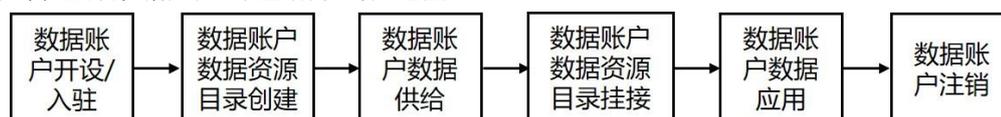


图3 数据账户业务流程图

6.2 数据账户开设及入驻

6.2.1 概述

数据账户的开设/入驻是指数据账户主体通过数据账户平台，按照数据账户的类型、范围和内容，选择数据来源，进行数据账户的注册和开通的过程。

6.2.2 数据账户开设

公共机构/企业/个人/其他类型实体（以下简称“各类实体”）数据账户开设流程如图4所示。各类实体在数据账户平台发起数据账户的开设活动，由数据账户平台形成各类实体数据账户，各类实体和数据账户平台签订授权协议，由数据账户平台返回开设成功的信息并建立各类实体数据账户。

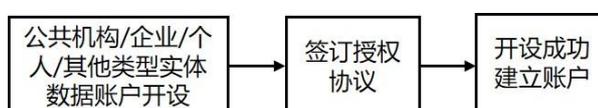


图 4 数据账户开设流程

6.2.3 数据账户入驻

数据账户相关方入驻流程如图5所示。由需要入驻数据账户的相关方在数据账户平台发起数据账户入驻请求，由数据账户管理方对相关方进行资格审查，相关方资格符合要求时，通过数据账户平台签订数据服务协议并入驻数据账户；其中数据提供方应提供合法合规采集数据的相关佐证，公共数据统一由深圳市数据共享交换相关平台供给，相关方资格不符合要求的可在具备条件后重新发起账户入驻请求。



图 5 数据账户相关方入驻流程

6.3 数据供给和数据资源目录挂接

数据账户数据供给及数据资源目录挂接流程见图6。由数据账户管理方通过数据账户平台接入数据提供方的已授权数据，并与数据账户的数据标准进行比对，比对通过后进行数据的核验或认证，核验或认证通过后，按约定将数据存入数据账户平台或以接口等方式提供数据供给服务。数据账户管理方应在数据账户平台进行数据资源编目，上架后形成数据账户基础目录。

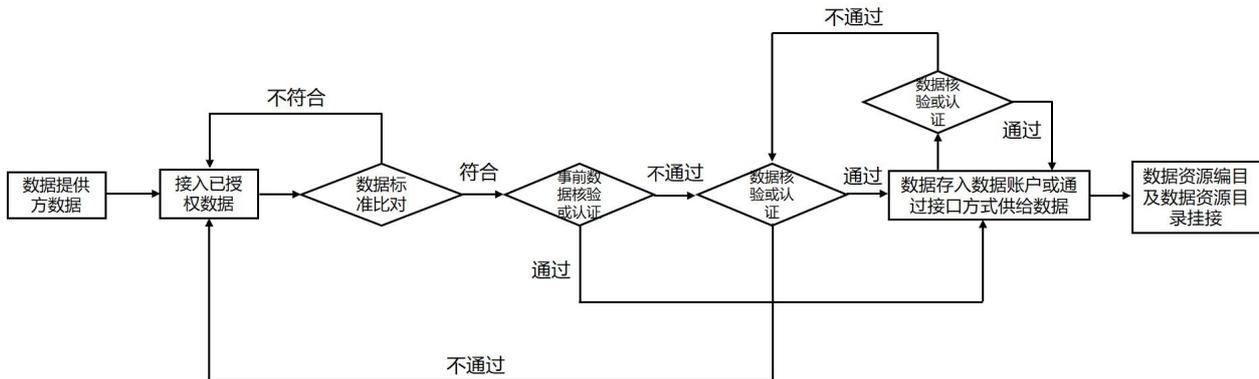


图 6 数据供给及目录挂接流程

6.4 数据账户数据目录创建

各类实体开设数据账户后，可经数据账户平台授权后使用数据账户的基础数据目录或在数据账户中自定义数据目录。

6.5 数据应用

数据账户数据应用及服务流程见图7。由数据应用方在数据账户平台发起数据应用请求，由数据账户管理方对数据应用方进行资质审查。数据应用方的资质审查通过后由数据账户主体在数据账户平台进行数据应用授权，授权通过后由数据账户管理方在数据账户平台发起数据的核验或认证，由第三方机构进行核验或认证，通过核验或认证后的数据对外进行数据应用。核验或认证不通过的数据重新进入数据供给环节。应符合以下要求：

- a) 数据应用方应提交详细的数据账户主体资料，包括各类实体的数据账户主体身份认证信息；

- b) 数据账户管理方负责发起数据核验或认证，确保数据的真实性、准确性和完整性；
- c) 第三方机构应对数据账户主体的身份进行验证，负责对数据内容、数据来源、数据处理进行检查，确保数据账户应用的安全性和有效性。

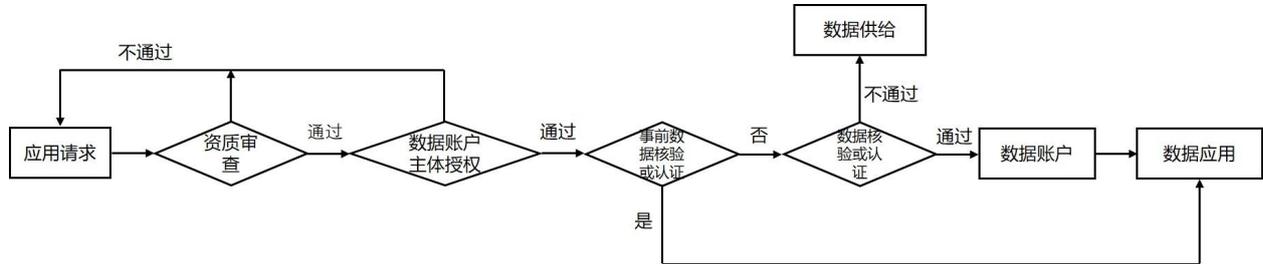


图7 数据账户数据应用流程

6.6 数据账户注销

数据账户注销流程见图8。由数据账户主体在数据账户平台提出账户注销申请，由数据账户管理方审核注销申请，注销申请通过审核后，由数据应用方进行业务的清理，同时数据提供方停止数据供给服务，数据账户管理方或数据应用方根据数据账户主体要求和授权进行数据的转存、删除或销毁，数据的删除或销毁应符合GB/T 35274和GB/T 37973中的规定，由数据账户管理方对数据账户主体的账户进行注销。

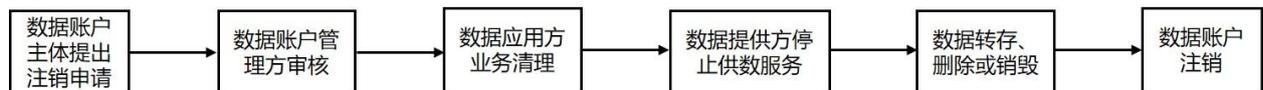


图8 数据账户注销流程

7 数据账户资源共享应用要求

7.1 概述

数据账户主体基于数据空间开发利用环境及数据账户平台的授权等能力支持，按数据账户资源共享应用要求进行数据的融合应用。根据数据账户资源的构成情况，将侧重于数据账户资源中最核心的数据共享应用要求进行明确，按公共数据、企业数据和个人数据等的不同开发利用方式，结合数据的共享、开放、授权运营、交易等应用场景开展。

7.2 数据共享应用基本要求

7.2.1 目的和范围

应明确数据共享应用的目的、范围以及可能存在的风险，清晰界定可共享数据的类型、数据量以及共享条件，数据共享应用全流程操作应可审计，数据可溯源。

7.2.2 授权

数据应在授权后进行共享应用，并可被查看、修改或删除，数据在共享应用过程中应可控，任何单位和个人不应擅自使用或传播共享数据。

7.2.3 数据安全和隐私保护

数据共享应用应遵守相关的法律法规和隐私保护要求，针对核心、重要、一般三个级别的数据通过数据的加密、访问控制、脱敏脱密、安全等保存储、审计监控等措施防止数据被非法使用、篡改或泄露。

7.2.4 数据质量

数据在共享应用过程中应建立统一的数据标准和格式，并进行核实和校验，满足数据的一致性、准确性、完整性、及时性等数据质量要求。

7.2.5 监督和管理

应建立数据共享应用的监督和管理机制，对数据共享应用过程进行监控和评估，并对共享数据的质量和安全性进行定期检查和评估，对违规行为进行处罚和纠正，以确保数据共享应用的合规性和有效性。

7.2.6 数据共享应用协议

应具有明确的数据共享应用流程，通过协议进行数据的共享应用，明确各方的权利、义务和责任，协议应涵盖数据的使用范围、期限、保密义务、违约责任等内容，并建立数据共享应用的申请、审批、使用、反馈等机制。

7.3 数据共享应用典型场景及要求

7.3.1 概述

数据账户资源共享应用场景主要包括无偿应用和有偿应用场景。

7.3.2 基本要求

7.3.2.1 无偿应用场景

7.3.2.1.1 无偿应用场景适用于公共数据应用于公共治理、公益事业等场景，以及企业和个人等数据账户主体之间无偿提供数据使用等相关业务，可通过数据共享和开放等方式，实现数据账户资源的具体应用。

7.3.2.1.2 数据共享可包括公共机构之间，企业、个人以及其他类型数据账户主体之间的数据共享等活动。

7.3.2.1.3 数据开放可包括公共机构向企业、个人或其他类型数据账户主体的数据开放，以及企业、个人及其他类型数据账户主体向其他主体的数据开放等活动。

7.3.2.2 有偿应用场景

7.3.2.2.1 有偿应用场景适用于公共数据应用于产业发展、行业发展等场景，或企业、个人及其他类型数据账户主体向其他主体有偿提供数据服务等场景，可通过数据授权运营和数据交易等方式，实现数据账户资源的市场化应用。

7.3.2.2.2 数据授权运营可包括公共机构以及企业、个人或其他类型数据账户主体按程序依法授权企业、个人或其他类型数据账户主体，对授权的公共数据等进行加工处理，开发形成数据产品和服务并无偿提供应用等活动。

7.3.2.2.3 数据交易可包括数据账户中数据的供需双方之间以数据产品作为交易标的，进行的以货币或货币等价物交换数据使用权和市场化流通等活动。

7.3.2.3 场景应用要求

7.3.2.3.1 数据账户平台应支持数据账户主体发起数据账户资源应用场景，并授权数据提供方提供数

据给数据应用方使用。

7.3.2.3.2 数据账户平台应支持数据应用方发起数据账户资源应用场景，数据应用方可通过查阅跨数据账户共享整合的综合性数据目录，向数据账户管理方和数据账户主体发出数据使用申请，数据账户主体可根据需求授权数据提供方提供数据给数据应用方使用。

7.3.3 数据共享场景

数据共享应符合包括但不限于以下要求：

- a) 可通过接口调用方式或主动适配方式进行；
- b) 按不同场景建立场景数据模型，描述不同场景涉及的数据；
- c) 满足完整性、一致性、准确性、时效性、可追溯性、真实性等数据质量管理要求；
- d) 接受共享方能对共享的数据进行解析和处理；
- e) 制定数据共享服务协议，对数据获取流程、权利、义务等进行说明。

7.3.4 数据开放场景

数据开放应符合包括但不限于以下要求：

- a) 支持不同的开放类型及形式；
- b) 支持编制全量基础数据目录及开放数据目录；
- c) 支持对数据目录的安全合规审查及数据融合的风险预判；
- d) 支持数据目录的定期动态更新及维护；
- e) 支持公共数据“原始数据不出域、数据可用不可见”以及通过算法模型获取结果数据等方式；
- f) 支持数据开放过程中的数据脱敏、安全域环境；
- g) 支持数据开放的条件审核及协议签订；
- h) 支持数据开放过程的监测、预警及应急处置。

7.3.5 数据授权运营场景

当符合行政级别和类别要求的公共机构，以及企业、个人等类型数据账户主体，按程序依法授权法人或者非法人组织，对授权的公共数据、企业数据和个人数据等进行加工处理，开发形成数据产品和服务并进行运营时，数据的授权运营应符合包括但不限于以下要求：

- a) 遵循统一性、安全性、可追溯、可审计性、协同性、社会性等原则；
- b) 按照受理申请、评审遴选、协议签订、运营评价、运营终止等授权运营全流程进行；
- c) 支持编制全量基础数据目录及授权运营数据目录；
- d) 支持对数据目录的安全合规审查及数据融合的风险预判；
- e) 支持数据目录的定期动态更新及维护；
- f) 支持公共数据“原始数据不出域、数据可用不可见”以及通过算法模型获取结果数据等方式；
- g) 支持数据授权运营过程中的数据脱敏、安全域环境；
- h) 界定明确的运营产品类型及计价方式；
- i) 建立授权运营安全保障体系。

7.3.6 数据交易场景

数据交易应符合包括但不限于以下要求：

- a) 支持数据来源的确认、使用范围的界定、流通过程的可追溯及安全风险防范；
- b) 支持数据质量、数据安全及合规、数据应用场景的管理；
- c) 支持数据的算法、算力资源的配置与调度；

DB4403/T XX-202X

- d) 支持交易过程信息的记录和保存;
- e) 支持交易过程中对各主体的行为管理;
- f) 支持数据的可信交易环境, 可对交易进行追溯、风险识别及合规检测;
- g) 支持对交易过程防攻击、防泄漏、防窃取的监测、预警、控制和应急处置;
- h) 支持对交易环境重要系统和数据库的容灾备份;
- i) 支持不同交易环境网络系统的等级保护措施。

7.4 数据账户相关方要求

7.4.1 数据提供方

数据提供方共享应用要求如下:

- a) 应具备数据的持有权和/或使用权, 并获得数据账户资源共享应用的权限;
- b) 应按照数据账户的目录要求提供数据;
- c) 应提供数据纠错处理能力, 如更正数据错误、补足数据丢失等。

7.4.2 数据账户主体

数据账户主体共享应用要求如下:

- a) 应提供数据共享应用过程中的认证和授权, 如数据供给授权、数据使用授权等;
- b) 应提供数据授权使用过程的监控记录, 如授权日志、报表等;
- c) 应对数据提供方提供的数据进行合规性验证, 如是否配置授权同意规则、数据使用范围、目的等;
- d) 应根据数据授权情况定期审核更新数据账户目录;
- e) 应提供多种数据加工和开发方式, 如联合计算、多方安全计算、数据元件、联邦计算、可信执行环境等;
- f) 应对无条件共享的公共数据提供多种接入能力, 如数据集、数据接口、数据库表等。

7.4.3 数据账户管理方

数据账户管理方共享应用要求如下:

- a) 应建立数据共享管理机制, 如申请、审批和反馈等;
- b) 应对数据账户主体提供授权和运营管理功能, 如提出申请、调用数据、数据出域审核、撤回授权等;
- c) 应支持对授权和运营全流程的监控, 保证授权和运营记录可追溯;
- d) 应提供对数据应用方提出的数据需求申请管理功能, 如数据使用申请, 数据加工申请等;
- e) 应提供数据账户使用场景的审核功能, 如用数单位、所需数据、共享模式、截止时间等。

7.4.4 数据应用方

数据应用方共享应用要求如下:

- a) 应根据数据账户管理方审核通过的场景使用数据;
- b) 应提供安全可控的开发环境, 如数据使用控制、开发环境控制等;
- c) 应对开发后的数据产品提供合规性审查, 如是否有携带原始数据、个人信息敏感数据、数据产品是否可反向识别原始数据等;
- d) 应对审核通过的数据产品提供安全封装, 如数字水印、接口熔断限流、调用存证等。

7.4.5 第三方

应按照鉴定标准和流程，对共享应用的数据进行鉴定，包括数据的来源、收集方式、处理过程等，确保数据的真实性和完整性。数据账户主体、管理方或应用方对鉴定结果存在争议时，第三方应负责处理争议并提供解决方案。

8 安全要求

8.1 相关方安全

8.1.1 数据账户主体

数据账户主体对数据账户进行目录管理、授权管理、账户管理、数据管理等业务时，应符合GB/T 35273、GB/T 37973和GB/T 39477的要求。

8.1.2 数据账户管理方

数据账户管理方对数据账户进行账户管理、质量管理、接入管理、应用管理、资源管理、安全管理、存证管理、合规管理并提供数据服务时，应提供相应的安全技术保障，并符合GB/T 35273、GB/T 37973和GB/T 39477的要求。

8.1.3 数据应用方

数据应用方应按国家相关法律法规要求进行数据应用管理，制定安全管理制度实施安全技术防护措施，并符合GB/T 35273、GB/T 37973和GB/T 39477的要求。

8.1.4 第三方

第三方参与数据账户和相关信息系统建设、维护，涉及数据处理的，应当经过严格的批准程序，明确工作规范和标准，建立事前审核、事中留痕、事后追溯机制，预防、发现、处置各类数据安全风险隐患。受委托的第三方应当按照法律法规规定和合同约定履行安全保护义务，不得超出授权范围擅自留存、使用、泄露或者向他人提供数据。

8.2 管理安全

8.2.1 目录管理

数据账户管理方进行基础目录管理和自定义目录管理时应满足以下要求：

- a) 按照数据分类分级要求形成数据资源目录；
- b) 目录发布共享时进行身份鉴别与审核，保证目录的规范性和准确性；
- c) 基于目录中数据资源的安全影响分析，对数据资源目录建立分级安全管理策略，保障数据账户在管理过程中数据资源的保密性和完整性；
- d) 对目录管理操作进行授权审计。

8.2.2 授权管理

数据账户主体根据授权进行数据的提供或使用，并应满足以下要求：

- a) 明确授权的范围和目的，保留授权记录；
- b) 采用技术措施防止数据被未授权使用或访问；
- c) 对敏感数据的使用应经过二次授权，并进行授权审计。

8.2.3 数据管理

DB4403/T XX-202X

数据账户管理方为数据账户主体进行数据的采集、查看、校核、修改、删除、补充和更新，在对数据账户进行备份和恢复时应提供安全保障措施，除应满足GB/T 35274、GB/T 37973、DB4403/T 271中的规定外，还应满足以下要求：

- a) 在数据管理过程进行安全审计；
- b) 根据数据分类分级要求对数据账户内数据进行定期数据备份，对敏感数据进行加密存储并采用签名技术防止备份数据被篡改；
- c) 数据恢复过程中进行数据的完整性校验；
- d) 数据在备份等操作过程中进行相关操作的日志记录。

8.2.4 账户管理

数据账户管理方对数据账户的注册、注销、角色和权限等进行管理时，应满足以下要求：

- a) 对数据账户的管理全过程进行安全审计；
- b) 对数据账户的管理进行授权与身份鉴别；
- c) 对数据账户的管理行为形成操作日志并进行行为审计；
- d) 日志记录和审计报告至少保存6个月。

8.2.5 接入管理

数据账户管理方对数据提供方以及数据应用方进行数据的接入管理，包括数据编目、数据接入、数据调度、数据质量稽核等，应满足以下要求：

- a) 提供标准化的数据接口，对接口规范、接口标准、接口安全进行标准化定义；
- b) 数据接入后对数据资产的变化、访问行为、数据流向、数据敏感程度变化等进行记录与安全审计；
- c) 数据接入后建立数据规则、行为模型或策略模型等匹配检查机制，对异常使用数据行为及时发现并告警制止；
- d) 数据接入满足授权与身份鉴别安全要求，授权接入过程相关操作满足安全审计要求。

8.2.6 应用管理

数据账户管理方应制定应用安全管理制度并实施安全技术防护措施，对数据账户的使用、开发和应用场景进行管理，经授权同意后遵循最小必要原则进行数据的获取、开发和应用。

8.2.7 监督管理

数据账户管理方应基于GB/T 35273、GB/T 37973和GB/T 39477的要求对数据来源、数据质量、数据账户及使用、存证、安全、授权等进行监督管理，并制定安全管理制度、实施安全技术防护措施。