ICS 35.240
CCS L 70

DB3205

苏 州 市 地 方 标 准

DB3205/T 1142.2—2024

综合数据库 数据服务管理规范
第 2 部分：自然人综合库

Comprehensive database data service management specification—

Part 2:Comprehensive database of natural persons

2024-10-09 发布 2024-10-16 实施

苏州市市场监督管理局 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。

本文件是DB3205/T 1142《综合数据库　数据服务管理规范》的第2部分。DB3205/T 1142已经发布了以下部分：

——第1部分：法人综合库；

——第2部分：自然人综合库。

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。

本文件由苏州市数据局提出、归口并组织实施。

本文件起草单位：苏州市信息中心、数字苏州建设有限公司、北京中软国际信息技术有限公司。

本文件主要起草人：余少华、秦龙焜、钱秋霜、周泽聿、褚彬、窦博文、周杨、朱时兵、符山、陈世伟、宋伟。

综合数据库　数据服务管理规范
第 2 部分：自然人综合库

1　范围

本文件规定了自然人综合库数据架构、数据汇聚、数据使用、异议数据处理、数据安全的要求。

本文件适用于自然人综合库数据建设和使用。

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 35273—2020　信息安全技术　个人信息安全规范

GM/T 0054　信息系统密码应用基本要求

DB3205/T 1142.1　综合数据库　数据服务管理规范　第1部分：法人综合库

3　术语和定义

DB3205/T 1142.1界定的以及下列术语和定义适用于本文件。

3.1

自然人综合库　database of integrated and comprehensive natural persons

基于苏州市人口基础库，以自然人为核心对象，苏服码为索引，通过归集、整合各公共管理和服务机构的自然人其他相关数据，经治理、加工后形成的自然人综合数据库。

3.2

自然人综合库建设运营机构　construction and operation organization of natural person comprehensive database

承担自然人综合库建设，负责自然人综合库管理和维护工作的机构。

3.3

自然人数据使用机构　natural person data usage organization

使用自然人综合库数据的公共管理和服务机构。

3.4

自然人数据来源机构　natural person data source organization

自然人综合库中自然人相关数据的来源部门或单位。

4　数据架构

4.1　模型设计原则

应按照DB3205/T 1142.1中4.1规定的模型设计原则进行自然人综合库实体数据模型设计。

4.2 数据分层

应按照DB3205/T 1142.1中4.2的规定进行自然人综合库数据分层。

4.3 数据分类

自然人综合库应涵盖自然人全生命周期相关信息，包含基本信息、教育信息、就业社保、资产信息、家庭关系、资质荣誉、医疗健康、司法信息、信用信息、生活服务及其他信息等内容。数据分类见表1。

表1 自然人综合库数据分类

序号	一级分类	二级分类	说明
1	基本信息	基本登记信息	自然人在公共管理和服务机构登记注册的相关信息。
2		出生信息	自然人个体出生相关信息。
3		死亡信息	自然人个体死亡相关信息。
4		联系信息	自然人的联系地址、邮箱、电话等相关信息。
5		苏服码信息	自然人的苏服码相关信息。
6	教育信息	学籍信息	自然人的学籍注册相关信息。
7		学历信息	自然人获得的学历相关信息。
8		学位信息	自然人获得的学位相关信息。
9	就业社保	就业信息	自然人的就业、创业、失业活动相关信息。
10		参保信息	自然人的社保参保、缴费、退休养老待遇等相关信息。
11		公积金信息	自然人的公积金缴纳、贷款等相关信息。
12	资产信息	固定资产	自然人拥有的房屋、车辆、设备等资产相关信息。
13		无形资产	自然人拥有的具备价值的知识产权相关信息。
14	家庭关系	户籍信息	自然人户籍、户籍迁移等相关信息。
15		婚姻信息	自然人的婚姻状况等相关信息。
16		亲缘关系信息	自然人的血亲相关信息。
17	资质荣誉	资质信息	自然人拥有的从事某种工作必备的资质或能力。
18		荣誉信息	自然人从事的可以产生正面评价的活动信息。
19		财政扶持信息	自然人享受的政府给予的财政资金补贴或税收优惠等政策性支持相关信息。
20	医疗健康	医疗信息	自然人的挂号就诊、疫苗接种等相关医疗信息。
21		健康信息	自然人的体检、职业病、工伤等相关健康信息。
22	司法信息	司法案件信息	自然人牵涉司法案件、或者自然人作为强制执行对象的相关信息。
23		限制消费信息	自然人受到的限制消费相关信息。
24	信用信息	黑名单信息	自然人的失信黑名单相关信息。
25		红名单信息	自然人的红名单相关信息。
26		信用承诺信息	自然人的信用承诺、履行践诺情况相关信息。
27		双公示信息	自然人受到行政许可、行政处罚相关双公示相关信息。
28		行政确认信息	自然人受到的行政确认的相关信息。
29		行政强制信息	自然人受到的行政强制相关信息。

表1　自然人综合库数据分类（续）

30	生活服务	政务服务信息	自然人享受的相关政务服务信息。
31	其他	其他	自然人享受的其他部门或单位服务信息。

5　数据汇聚

5.1　数据汇聚原则

应按照DB3205/T 1142.1中5.1规定的数据汇聚原则进行自然人综合库数据汇聚。

5.2　数据汇聚流程

应按照DB3205/T 1142.1中5.2规定的数据汇聚流程进行自然人综合库数据汇聚。

5.3　数据汇聚方式

5.3.1　库表汇聚

结构化程度高、有信息系统支撑的数据应采用库表方式进行汇聚，以库表数据作为对象进行数据汇聚时，自然人数据来源机构应向部门前置库推送数据，数据共享平台交换数据至自然人综合库建设运营机构前置库。库表数据如涉及个人敏感信息，应进行脱敏加密，并向自然人综合库建设运营机构提供脱敏加密算法。

5.3.2　文件汇聚

格式多样的数据可采用文件方式进行汇聚，以文件作为对象进行数据汇聚时，自然人数据来源机构应将文件写入部门前置机的指定目录，数据共享平台按时抽取文件。文件抽取后，自然人综合库建设运营机构对于具有固定结构的文件，通过解析按照结构化格式进行存储，对于不具有固定结构，无法直接解析入库的文件，以文件方式存储。文件数据如涉及个人敏感信息，应加密传输，并向自然人综合库建设运营机构提供加密算法。

5.3.3　接口汇聚

无法提供数据库访问权限、实时性要求较高的数据或自然人数据来源机构有明确规定无法提供库表及文件的情况下，可采用接口方式进行汇聚，以接口作为对象进行数据汇聚时，自然人数据来源机构应提供原始接口及文档，数据共享平台通过服务网关代理后统一提供服务。

5.4　数据质量

5.4.1　可用性

应按照DB3205/T 1142.1中5.4.1的规定落实自然人综合库数据质量可用性要求。

5.4.2　完整性

5.4.2.1　目录完整

应按照DB3205/T 1142.1中5.4.2.1的规定落实自然人综合库数据质量的目录完整性要求。

5.4.2.2　字段完整

自然人数据来源机构提供的数据应包含该类信息内容的所有有效字段。

示例：“政务人口基本信息”包括“姓名、出生日期、性别、身份证号码、籍贯、曾用名”等全部字段信息。

5.4.2.3 释义完整

自然人数据来源机构提供的数据应包含数据的完整解释。

示例：“SEX”字段对应的字典名称为“性别”，数据内容为“0”、“1”，“0”对应的实际内容为“男”，“1”对应的实际内容为“女”。

5.4.2.4 周期完整

应按照DB3205/T 1142.1中5.4.2.4的规定落实自然人综合库数据质量的周期完整性要求。

5.4.3 准确性

5.4.3.1 数据格式合规

自然人数据来源机构提供的数据应保证数据类型、数值范围、数据长度、精度等满足格式规范约束。

示例1：“年龄”中出现非数值，为“%%”。

示例2：“身份证号码”不符合GB11643—1999的规定。

示例3：“年龄”中出现小数点，为“50.2”。

5.4.3.2 数据逻辑正确

自然人数据来源机构提供的数据应符合业务逻辑，避免出现脏数据。

示例1：“姓名”取值为“test”。

示例2：“身份证号码”7到10位表示出生年月，值为“1790”。

示例3：“自然人登记信息”中的“姓名”字段为空。

5.4.3.3 数据不重复

自然人数据来源机构提供的数据不应包括因业务或技术产生的冗余数据。

示例：数据表中出现2条完全相同记录。

5.4.4 一致性

5.4.4.1 目录一致

应按照DB3205/T 1142.1中5.4.4.1的规定落实自然人综合库数据质量的目录一致性要求。

5.4.4.2 内容一致

所提供数据应确保数据表、数据项内容一致：

a） 不应存在数据表名称相同，数据项不同的情况；

示例：两类数据表名称均为“政务人口基本信息”，其中一类数据项为“姓名、性别、曾用名”，另外一类数据项为“姓名、年龄、居住地”。

b） 不应存在数据项相同、数据表名称不同的情况。

示例：两类数据项名称均为“姓名、年龄、性别、曾用名、居住地”，其中一类数据表名称为“政务人口基本信息”，另外一类数据表名称为“基本信息”、“人口信息”。

5.4.5 时效性

应按照DB3205/T 1142.1中5.4.5的规定落实自然人综合库数据质量时效性要求。

6 服务使用

6.1 使用方式

6.1.1 数据共享调用

在自然人数据使用机构有自然人综合库明细数据查询需求的情况下，应通过数据共享平台提出申请，经过审批通过后，按GB/T 35273—2020第7章规定的要求使用数据。原则上明细数据都应以API接口方式提供。

6.1.2 数据开发利用

在自然人数据使用机构对自然人综合库有数据开发利用需求的情况下，或在自然人数据使用机构无数据开发利用能力的情况下，应委托自然人综合库建设运营机构按照需求进行数据治理、融合、开发，处理形成的自然人标签类、统计分析类、算法挖掘类数据，自然人数据使用机构应通过数据共享平台进行申请，并按GB/T 35273—2020第7章规定的要求使用数据。

6.1.3 数据产品开发

在自然人数据使用机构对自然人综合库有数据产品开发需求的情况下，或在自然人数据使用机构无数据产品开发能力的情况下，应通过数据共享平台申请数据产品开发所需要的自然人相关数据，并在自然人综合库建设运营机构提供的可信数据开发环境中完成数据产品开发，使用时应遵循GB/T 35273—2020第7章规定的要求。

6.2 发布方式

在按照数据共享调用、数据开发利用方式提供服务的情况下，自然人综合库建设运营机构应先在数据共享平台发布数据资源目录，并挂接相应的数据资源。

6.3 服务使用流程

6.3.1 服务申请

在有数据查询需求、数据开发利用需求的情况下，自然人数据使用机构应在服务申请前，充分与自然人综合库建设运营机构进行沟通，确认具体数据需求和数据提供方式，并通过数据共享平台进行数据申请。

6.3.2 服务审批

6.3.2.1 自然人综合库建设运营机构审批

自然人数据使用机构以履职为目的申请自然人非明细数据时，如不涉及个人敏感信息，应由自然人综合库建设运营机构审批，审批流程见图1。

注：非明细数据包括由自然人综合库建设运营机构加工后形成的自然人非敏感标签类、统计分析类、算法挖掘类数据。

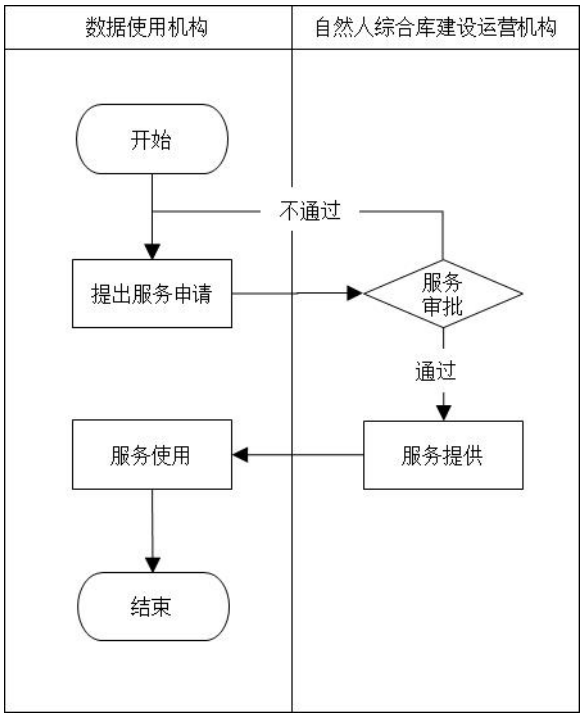

图 1　自然人综合库建设运营机构审批流程图

6.3.2.2　自然人综合库建设运营机构与自然人数据来源机构联合审批

自然人数据使用机构以履职为目的申请自然人明细数据或自然人敏感标签数据时，应由自然人综合库建设运营机构审批，审批流程见图2。

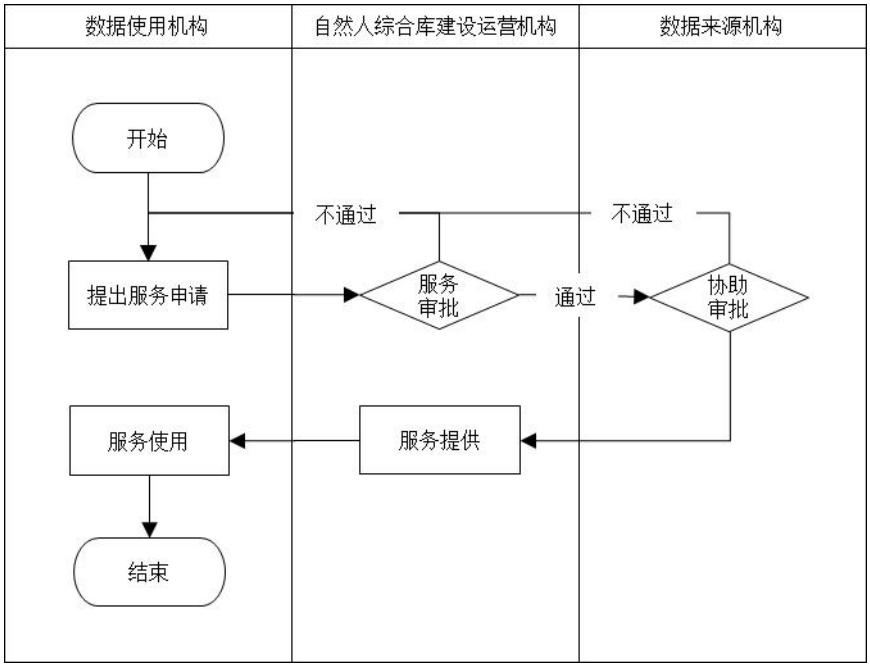

图 2　自然人综合库建设运营机构与自然人数据来源机构联合审批流程图

6.3.3　服务提供

6.3.3.1 提供方式

服务提供方式分为以下三种：

a） 库表方式：是指自然人数据使用机构通过数据共享平台向自然人综合库建设运营机构申请服务，申请通过后，自然人综合库以数据库形式将资源推送至数据共享平台，供自然人数据使用机构在数据共享平台上获得数据，在不影响使用的情况下库表数据应脱敏；

b） 文件方式：是指自然人数据使用机构通过数据共享平台向自然人综合库建设运营机构申请服务，申请通过后，自然人综合库以文件格式将资源加密推送至数据共享平台，供自然人数据使用机构在数据共享平台上获得数据；

c） 接口方式：是指自然人数据使用机构通过数据共享平台向自然人综合库建设运营机构申请服务，申请通过后，自然人综合库以资源链接端口推送至数据共享平台，供自然人数据使用机构在数据共享平台上调用接口资源，自然人综合库建设运营机构应对接口进行监控。

6.3.3.2 保障措施

自然人综合库建设运营机构应配合自然人数据使用机构进行系统对接、网络联通、接口联调测试等工作，保障自然人数据使用机构正常取数、用数。

6.3.4 服务使用

自然人数据使用机构应当按照数据资源的用数场景、使用期限或者其他要求使用数据，不应跨越数据使用边界，并应及时反馈数据使用情况。如用数场景为对公众提供数字化应用时，应获得自然人数据授权并留存授权证明。

7 异议数据处理

应按照DB3205/T 1142.1第7章的规定对自然人综合库的异议的数据进行处理。

8 数据安全管理

8.1 安全管理参与方

根据自然人综合库提供服务过程中的角色类型，可以分为数据管理者、数据提供者、数据加工者、数据使用者四类，各参与方的定义见表2。

表 2 自然人综合库安全管理参与方

角色	定义
数据管理者	有权决定自然人相关数据处理目的、方式，对数据进行管理的组织
数据提供者	生产、提供自然人相关数据的组织
数据加工者	清洗、加工自然人相关数据的组织
数据使用者	使用、消费自然人相关数据的组织

8.2 参与方管理要求

8.2.1 数据管理者

数据管理者应遵循要求如下：

a） 获得数据提供者的授权，并在授权范围内合法处理利用数据；
b） 根据数据的类型、重要性、使用频率、敏感性等因素制定数据分类分级要求，确保数据安全；
c） 对数据加工者进行授权，明确授权目的和范围；
d） 制定数据加工规程，明确自然人综合库数据资源清洗、融合、脱敏、标识等相关要求；
e） 设置严格的数据访问控制规则，采取限制数据加工终端外部接入的互联网地址等措施，保证数据加工在合法授权范围内，禁止未经授权的操作行为；
f） 应对自然人综合库数据加工过程制定审计规则，对数据加工过程进行审计、监管，并定期对数据加工者的数据加工行为进行日志审计；
g） 对数据使用者进行授权，明确授权目的和范围；
h） 审核数据使用场景，确保数据使用没有超过数据提供者的授权范围；
i） 制定数据安全使用策略，采取权限控制、加解密、水印、脱敏、隐私计算等安全技术措施，保证数据使用安全；收集并永久留存数据加工日志。

8.2.2 数据提供者

数据提供者应遵循要求如下：

a） 确保所提供的数据的合法性、真实性和有效性；
b） 采取适当的管理和技术措施，包括对数据分级分类，数据加密传输等，确保数据安全；
c） 向数据管理者进行授权，明确所提供数据的使用范围和条件；
d） 配合数据管理者向数据加工者、数据使用者进行授权，明确所提供数据的使用范围和条件。

8.2.3 数据加工者

数据加工者应遵循要求如下：

a） 获得数据管理者的授权，并在授权范围内合法加工数据，如涉及原始数据还需获得数据提供者的授权；
b） 全面准确理解数据加工安全规范，并按照相关要求执行；
c） 根据数据的类型、重要性、使用频率、敏感性等因素进行数据分类分级存储；
d） 数据出域需符合相关数据安全要求，敏感数据出域需脱敏加密，同时需对数据进行严格审计，防止敏感数据泄露；
e） 留存数据加工日志，记录安全事情处置情况，如出现突发数据安全事件，应立即上报数据管理者，并采取必要的挽救措施。

8.2.4 数据使用者

数据使用者应遵循要求如下：

a） 获得数据管理者的授权，在授权范围内合法使用数据，如涉及原始数据还需获得数据提供者的授权；
b） 保证数据使用环境和使用过程安全性，以防数据的泄露和滥用；
c） 使用场景涉及个人信息的，应得到个人信息主体对数据使用授权（未成年人则需其监护人代理授权），并对授权文件进行永久留存。

8.3 数据处理安全要求

8.3.1 数据传输

数据传输过程应遵循安全要求如下：

a） 涉及个人敏感信息，应采用加密等安全措施；
b） 密码技术应符合 GM/T 0054 等相关标准的规定，保证传输过程中数据的保密性和完整性；
c） 管控数据传输过程，确保及时发现问题，并进行告警、阻断；
d） 定期检查或评估数据传输的安全性和可靠性。

8.3.2 数据存储

数据存储过程应遵循安全要求如下：

a） 存储数据过程中密码技术应符合GM/T 0054等相关标准的规定,对敏感数据进行加密存储保护；
b） 个人生物识别信息应与个人身份信息分开存储；
c） 对明细数据的存储环境进行分域分级设计，根据数据重要性、量级、使用频率等因素将数据分域分级存储；
d） 敏感数据的存储应制定特定的安全策略，包括但不限于物理隔离、网络隔离等；
e） 建立数据冗余一致性校验策略；
f） 制定数据的备份策略和恢复策略，包括但不限于备份数据的放置场所、介质替换频率、备份周期/频率、备份范围等。

8.3.3 数据加工

应按照DB3205/T 1142.1中8.3.3规定的要求进行自然人综合库数据加工。

8.3.4 数据使用

8.3.4.1 身份鉴别

应按照DB3205/T 1142.1中8.3.4.1规定的要求进行自然人综合库数据身份鉴别。

8.3.4.2 访问控制

数据访问控制过程应遵循安全要求如下：

a） 针对服务器系统、数据库系统等重要系统设置用户访问控制策略，为不同用户授予其完成各自承担任务所需的最小权限，同时增加角色设定；
b） 应及时清理系统中僵尸账号，确保一人一号一权限，杜绝一号多用的情况；
c） 账号应采用实名认证，实现追责溯源；
d） 因工作需要，需授权特定人员超权限访问个人信息的，充分审批其权限并记录在册，访问结束后及时收回权限；
e） 应阻断对数据、应用、系统等的任何非授权访问，提出告警并记录审计日志；
f） 应限制对重要服务器的白名单控制；
g） 应只开启业务所需的最少系统服务及端口，并定期核查、审计、清理。

8.3.4.3 数据脱敏

应按照DB3205/T 1142.1中8.3.4.3规定的要求进行自然人综合库数据脱敏。

8.3.4.4 数据防泄漏

应按照DB3205/T 1142.1中8.3.4.4规定的要求进行自然人综合库数据防泄漏。

8.3.5 数据销毁安全

数据销毁过程应遵循安全要求如下：

a） 建立符合数据销毁策略和管理制度的销毁审批机制，记录审批过程；

b） 在销毁审批后以不可逆方式销毁数据内容；

c） 对数据销毁处理过程相关的操作进行记录，以满足安全审计的要求；

d） 应按照 GB/T 35273—2020 中 8.3 规定的要求执行个人信息删除操作。

参 考 文 献

[1] GB/T 36344—2018 信息技术 数据质量评价指标
[2] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求
[3] DB32/T 4040.1—2021 政务大数据 数据元规范 第1部分：总则
[4] DB32/T 4040.3—2021 政务大数据 数据元规范 第3部分：综合人口数据元