

# DB4403

## 深圳市地方标准

DB4403/T XXX—XXXX

### 公共数据分类分级指南

Guidelines for public data classification and grading

(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

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 基本原则 ..... 2

5 数据分类规则 ..... 3

6 数据分级规则 ..... 3

    6.1 数据分级框架 ..... 3

    6.2 数据分级要素 ..... 3

    6.3 数据影响分析 ..... 3

    6.4 级别规则 ..... 4

7 数据分类分级流程 ..... 6

    7.1 分类流程 ..... 6

    7.2 分级流程 ..... 7

附录 A（资料性） 公共数据分类示例 ..... 10

附录 B（资料性） 影响程度参考示例 ..... 11

附录 C（资料性） 数据级别变更情形 ..... 13

附录 D（资料性） 加工程度维度的数据分类 ..... 14

参考文献 ..... 15

## 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、深圳市坪山区政务服务和数据管理局、深圳市智慧城市科技发展集团有限公司、深圳市城市公共安全技术研究院。

本文件主要起草人：王耀文、张军、张永昌、罗菁春、刘洋、潘晓军、孙飞、唐增来、胥少卿、刘素云、陈海康、赵娜、穆端端、郭阳博、王刚、伍可、莫俊宁、石海洋、陈超慧、冯敬之。

# 公共数据分类分级指南

## 1 范围

本文件给出了公共数据分类分级的基本原则、数据分类规则、数据分级规则与数据分类分级流程。  
本文件适用于指导深圳市公共管理和服务机构开展公共数据的分类分级工作。  
本文件不适用于涉及国家秘密或者法律法规另有规定的公共数据。

## 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 25069—2022 信息安全技术 术语
- GB/T 35295—2017 信息技术 大数据 术语
- GB/T 38667—2020 信息技术 大数据 数据分类指南
- GB/T 43697—2024 数据安全技术 数据分类分级规则

## 3 术语和定义

GB/T 43697—2024界定的以及下列术语与定义适用于本文件。

### 3.1

**公共数据** public data

公共管理和服务机构在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

### 3.2

**数据分类** data classification

根据数据的属性或特征，将其按一定的原则和方法进行区分和归类，并建立起一定的分类体系和排列顺序的过程。

[来源：GB/T 43697—2024，有修改]

### 3.3

**数据分级** data grading

根据数据的敏感程度和数据一旦遭到泄露、篡改、毁坏或者非法获取、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，按照一定的原则和方法进行定级。

### 3.4

**数据共享** data sharing

公共管理和服务机构依法履行公共管理职责时使用其他公共管理和服务机构的数据资源，以及为其他公共管理和服务机构提供公共服务过程中产生、处理的数据的行为。

### 3.5

**数据开放 data opening**

公共管理和服务机构通过公共数据开放平台向社会提供可机器读取的公共数据的活动。

**3.6**

**原始数据 raw data**

公共管理和服务机构采集未经加工处理的数据。

**3.7**

**衍生数据 derived data**

经过统计、关联、挖掘、聚合、去标识化等加工活动而产生的数据。

**3.8**

**数据项 data item**

数据不可分割的最小单位，具有独立含义且不可分割，如库表的字段。

**3.9**

**数据集 data set**

由多个数据项组成的集合，如数据库表、数据文件等。

**3.10**

**重要数据 key data**

特定领域、特定群体、特定区域或达到一定精度和规模的，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

[来源：GB/T 43697—2024，3.2]

**3.11**

**核心数据 core data**

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

[来源：GB/T 43697—2024，3.3]

**3.12**

**一般数据 general data**

核心数据、重要数据之外的其他数据。

[来源：GB/T 43697—2024，3.4]

## **4 基本原则**

遵循国家数据分类分级保护要求，按照数据所属行业领域进行分类分级管理，依据以下原则对数据进行分类分级：

- a) 合法合规原则：符合相关法律法规和国家或行业主管部门有关规定和要求，优先识别法律法规中规定的数据类别或等级；
- b) 分类多维原则：数据分类宜以多种视角和维度，从便于数据管理和使用角度，考虑国家、行业、组织等多个视角，进行科学和系统化的数据分类。数据分类的实施对象为数据集，原则上一个数据集只隶属于一个分类，一个分类下可有多个数据集；
- c) 分级明确原则：数据分级的各级别宜边界明确，不同级别的数据采取不同的保护措施；
- d) 就高从严原则：数据分级采用就高不就低的原则，当多个因素可能影响数据分级时，按照可能造成的各个影响对象的最高影响程度确定数据级别。如果数据集包含多个等级的数据项，按照数据项的最高等级对数据集进行定级。对于等级较高的数据集，可通过数据脱敏实现降级使用，或申请其中较低等级的数据项或数据集，从而提高可用性；

- e) 动态调整原则：数据类别或等级根据时间变化、政策环境变化、规模变化、安全事件发生或不同业务场景的敏感性变化进行定期审核并及时调整。

5 数据分类规则

数据按照先行业领域分类、再业务属性分类的思路进行分类，具体要求如下：

- a) 按照行业领域，将数据分为工业数据、电信数据、金融数据、能源数据、交通运输数据、自然资源数据、卫生健康数据、教育数据、科学数据等；
- b) 各行业各领域主管(监管)部门根据本行业本领域业务属性，对本行业领域数据进行细化分类。参考 GB/T 43697—2024 常见业务属性包括但不限于业务领域、责任部门、描述对象、流程环节、数据主体、内容主题、数据用途、数据处理、数据来源,在此基础上扩充细分如下,具体分类示例可参见附录 A：
  - 1) 按照数据所属类型分类，包括基础数据库、主题数据库、业务数据库，其中基础数据库可细分为人口、法人、房屋、自然资源与空间地理、电子证照、公共信用等类型；
  - 2) 按照数据对象主体分类，如个人数据、组织数据、城市部件数据等；
  - 3) 按照数据共享类型分类，如无条件共享、有条件共享和不予共享；
  - 4) 按照数据开放类型分类，如无条件开放、有条件开放和不予开放；
  - 5) 按照来源机构分类，如交通运输局、教育局等；
  - 6) 按照来源机构行政层级分类，如国家级、省级、市级、区级、其他等；
  - 7) 按照来源系统分类，如自建、国直、省直、市直等；
  - 8) 按照来源途径分类，如系统产生数据、采购数据、共享渠道获取数据和其他渠道获取数据；
  - 9) 按照数据结构化特征分类，如结构化数据（库表结构/Excel/结构化文件）、半结构化数据（JSON/XML）和非结构化数据（文本、图片、音频、视频）等；
  - 10) 按照数据产生频率分类，如每秒、分、时、天、周、月、季度、半年、年，实时，不更新等；
  - 11) 按照数据加工程度分类，如原始数据、衍生数据，具体分类见附录 D；
  - 12) 按照数据使用频率、访问频次和分析引用层面分类，如冷数据、温数据、热数据。

注：个人信息及敏感个人信息的识别和分类见GB/T 43697—2024及敏感个人信息相关国家标准。

6 数据分级规则

6.1 数据分级框架

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、一般数据三个级别。

6.2 数据分级要素

数据分级基于分级要素进行综合判定，影响数据分级的要素，包括数据的领域、群体、区域、精度、规模、深度、覆盖度、重要性等，其中领域、群体、区域、重要性通常属于定性描述的分级要素，精度、规模、覆盖度属于定量描述的分级要素，深度通常作为衍生数据的分级要素。

注：详细内容请参考GB/T 43697—2024。

6.3 数据影响分析

### 6.3.1 影响对象

影响对象是指数据面临安全风险时，可能影响的对象。其中，安全风险主要考虑数据遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享等风险。影响对象的影响范畴包括：国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益。

- a) 国家安全：影响国家政治、国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等国家利益安全；
- b) 经济运行：影响市场经济运行秩序、宏观经济形势、国民经济命脉、行业领域产业发展等经济运行机制；
- c) 社会稳定：影响社会治安和公共安全、社会日常生活秩序、民生福祉、法治和伦理道德等社会秩序；
- d) 公共利益：影响社会公众使用公共服务、公共设施、公共资源或影响公共健康安全等公共利益；
- e) 组织权益：影响组织自身或其他组织的生产运营、声誉形象、公信力、知识产权等组织权益；
- f) 个人权益：影响自然人的的人身权、财产权、隐私权、个人信息权益等个人权益。

### 6.3.2 影响程度

影响程度是指数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能造成的影响程度。影响程度包括特别严重危害、严重危害、一般危害、无危害。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是国家安全、经济运行、社会秩序或公共利益，则以国家、社会或行业领域的整体利益作为判断影响程度的基准。如果影响对象仅是组织或个人权益，则以组织或公民个人的权益作为判断影响程度的基准。影响程度参考示例见附录B。开展数据影响分析时，宜按照以下规则确定影响程度：

- a) 当影响对象是国家安全时：
  - 1) 如果直接影响政治安全，应将影响程度确定为特别严重危害；
  - 2) 如果关系其他国家安全重点领域，应将影响程度确定为严重危害；
  - 3) 其他直接危害国家安全的情形，应将影响程度确定为一般危害。
- b) 当影响对象是经济运行时：
  - 1) 如果关系国民经济命脉，应将影响程度确定为特别严重危害；
  - 2) 如果直接危害宏观经济运行，或对行业领域或地区的经济发展造成严重危害，应将影响程度确定为严重危害。
- c) 当影响对象是社会秩序时：
  - 1) 如果关系重要民生，应将影响程度确定为特别严重危害；
  - 2) 如果直接危害社会稳定，应将影响程度确定为严重危害。
- d) 当影响对象是公共利益时：
  - 1) 如果关系重大公共利益，应将影响程度确定为特别严重危害；
  - 2) 如果直接危害公共健康和安全，应将影响程度确定为严重危害。
- e) 当影响对象是个人或组织权益时，如果影响大规模的个人或组织权益，需要同时研判是否会对国家安全、经济运行、社会秩序或公共利益造成影响以及影响程度。

## 6.4 级别规则

### 6.4.1 数据级别规则

核心数据、重要数据、一般数据的确定规则如下：

- a) 满足以下任一条件的数据，识别为核心数据：



- 1) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对国家安全造成特别严重危害（如直接影响政治安全）或严重危害（如关系其他国家安全重点领域）；
  - 2) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对经济运行造成特别严重危害（如关系国民经济命脉）；
  - 3) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对社会秩序造成特别严重危害（如关系重要民生）；
  - 4) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对公共利益造成特别严重危害（如关系重大公共利益）；
  - 5) 对领域、群体、区域具有较高覆盖度，直接影响政治安全的重要数据；
  - 6) 达到较高精度、较大规模、较高重要性或深度，直接影响政治安全的重要数据；
  - 7) 经有关部门评估确定的核心数据。
- b) 满足以下任一条件的数据，识别为重要数据：
- 1) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对国家安全造成一般危害；
  - 2) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对经济运行造成严重危害；
  - 3) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对社会秩序造成严重危害（如影响社会稳定）；
  - 4) 数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，直接对公共利益造成严重危害（如危害公共健康和安全）；
  - 5) 数据直接关系国家安全、经济运行、社会稳定、公共健康 and 安全的特定领域、特定群体或特定区域；
  - 6) 数据达到一定精度、规模、深度或重要性，直接影响国家安全、经济运行、社会稳定、公共健康和安全；
  - 7) 经行业主管（监管）部门评估确定的重要数据。
- c) 未识别为核心数据、重要数据的其他数据，确定为一般数据。

6.4.2 数据安全等级

本文件设定数据级别为3级，主要从影响对象和影响程度要素完成定级，将数据从高到低分为核心数据、重要数据、一般数据3个基本级别，详见表1。根据本市安全管理要求，进一步细分为4个安全等级，建立安全等级与判别标准，详见表2。

表 1 数据级别定义表

数据级别	安全等级	定义
一般数据	一级	对国家安全、社会秩序、公共利益、行业发展、信息主体均无危害。
	二级	对单个组织或个人的合法权益造成一般危害、严重危害或特别严重危害； 对经济运行、社会秩序、公共利益造成一般危害；
重要数据	三级	参考6.4.1 b)数据级别重要数据识别规则
核心数据	四级	参考6.4.1 a)数据级别核心数据识别规则

表 2 数据级别确定规则表

影响对象	影响程度			
	特别严重危害	严重危害	一般危害	无危害
国家安全	核心数据 (四级)	核心数据 (四级)	重要数据 (三级)	一般数据 (一级)
经济运行	核心数据 (四级)	重要数据 (三级)	一般数据 (二级)	一般数据 (一级)
社会秩序	核心数据 (四级)	重要数据 (三级)	一般数据 (二级)	一般数据 (一级)
公共利益	核心数据 (四级)	重要数据 (三级)	一般数据 (二级)	一般数据 (一级)
组织权益、个人权益	一般数据 (二级)	一般数据 (二级)	一般数据 (二级)	一般数据 (一级)

7 数据分类分级流程

7.1 分类流程

7.1.1 基于数据资源目录进行数据分类

公共管理和服务机构对数据资源进行全面梳理，确定待分类分级的数据资源及其所属的行业领域，同时根据深圳市公共数据资源目录编制相关要求形成数据资源目录，报同级公共数据主管部门汇总和审核。公共管理和服务机构负责本机构公共数据分类工作，在本文件的基础上进一步根据行业细分，行业主管部门负责根据本文件提出本行业分类工作实施细则，指导行业内公共管理和服务机构开展分类工作并监督分类工作结果，市公共数据主管部门负责对应的省政务大数据中心市级分节点汇聚的公共数据分类工作。

7.1.2 确定数据分类规则

各公共管理和服务机构选择合适维度识别数据，明确数据集的分类规则。分类工作宜以形成明确分类维度、分类层次和分类结果为目的，分类层次可由分类工作实施主体自行确定，原则上不超过四级层次。若使用第5章范围外的分类维度或因实际业务分类层次超过四级，可结合国家、地方、行业数据分类法律及监管要求拓展数据分类规则，同时报市公共数据主管部门备案。通过数据管理相关平台进行数据分类，形成数据分类规则。

7.1.3 审查发布

市公共数据主管部门进行内部审查，并通过数据管理相关平台发布。

7.1.4 分类评估和变更

按需评估数据分类维度和方法的合理性，检查其是否符合业务场景变化和数据管理需要。如变更数据分类，公共管理和服务机构需制定变更计划，评估变更对数据资源数据分类工作的影响，包括分类维度、分类规则改变等，变更计划由市公共数据主管部门审核通过后执行。

7.1.5 分类结果反馈与闭环处理

各公共管理和服务机构可通过数据管理相关平台对数据分类存在的错误、不合理等情形提出异议。责任单位应及时处理并反馈，如需变更数据分类则按分类变更流程执行，数据分类流程见图 1。

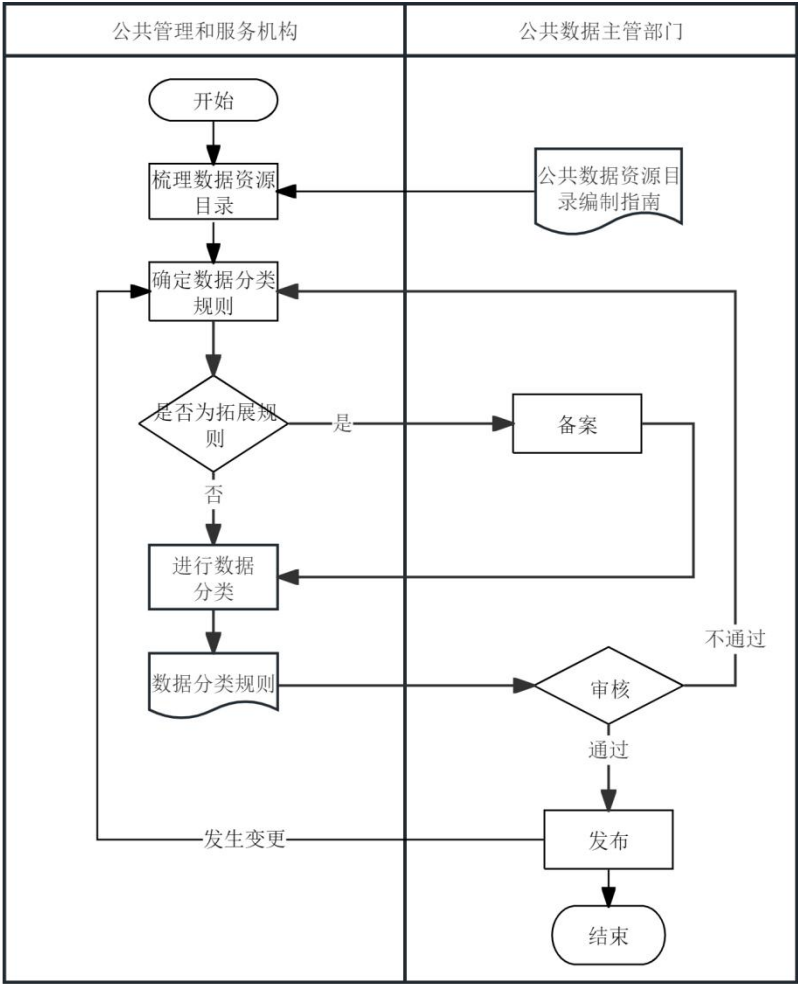


图 1 数据分类流程

7.1.6 分类定期审核

分类级别可能因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化或行业相关规则而发生改变，因此需要行业主管部门对数据分类进行定期审核并及时调整。

7.1.7 监督检查

为确保数据分类制度能有效执行，公共数据主管部门需要加强监督，定期检查各公共管理和服务机构是否按照规定进行数据分类，并对未按规定执行的行为进行纠正。

7.2 分级流程

7.2.1 分级对象确定

公共管理和服务机构根据数据资源目录以及合规要求，结合业务现行情况确定数据范围和对象，明确数据分级的颗粒度（如数据项、数据集、数据库等）。

### 7.2.2 确定数据分级规则

公共管理和服务机构在完成数据分类的基础上，结合现有和可预期的数据应用场景，综合考虑数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度等因素，通过数据管理相关平台，初步确定数据安全等级，原则上数据集的安全等级应该取数据集中数据项的最高安全等级（如某一数据集中有一个数据项安全等级为四级，其他均为三级，则数据集的安全等级应定义为四级）。

### 7.2.3 审核发布

市公共数据主管部门对数据分级结果进行审核并发布，确保分级的准确性和科学性。定级结果和对应安全保护要求可作为有关信息系统项目立项、审批、验收等工作的依据之一。

### 7.2.4 分级评估及变更

#### 7.2.4.1 按需评估

数据处理活动过程中，各公共管理和服务机构需评估数据分级结果合理性，检查数据是否发生影响分级要素的相关变化，并按需评估数据分级结果的有效性和应用情况，检查其是否满足业务应用场景，评估定级结果是否达到对数据的安全防护要求。出现下列情形之一时，应重新定级：

- a) 数据内容发生变化，导致原有数据的安全级别不再适用；
- b) 数据内容未发生变化，但数据时效性、数据规模（包括数据量、数据增长速度、数据种类等）、数据应用场景、数据加工处理方式等发生变化；
- c) 多个原始数据直接合并，导致原有的安全级别不再适用合并后的数据；
- d) 因对不同数据选取部分数据进行合并形成的新数据，导致原有数据的安全级别不再适用合并后的数据；
- e) 不同数据类型经汇聚融合形成新的数据类别，导致原有的数据级别不再适用于汇聚融合后的数据；
- f) 因国家或行业主管部门要求，导致原定的数据级别不再适用；
- g) 需要对数据安全级别进行变更的其他情形；
- h) 在数据共享开放后的汇总数据、衍生数据，责任主体是数据使用的公共管理的服务机构，原则上沿用原公共管理和服务机构的定级，如满足等级变更情形需由数据使用机构重新定级。

#### 7.2.4.2 变更控制

确认数据级别需要变更的，公共管理和服务机构应向公共数据主管部门申请，并及时对变更后数据重新级别判定，数据级别可能发生变更的场景包括但不限于数据汇聚融合、加工、脱敏、超过时效等情况，同时遵循以下原则：

- a) 从原始数据中直接部分复制出来的数据安全等级不高于原有安全等级；
- b) 从多个原始数据合并的新数据不低于原有安全等级，宜高于原安全等级；
- c) 对不同数据选取部分数据进行合并形成的新数据，根据内容的关键要素进行重新安全等级判定；
- d) 数据内容不发生变化进行升降级需有明确的敏感内容失效/生效依据。

其他影响数据级别变化的因素和场景见附录C。

### 7.2.5 分级结果反馈与闭环处理

各公共管理和服务机构可通过数据管理相关平台对数据分级存在的错误、不合理等情形提出异议。责任单位应当及时处理并反馈，如需变更数据级别则按分级变更流程执行，数据分级流程见图2。

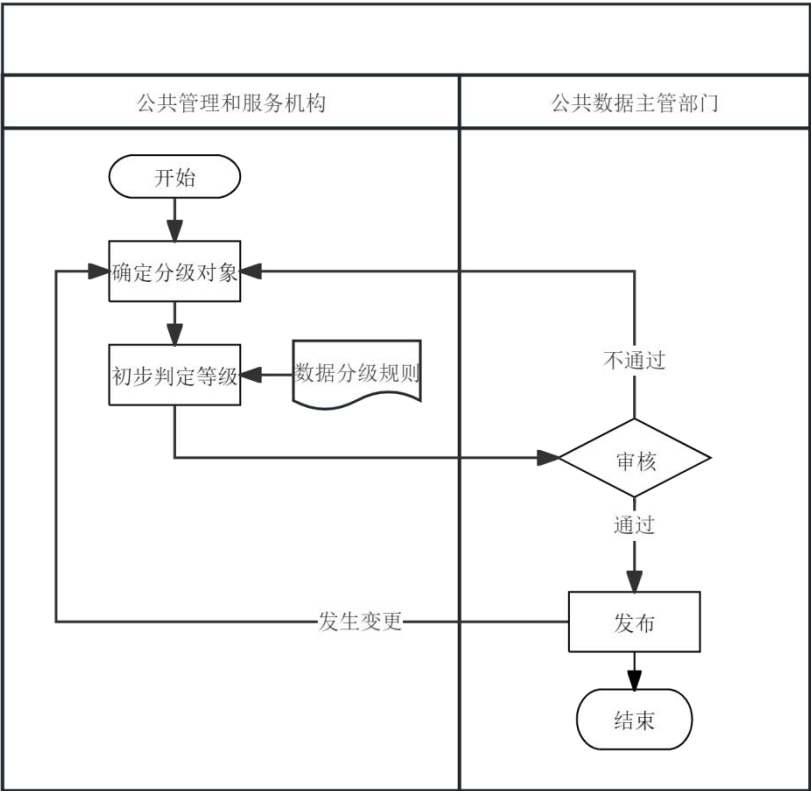


图2 数据分级流程

7.2.6 分级定期审核

分级级别可能因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化和行业相关规则而发生改变，因此需要行业主管部门对数据分级进行定期审核并及时调整。

7.2.7 监督检查

为确保数据分级制度能有效执行，公共数据主管部门需要加强监督，宜定期检查各公共管理和服务机构是否按照规定进行数据分级，并对未按规定执行的行为进行纠正。

附 录 A  
(资料性)  
公共数据分类示例

表 A.1 给出了公共数据分类的示例。

表 A.1 公共数据分类示例

分类维度	一级分类	二级分类
所属类型	基础数据库	人口、法人、房屋、自然资源与空间地理、电子证照、公共信用
	主题数据库	互联网监管、危化品监管、网办、行政执法等围绕经济社会发展的同一主题领域，由多部门共建项目形成的数据库
	业务数据库	教育局数据库、公安局数据库等不属于以上两类的数据库
对象主体	个人数据	个人基本资料、个人身份信息、个人生物识别信息、网络身份标识信息、个人健康生理信息、个人教育工作信息、个人财产信息等
	组织数据	政府部门、企事业单位、团体资源信息、企业经营管理信息、业务信息等
	城市部件	指非个人或组织的实体部件，如道路、建筑、视频捕捉设备等
共享类型	无条件共享、有条件共享和不予共享	/
开放类型	无条件开放、有条件开放和不予开放	/
来源机构	交通运输局、教育局等	/
行政层级	国家级、省级、市级、区级、其他	/
来源系统 <sup>a</sup>	自建、国直、省直、市直	/
来源途径	系统产生数据、采购数据、共享渠道获取数据和其他渠道获取数据	/
结构化特征	结构化、半结构化和非结构化	/
产生频率	每秒、分、时、天、周、月、季度、半年、年，实时，不定期，不更新等	/
加工程度	原始数据、衍生数据	脱敏数据、标签数据、统计数据、融合数据
使用频率	冷数据	离线的数据，长期存档的数据，很少被访问和使用的数据等
	温数据	经常被访问和使用的数据等
	热数据	需要被计算节点频繁访问的在线类数据等
<sup>a</sup> 根据GDZW 0031—2020 广东省政务信息资源目录编制指南进行分类。		

附 录 B  
(资料性)  
影响程度参考示例

表 B.1 参考 GB/T 43697—2024 给出了数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，不同影响对象对应的影响程度参考示例。

表B.1 影响程度参考示例

影响对象	影响程度	参考说明
国家安全	特别严重危害	直接影响国家政治安全
	严重危害	关系其他国家安全重点领域，或者对国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等安全造成严重威胁
	一般危害	对国土、军事、经济、文化、社会、科技、电磁空间、网络、生态、资源、核、海外利益、太空、极地、深海、生物、人工智能等安全造成威胁
经济运行	特别严重危害	1) 直接影响关系国民经济命脉的重要行业和关键领域的经济利益安全，如涉及国家安全的行业、提供重要公共产品的行业、重要资源行业等 2) 直接影响关系国民经济命脉的重点产业、重大基础设施、重大建设项目以及其他重大经济利益安全 3) 对一个或多个行业领域的经济发展、业务生产、技术进步、产业生态造成特别严重危害，如对支柱产业和高新技术产业中的重要骨干企业造成重大损害，导致大面积业务中断、大量业务处理能力丧失等 4) 对一个或多个省级行政区的经济运行造成特别严重危害，例如导致大范围停工停产、大规模基础设施长时间中断运行等
	严重危害	1) 直接影响宏观经济运行状况和发展趋势，如社会总供给和总需求、国民经济总值和增长速度、国民经济主要比例关系、物价总水平、劳动就业总水平与失业率、货币发行总规模与增长速度、进出口贸易总规模与变动等 2) 直接影响一个或多个地区、行业内多个企业或大规模用户，对行业发展、技术进步和产业生态等造成严重影响，或者直接影响行业领域核心竞争力、核心业务运行、关键产业链、核心供应链等
	一般危害	1) 对单个行业领域发展、业务经营、技术进步、产业生态等造成一般危害，如受影响的用户和企业数量较小、生产生活区域范围较小、持续时间较短、社会负面影响较小 2) 对单个行业领域或地区的经济运行造成一般危害
社会秩序	特别严重危害	1) 关系重要民生，直接影响人民群众重要民生保障的事项、物资、工程或项目等 2) 直接导致特别重大突发事件、特别重大群体性事件、暴力恐怖活动等，引起一个或多个省级行政区大部分地区的社会恐慌，严重影响社会正常运行
	严重危害	1) 直接导致重大突发事件、重大群体性事件等，影响一个或多个地区的社会稳定 2) 严重影响人民群众的日常生活秩序 3) 严重影响各级政务部门履行公共管理和公共服务职能
	一般危害	1) 对人民群众的日常生活秩序造成一般影响 2) 直接影响企事业单位、社会团体的生产秩序、经营秩序、教学科研秩序、医疗卫生秩序 3) 直接影响公共场所的活动秩序、公共交通秩序

表B.1 影响程度参考示例（续）

影响对象	影响程度	参考说明
公共利益	特别严重危害	1) 关系重大公共利益，导致一个或多个省级行政区大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员（如 1000 万人以上）无法使用公共设施、获取公开数据资源、接受公共服务 2) 导致特别重大网络安全和数据安全事件，或者导致特别重大事故级别的安全生产事故，对公共利益造成特别严重影响，社会负面影响大 3) 导致特别重大突发公共卫生事件（I 级），造成社会公众健康特别严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件
	严重危害	1) 直接危害公共健康和安全，如严重影响疫情防控、传染病的预防监控和治疗等 2) 导致重大突发公共卫生事件（II 级），造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的事件 3) 导致一个或多个地市大部分地区的社会公共资源供应较长期中断，较大范围社会成员（如 100 万人以上）无法使用公共设施、获取公开数据资源、接受公共服务
	一般危害	对公共利益产生一般危害，影响小范围社会成员使用公共设施、获取公开数据资源、接受公共服务等
组织权益	特别严重危害	导致组织遭到监管部门严重处罚（如取消经营资格、长期暂停相关业务等），或者影响重要/关键业务无法正常开展的情况，造成重大经济或技术损失，严重破坏机构声誉，企业面临破产
	严重危害	导致组织遭到监管部门处罚（如一段时间内暂停经营资格或业务等），或者影响部分业务无法正常开展的情况，造成较大经济或技术损失，破坏机构声誉
	一般危害	导致个别诉讼事件，或在某一时间造成部分业务中断，使组织的经济利益、声誉、技术等轻微受损
个人权益	特别严重危害	个人信息主体遭受重大的、不可消除的、可能无法克服的影响，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害。如遭受无法承担的债务、失去工作能力、导致长期的心理或生理疾病、导致死亡等
	严重危害	个人信息主体遭受较大影响，个人信息主体克服难度高，消除影响代价较大。如遭受诈骗、资金被盗用、被银行列入黑名单、信用评分受损、名誉受损、造成歧视、被解雇、被法院传唤、健康状况恶化等
	一般危害	个人信息主体会遭受困扰，但尚可以克服。如付出额外成本、无法使用应提供的服务、造成误解、产生害怕和紧张的情绪、导致较小的生理疾病等



附 录 C  
(资料性)  
数据级别变更情形

### C.1 影响数据级别变化因素

数据级别变更的主要因素如下：

- a) 数据聚合因素：因业务需要将相同或不同级别的数据汇聚并进行分析、处理，导致数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围、可控程度等发生较大变化时，应重新定级；
- b) 数据时效因素：数据在不发生变化的情况下，因为其超过授权时间后，导致数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围、可控程度等发生较大变化时，应重新定级；
- c) 数据处理因素：当数据进行汇总、分析、加工后产生的衍生数据，若与原始数据之间存在较大差异，应对新产生的数据重新定级；
- d) 数据场景因素：在数据应用场景发生变化时，导致数据遭到篡改、破坏、泄露或者非法获取、非法利用后的影响对象、影响程度、影响范围、可控程度等发生较大变化时，应重新分级。

### C.2 影响数据级别变更场景

#### C.2.1 变更场景

当数据状态、服务范围等发生变化，导致数据敏感程度以及发生泄露、篡改、滥用后的影响对象、影响程度、影响范围发生较大变化时，应按照 7.2.4 重新对数据进行分级。

#### C.2.2 升降级情况

数据安全级别升降级有 2 种情况：

- a) 在原始数据发生变化时需要重新进行级别判定，此时数据可能发生升级或降级；
- b) 数据在不发生变化的情况下，因为一定时间或发生一定事情后，失去或具有其敏感性。

#### C.2.3 升降级原则

升降级有以下 4 点原则：

- a) 从原始数据中直接复制部分出来的新数据，安全级别不高于原有安全级别；
- b) 从多个原始数据合并的新数据，不低于原有安全级别；
- c) 对不同数据选取部分数据进行合并形成的新数据，根据内容的关键要素进行重新安全级别判定；
- d) 数据内容不发生变化进行升降级，需有明确的敏感内容失效或生效依据。

附 录 D  
(资料性)  
加工程度维度的数据分类

按照数据加工程度不同，数据通常可分为原始数据、脱敏数据、标签数据、统计数据、融合数据，其中脱敏数据、标签数据、统计数据、融合数据均属于衍生数据，数据类别、类别定义和数据示例见表 D. 1。

表 D. 1 加工程度维度的数据分类

数据类别	类别定义	数据示例
原始数据	公共管理和服务机构采集未经加工处理的数据	如采集的原始数据等
脱敏数据	对数据（如个人信息）按照脱敏规则进行数据变形处理后的新数据	如去标识化的手机号码（如138*****6）等，个人信息去标识化、匿名化处理后的数据属于脱敏数据
标签数据	对用户个人敏感属性等数据进行区间化、分级化、统计分析后形成的非精确的模糊化标签数据	偏好标签、关系标签等
统计数据	即群体性综合性数据，是由多个用户个人或实体对象的数据进行统计或分析后形成的数据	如群体用户位置轨迹统计信息、群体统计指数、交易统计数据、统计分析报表、分析报告方案等
融合数据	对不同业务目的或地域的数据汇聚，进行挖掘或聚合	如多个业务、多个地市的数据整合、汇聚等

## 参 考 文 献

- [1] GB/T 4754—2017 国民经济行业分类与代码
- [2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
- [3] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
- [4] GB/T 25069—2022 信息安全技术 术语
- [5] GB/T 35273—2020 信息安全技术 个人信息安全规范
- [6] GB/T 35274—2017 信息安全技术 大数据服务安全能力要求
- [7] GB/T 35295—2017 信息技术 大数据 术语
- [8] GB/T 37973—2019 信息安全技术 大数据安全管理指南
- [9] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
- [10] GB/T 38667—2020 信息技术 大数据 数据分类指南
- [11] DB44/T 2109—2018 政务信息资源标识编码规范
- [12] DB4403/T 271—2022 公共数据安全要求
- [13] GDZW 0031—2020 广东省政务信息资源目录编制指南
- [14] TC260—PG—20212A 网络安全标准实践指南—网络数据分类分级指引
- [15] 广东省政务服务数据管理局. 广东省数据资源“一网共享”平台数据资源分类分级指南: 粤政数函〔2022〕666号. 2022年
- [16] 深圳市第七届人民代表大会常务委员会. 深圳经济特区数据条例: 深圳市第七届人民代表大会常务委员会公告〔第十号〕. 2021年