ICS 35.240.70
CCS L 70

DB3203

徐 州 市 地 方 标 准

DB 3203/T 1024—2023

公共数据分类分级指南

Guidelines for public data classification and grading

2023－05－08 发布　　2023－05－30 实施

徐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。

本文件由徐州市大数据管理中心提出。

本文件由徐州市政务服务管理办公室归口。

本文件起草单位：徐州市大数据管理中心、中国电子系统技术有限公司、中电国泰（江苏）数字技术有限公司。

本文件主要起草人：陈炜、王冠、董海、李岩、杨欣欣、庄艳、赵欣磊、宋远臣、戴冰、马强。

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原则、方法、流程、变更的建议和指导，以及公共数据的安全分级管控要求。

本文件适用于徐州市公共数据的分类分级工作。

本文件不适用于涉及国家秘密的数据和军事数据的分类分级工作。

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 4754—2017 国民经济行业分类

GB/T 21063.4—2007 政务信息资源目录体系 第4部分：政务信息资源分类

GB/T 38667—2020 信息技术 大数据 数据分类指南

3 术语和定义

下列术语和定义适用于本文件。

3.1

公共管理和服务机构 public management and service institutions

各级国家机关、法律法规授权的具有管理公共事务职能的组织、公共企事业单位。

3.2

公共数据 public data

公共管理和服务机构为履行法定职责、提供公共服务收集、产生的，以电子或者其他方式对具有公共使用价值的信息的记录。

3.3

数据分类 data classification

根据数据资源的属性或特征，将其按照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，以便更好地管理和使用数据。

3.4

数据分级 data grading

根据数据的敏感程度和数据遭篡改、破坏、泄露或非法利用后对受侵害客体的影响程度，按照一定的原则和方法进行定级。

3.5

敏感数据 sensitive data

相关组织、机构和个人收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的公共数据，包括但不限于个人敏感信息。

注1：个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。

注2：个人敏感信息是指一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3.6

数据采集 data collection

组织机构内部系统中新产生公共数据，以及从外部系统收集公共数据的阶段。

3.7

数据传输 data transmission

公共数据从一个实体传输到另一个实体的阶段。

3.8

数据存储 data storage

公共数据以任何数字格式进行物理存储或云存储的阶段。

3.9

数据处理 data processing

公共数据操作的系统执行，包括对公共数据进行计算、分析、可视化等操作。

3.10

数据共享 data sharing

公共管理和服务机构因履行职责需要使用其他公共管理和服务机构的数据或者为其他公共管理和服务机构提供数据的行为。

3.11

数据开放 data opening

公共管理和服务机构面向个人、法人和其他组织提供具有原始性、可机器读取、可供社会化利用的数据集的公共服务。

3.12

数据销毁 data destruction

通过对数据及数据存储介质进行相应的操作手段，使数据彻底消除且无法通过任何手段恢复的过程。

4 公共数据分类

4.1 分类原则

4.1.1 系统性

按照公共数据的多维特征及其相互间客观存在的逻辑关联进行科学化和系统化的分类。

4.1.2 扩展性

数据分类应具有概括性和包容性，能够实现各种类型公共数据的分类，以及满足将来可能出现的数据类型。

4.1.3 准确性

使用的词语或短语应能准确表达数据类目的实际内容、内涵和外延，相同概念的用语应保持一致。

4.1.4 实用性

应结合现实需求，符合用户对公共数据区分和归类的普遍认知。每个类目下都应有公共数据，不设没有意义的类目。原则上同一分类维度内，同一条公共数据只分入一个类目。

4.1.5 时效性

提供数据的公共管理和服务机构应定期评估分类维度、方法、结果的合理性，根据实际需要进行动态调整。

4.2 分类维度

4.2.1 数据管理维度

应从元数据角度对公共数据进行数据管理维度分类，主要包括：

——数据产生频率：根据数据产生的频率（单位时间内产生的数据量或达到指定数据量的频率）对数据进行分类，数据产生与更新的单位周期可分为：每秒、分、时、天、周、月、季度、半年、年，不定期，不更新等；

——数据产生方式：根据公共数据产生方式，可分为人工采集数据、信息系统产生数据、感知设备产生数据，原始数据、二次加工数据等；

——数据结构化特征：根据公共数据的结构化特征，可分为结构化数据、半结构化数据和非结构化数据；

——数据存储方式：根据公共数据储存方式，可分为关系型数据库存储数据、键值数据库存储数据、列式数据库存储数据、图数据库存储数据、文档数据库存储数据等；

——数据质量要求：根据数据完整性、时效性、准确性等维度的质量要求对数据进行分类。

4.2.2 业务应用维度

对公共数据进行业务应用维度分类，主要包括：

——数据产生来源：根据数据产生的实际情景对数据进行分类，包括数据产生主体和数据权属，数据产生主体如人工、机器、传感器、应用软件、信息系统等；

——数据所属行业：根据数据内容所属的行业对数据进行分类；

——数据应用领域：根据数据应用领域分类体现公共数据对数字化改革的支撑作用；

——数据使用频率：根据数据使用的频率进行分类，综合考虑数据的访问频次和分析引用层面；

——数据共享属性：根据数据共享属性分类；

——数据开放属性：根据数据开放属性分类。

4.2.3 其他分类维度

其他分类维度如安全保护维度和数据对象维度，安全保护维度从数据的重要程度等对公共数据进行安全保护维度分类。

4.3 分类方法

4.3.1 分类概述

在主题、行业、对象、来源部门、共享属性、开放属性等多个维度对公共数据进行分类，对于每个维度采用线分类法将其分为大类、中类和小类三级。公共管理和服务机构按上述方法进行分类，可以根

据业务需要对小类之后再行细分。对小类的细分，可以根据业务数据的性质、功能、技术手段等一系列问题进行扩展细分。

4.3.2 按主题分类

按照数据资源所涉及的主题范畴，参考GB/T 21063.4—2007的规定，将公共数据按照主题进行分类，采取大类、中类和小类三级分类法。

按主题将大数据分为以下基础大类：生活服务、设立变更、文物保护、医疗卫生、行业准营、“三农”服务、工程建设、社会保障、民族宗教、教育培训、环境资源、安全生产、交通旅游、职业资格、住房保障、纳税纳费、投资立项、劳动就业、出境入境、涉外服务、破产注销、死亡殡葬、婚育收养、其他。

其他主题可以作为扩展主题，即分类不满足工作需要，可另行根据实际业务情况建立主题。

4.3.3 按行业分类

根据数据资源所涉及的行业领域范畴，按照GB/T 4754—2017的规定，将其四级类目的前二级（即门类、大类）对应为行业分类中的大类、小类。

4.3.4 按对象分类

按照公共数据所描述的对象分为个人数据、组织数据、客体数据三类：

——个人数据是指自然人的属性数据和行为数据，属性数据包括但不限于姓名、证件信息、户籍信息、联系地址信息等，行为数据包括但不限于交通出行、投资资产等；

——组织数据指政府部门、企事业单位、其他法人和非法人组织、社会团体等组织的属性数据和业务数据，属性数据包括但不限于名称、编码、证件信息等，业务数据包括但不限于税务、资本资产、社保公积金等；

——客体数据指非个人或组织的客观实体（如河流、道路、建筑）的属性数据和感应数据，包括但不限于基础设施、位置、指标参数、运行状态、气象数据、空气质量、水质等数据。

4.3.5 按来源部门分类

依据数据来源，按照公共管理和服务机构设置分类，根据徐州市实际的公共管理和服务机构设置对数据的部门分类进行实时调整分类。

4.3.6 按共享属性分类

依照数据共享属性，数据分为无条件共享、有条件共享、不予共享：

——无条件共享数据：可以提供给所有公共管理和服务机构共享使用的公共数据属于无条件共享类；

——有条件共享数据：可以按照一定条件提供给有关公共管理和服务机构共享使用的公共数据依据不同程度分为一般条件共享类和严格条件共享类；

——不予共享数据：不宜提供给其他公共管理和服务机构共享使用的公共数据属于不予共享类。

4.3.7 按开放属性分类

依照数据开放属性，数据分为无条件开放、有条件开放、不予开放：

——无条件开放数据：公共管理和服务机构应当通过公共数据平台主动向社会开放无条件开放类公共数据，公民、法人和其他组织登录即可获取、使用；

——有条件开放数据：在法律法规允许限定对象、用途、使用范围等特定条件下可以提供给公民、法人和其他组织使用的公共数据属于一般条件开放类或严格条件开放类。公共管理和服务机构应当明确一般条件开放类和严格条件开放类公共数据的开放要求，向符合条件的公民、法人和其他组织开放；

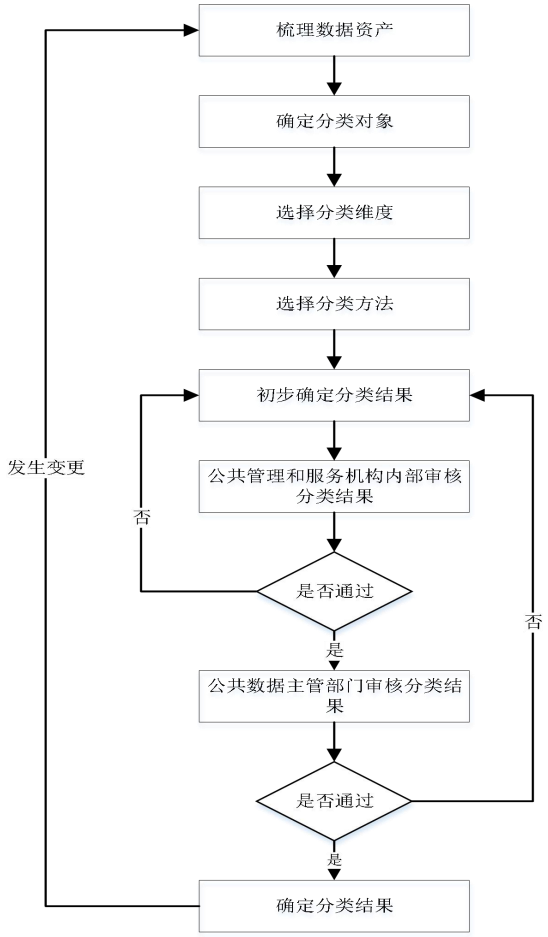
——不予开放数据：应当依法予以保密的公共数据以及法律、法规、规章规定不得开放的其他公共数据属于不予开放类。

4.3.8 其他分类法

具体分类方法可参考GB/T 38667—2020第8章的相关要求。

4.4 分类流程

数据分类流程见图1。



[a] 确定分类对象：根据数据的业务类型、应用场景、产生来源等特性确定分类对象。

[b] 选择分类维度：选择分类维度，梳理分类视角的数据特征和根据数据特征选取分类维度。

[c] 选择分类方法：选择分类方法过程需明确分类维度的排列顺序和组合方式。

[d] 确定分类结果：初步确定分类结果。

[e] 公共管理和服务机构内部审核分类结果：测试评估本机构内的数据分类情况，给出审核结果和意见。

[f] 公共数据主管部门审核分类结果：公共数据主管部门审核分类结果。

图 1 数据分类流程

4.5 分类变更

4.5.1 变更类型

分类变更包含新增分类、修改分类、删除分类。

4.5.2 变更原则

分类变更过程需符合本文件中定义的分类原则、要求、维度及方法，变更流程经审批通过后执行变更操作。

4.5.3 变更流程

变更申请需明确变更类型、变更范围以及变更原因，变更审核不通过的需返回未通过原因，对于删除类的变更，申请单位需提供相对应的数据处置方案。

5 公共数据分级

5.1 分级原则

5.1.1 依法依规

数据级别划分应满足相关法律、法规及监管要求。

5.1.2 自主定级

各级公共管理和服务机构在采集、存储、传输、处理、共享、开放、销毁公共数据等行为之前，应按照本文件自主对各种类型公共数据进行分级。

5.1.3 综合判定

公共数据的分级是客观且可被校验的，即通过数据自身的属性和分级规则即可判定其分级。应与其共享、开放的类型、范围、审批和管理要求直接相关。应充分考虑数据聚合情况、数据体量、数据时效性、数据脱敏处理等因素。应结合字段的含义和具体应用场景进行定级。在多类数据中均出现的通用数据，可根据实际内容独立分级。

5.1.4 就高从严

应按照就高从严原则确定数据级别，数据集的级别应根据其包含数据项的最高级来定级。

5.1.5 分级管控

各级公共管理和服务机构确定数据等级后，根据数据等级实施分级管控措施，在公共数据全生命周期采取差异化管理措施。

5.1.6 及时更新

数据的分级具有一定的时效性。数据的级别可能因时间变化而按照一些预定的安全策略发生改变。

5.1.7 科学合理

数据级别具有合理性。级别划定过低可能导致数据不能得到有效保护；级别划定过高可能导致不必要的业务开支。

5.2 分级方法

5.2.1 分级概述

数据分级通过定量与定性相结合的方式，首先识别数据分级要素情况，然后对数据因素进行分析，确定数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响的对象和影响程度，最终综合确定数据级别。

5.2.2 分级要素

数据分级的要素，包括数据领域、群体、区域、精度、规模、深度、覆盖度、重要性、安全风险等，其中领域、群体、区域、重要性、安全风险通常属于定性要素，精度、规模、覆盖度属于定量要素，深度通常作为衍生数据的分级要素。识别数据定级要素相关情况。分级要素定义见附录A。

5.2.3 影响分析

数据分级基于影响分析进行综合判定，影响分析包括：数据发生泄露、篡改、丢失或滥用后的影响对象和影响程度。

5.2.3.1 影响对象

通常包括国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益等，影响对象定义和判断可能对影响对象产生影响的常见考虑因素见附录B。

5.2.3.2 影响程度

影响程度从高到低划分为四个程度分别是严重危害、一般危害、轻微危害和无危害，影响程度参考示例见附录C，可作为危害程度判别的参考；影响程度的确定需综合考虑数据类型、数据特征、数据规模等因素，并结合业务属性确定数据安全性遭到破坏后的影响程度。

5.2.4 分级规则

公共数据分级按照基本级别、细分级别划分，基本级别从低到高分为一般数据、重要数据、核心数据三个级别；细分级别对应到基本级别，从低到高分为一级到四级，数据分级后需与数据的开放和共享形成对应。分级规则见表1。

表1 分级规则

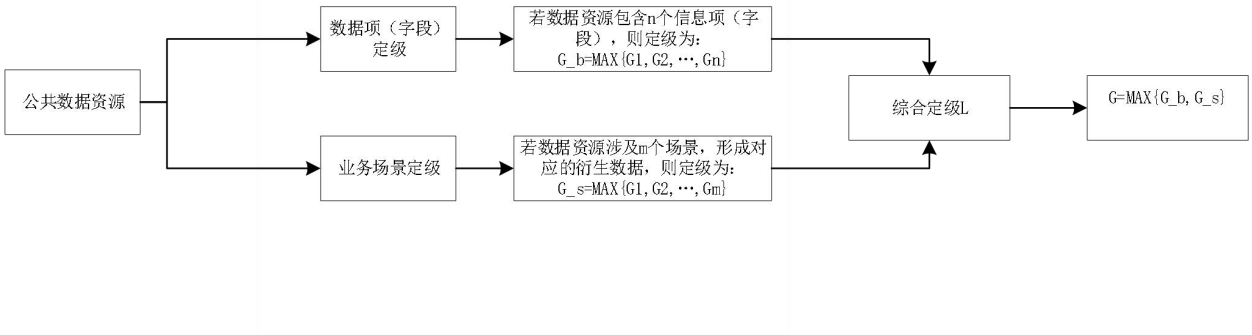
<table>
<tr><th rowspan="2">基本级别</th><th rowspan="2">细分级别</th><th rowspan="2">敏感程度</th><th colspan="6">影响对象</th><th rowspan="2">共享属性</th><th rowspan="2">开放属性</th></tr>
<tr><th>国家安全</th><th>经济运行</th><th>社会稳定</th><th>公共利益</th><th>个人权益</th><th>组织权益</th></tr>
<tr><td>核心数据</td><td>四级</td><td>高敏感数据</td><td>一般危害、严重危害</td><td>严重危害</td><td>严重危害</td><td>严重危害</td><td>严重危害</td><td>严重危害</td><td>有条件共享/不予共享</td><td>不予开放</td></tr>
<tr><td>重要数据</td><td>三级</td><td>敏感数据</td><td>轻微危害</td><td>轻微危害、一般危害</td><td>轻微危害、一般危害</td><td>轻微危害、一般危害</td><td>一般危害</td><td>一般危害</td><td>有条件共享/不予共享</td><td>有条件开放/不予开放</td></tr>
<tr><td rowspan="2">一般数据</td><td>二级</td><td>低敏感数据</td><td rowspan="2">无危害</td><td rowspan="2">无危害</td><td rowspan="2">无危害</td><td rowspan="2">无危害</td><td>轻微危害</td><td>轻微危害</td><td>无条件共享/有条件共享</td><td>有条件开放</td></tr>
<tr><td>一级</td><td>不敏感数据</td><td>无危害</td><td>无危害</td><td>无条件共享</td><td>无条件开放</td></tr>
</table>

5.3 定级实施

5.3.1 定级概述

根据影响分析和分级规则对库表、文件、接口存储和传输的数据做定级。对于没有分级的公共数据，暂时不予开放，待确定等级之后安全有序开放。

数据资源的等级划分要结合数据项（字段）和业务场景进行综合判定并实施定级，公共数据级别判定流程包括数据项（字段）定级、业务场景定级、综合定级三个步骤，最后按照就高从严、综合判定的原则确定数据资源安全等级，具体分级示例见附录D，数据级别判定流程见图2。



[a] 数据项（字段）定级。依据字段含义，按照数据分级规则，对待定级的数据资源包含的所有数据项（字段）进行等级划分，数据资源定级为其包含的数据项的最高安全等级，记为G_b；

[b] 业务场景定级。依据数据资源的业务场景，根据原始数据在业务场景中可形成的衍生数据情况，判断衍生数据的安全等级，数据资源定级为其业务场景下衍生的数据的最高安全等级，记为G_s；

[c] 综合定级。步骤1的数据项（字段）定级G_b与步骤2的业务场景定级G_s，两者取最大值作为待定级数据资源的最终定级G=MAX{G_b,G_s}。

图2 数据级别判定流程

5.3.2 数据项定级

根据数据项定级可参考如下规则：

a) 已合法公开披露的公共数据可定为一级；法律法规规章未明确要求公开的个人信息等级不得低于二级；法律法规明确要求保护的公共数据，数据安全等级应定为三级以上；

b) 一般个人信息不低于二级；敏感个人信息不低于三级；个人一般信息和敏感信息参考清单见附录E；

c) 对于在库表、数据文件存储的数据分级标记应细化至数据的字段级，相关库表、文件的级别按照包含字段的最高安全级别定级；

d) 对数据接口定级按照其响应请求返回字段中安全级别最高的字段级别定级。

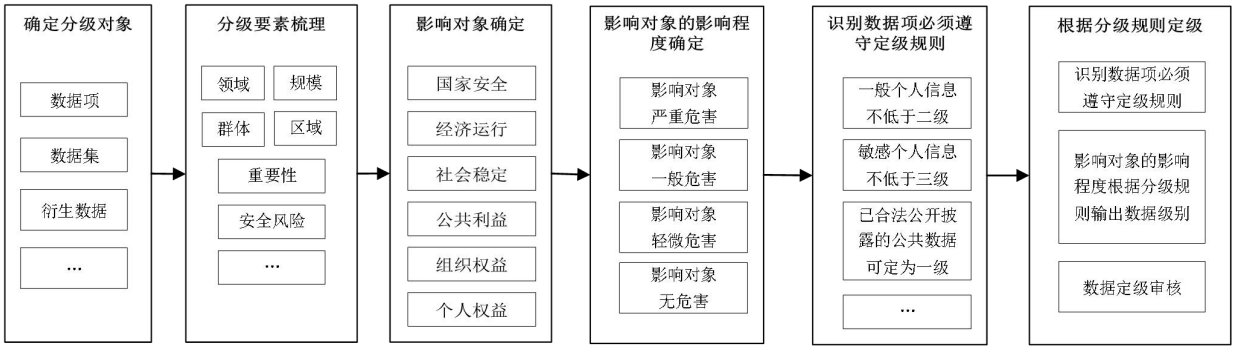
5.3.3 业务场景定级

对有数据融合场景的应用数据，注意根据数据融合风险对数据定级，应结合场景、数据可整合关联的信息综合判定数据级别，因数据整合应用产生更高级别的敏感度的情况下，按照高级别的敏感度定级；例如：数据集A采用了屏蔽身份证号码中间8位的匿名处理后开放方式（样例数据：320324********4321），但数据表字段B可获取自然人的出生年月日8位数，两个数据集整合后可能存在泄露个人信息的情况，需

对数据集A改变匿名方式或者对上述两个字段重新定级，对于无法评估或者不能完全清楚的潜在不确定风险，建议通过组织专家评审方式数据定级。

5.3.4 定级实施流程

数据定级实施流程见图3。



[a] 确定分级对象。确定待分级的数据，如数据项、数据集、衍生数据等。

[b] 识别分级要素。识别数据的领域、群体、区域、精度、规模、深度、重要性、安全风险等分级要素情况。

[c] 确定影响对象。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响的范围，包括个人利益相关、公共利益相关、社会秩序相关、国家安全相关。

[d] 确定影响程度。确定该类数据安全属性（完整性、保密性、可用性）遭到破坏后可能影响程度，包括严重、一般、轻微、无。

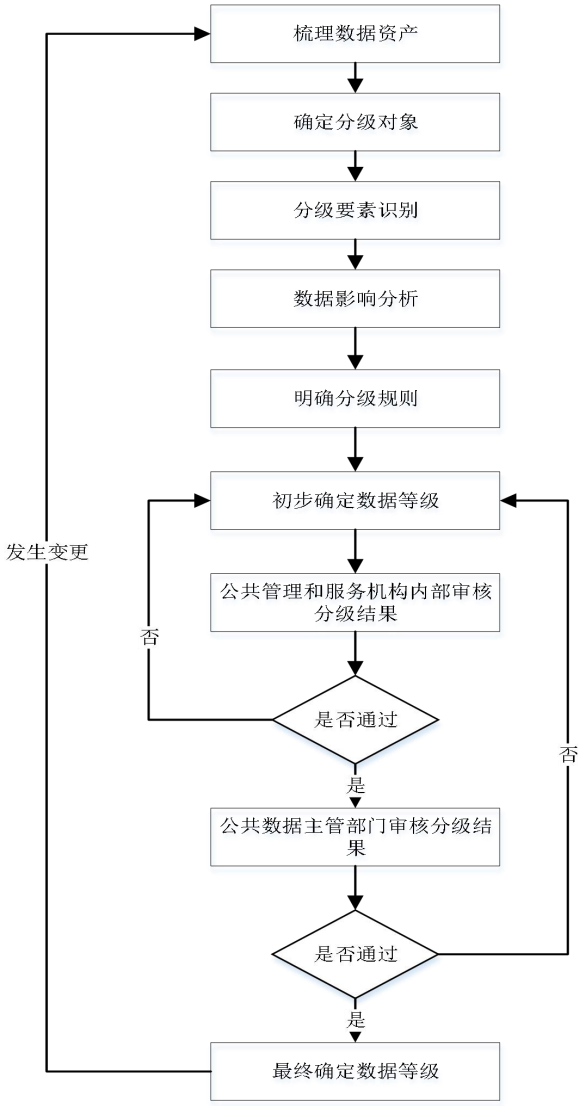
[e] 数据定级综合判别。必须遵守原则包括已合法公开披露的公共数据可定为一级；法律法规规章未明确要求公开的个人信息等级不得低于二级；法律法规明确要求保护的公共数据，数据安全等级应定为三级以上；其他数据参考上文判定标准自主定级。

[f] 数据定级。综合上述步骤确定的该类数据安全属性（完整性、保密性、可用性）遭到破坏后的影响对象、影响范围、影响程度，对数据进行定级。

图 3 数据定级实施流程

5.4 分级流程

数据分级流程见图4。



[a] 数据分级：公共管理和服务机构按照本文件指导实施数据分级工作，工作步骤包括确定分级对象、分级影响要素识别、数据影响分析、明确分级规则并初步确定数据等级。

[b] 公共管理和服务机构内部审核分级结果：公共管理和服务机构应对数据的分级结果进行内部审核。

[c] 公共数据主管部门审核分级结果：公共数据主管部门审核数据分级结果。

图 4　数据分级流程

5.5　分级变更

对于需要进行级别变更的数据，按照分级原则要求重新进行分级。

5.5.1　变更原则

数据安全级别变更必须遵循以下的原则：

a)　从原始数据中直接部分复制出来的新数据级别不应高于原有数据级别；

b)　从多个原始数据直接合并的新数据不应低于原有数据最高级别；

c)　对不同数据选取部分数据进行合并形成的新数据，应根据新数据的关键要素进行重新判定；

d)　数据内容不发生变化时，进行级别变更时需有明确的依据；

e） 安全级别变更时，应由本组织机构的主要领导人进行审批同意；
f） 汇聚数据的安全级别须经数据使用方和数据资源管理机构联合评估确认后进行判定。

5.5.2 变更制度

公共数据分级变更必须遵守以下变更制度要求，除本变更制度规定以外任何形式的变更通知均不予接受：

a） 变更类型包含：新增分级、修改分级、删除分级；变更范围包含：维度变更和级别调整；
b） 数据变更需符合本文件中定义的分级原则、要求、维度及方法；
c） 变更申请单需明确变更类型、变更范围以及变更原因；
d） 审核不通过的两种情况：内部审核不通过的直接结束流程并返回不通过原因，数据审核部门审核不通过的则返回申请人重新提交变更申请并返回不通过原因；
e） 进入执行阶段的流程不可进行取回、回退、中断等操作；
f） 对于删除类的变更，申请单位需提供相对应的数据处置方案。

5.5.3 变更场景

公共数据分级完成以后，出现以下情形之一时，宜对相关数据的安全级别进行变更，并按照数据分级办法对变更后的数据重新分级，安全级别变更情况包括：

a） 数据内容发生变化，导致原有数据的安全级别不适用变化后的数据；
b） 数据内容未发生变化，但因数据时效性、数据规模、数据使用场景、数据加工处理方式等发生变化，导致原定的数据安全级别不再适用；
c） 因数据汇集融合，导致原有数据安全级别不再适用汇聚融合后的数据；
d） 因国家和行业主管部门要求或新政策法规要求，导致原定的安全级别不再适用；
e） 需要对数据安全级别变更的其他情况。

5.5.3.1 安全级别提升

发生以下场景时，应考虑提升数据级别：

a） 聚合多家业务部门数据；
b） 大量数据进行聚合；
c） 发生特定事件导致数据具有敏感性。

5.5.3.2 安全级别降低

发生以下场景时，可考虑降低数据级别：

a） 数据已被公开或披露；
b） 数据进行脱敏或删除关键字段；
c） 数据经过较长时间（需明确数据含义和时间点）；
d） 发生特定事件导致数据失去敏感性时。

5.6 分级管控

5.6.1 各级数据共享开放要求

对于各级数据对应的共享开放要求见表2。

表 2　各级数据共享开放要求

基本级别	细分级别	敏感程度	共享属性	开放属性	共享开放要求
核心数据	四级	高敏感数据	有条件共享/不予共享	不予开放	对于四级数据的共享需要通过专家委员会一事一议，四级数据不予开放。技术能力上，使用两种以上方式对数据使用者身份鉴权，具备网络流向控制、请求控制和限流，建立专门的数据流转通道；保证系统高可用性；必须对数据进行脱敏处理；具备数据溯源能力，对开放、共享过程进行日志记录和评审；业务结束后以不可逆方式销毁数据，对销毁过程有审批、记录、监督。
重要数据	三级	敏感数据	有条件共享/不予共享	有条件开放/不予开放	有条件共享适用于二级、三级、四级敏感数据。管理监督上，需要明确数据共享目的、用途和范围；评估认定数据共享、开放不产生轻微以上的影响，对数据安全问题可控制；需数据使用方依法合规使用数据；严格审批流程。技术能力上，对数据使用者能够进行身份鉴权；具备网络流向控制，建立专门的数据流转通道；保证系统高可用性，具备数据脱敏处理能力；对共享过程进行日志记录和审计；业务结束后采用删除、覆盖和格式化方式销毁数据，确保销毁数据不可恢复并对销毁过程有审批、记录、监督。有条件开放适用于二级、三级敏感数据。管理监督上，需要确保数据开放的目的、用途和范围，原则上向特定对象授权使用；评估认定数据开放不产生一般以上的影响，对数据安全问题全程可控，数据使用者依法合规使用数据；严格规范整个审批流程。
一般数据	二级	低敏感数据	无条件共享/有条件共享	有条件开放	
	一级	不敏感数据	无条件共享	无条件开放	一级数据无条件共享，无条件开放。

5.6.2　数据全生命周期分级管控

不同级别数据对其数据生命周期进行差异化的管控，按照采集、传输、存储、处理、共享、开放、销毁等阶段实施数据生命周期分级管控，具体管控要求见附录F。

5.6.3　数据各类形态分级管控

5.6.3.1　数据形态

数据存在形态一般分为原始数据、统计数据、脱敏数据，数据形态描述见表3。

表 3　数据形态

数据形态	描述
原始数据	汇聚数据的原本形式和内容，没做任何加工处理。
脱敏数据	对各类敏感数据所包含的敏感信息进行模糊化、加扰、加密或转换后（如：对身份证号码进行不可逆置换，但仍保持相应格式）形成的，无法通过推算演绎（含逆向推算、枚举推算等）、关联分析等方式识别出敏感信息的新数据。
统计数据	通过对采集的数据（如税务数据、移动运营商数据、市民刷卡交易统计数据）等进行统计分析、挖掘、统计，以图形、图像处理、计算机视觉以及用户界面的技术，通过表达、建模以及对立体、表面、属性加以动画的显示，对数据加以统计及可视化等。

5.6.3.2　数据各类形态分级管控要求

数据三种形态在数据共享、开放、处理时应遵循的分级管控要求：

——一级数据在共享时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在共享时，允许以原始数据、脱敏数据以及统计数据形态经加密处理后提供；四级数据在共享时，不允许以原始数据、脱敏数据形态提供，允许以统计数据形态经加密处理后提供。

——一级数据在开放时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在开放时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态经加密处理后提供；四级数据在开放时，不允许以原始数据、脱敏数据形态提供，允许以统计数据形态经加密处理后提供。

——一级数据在部门内加工、分析时，允许以原始数据、脱敏数据以及统计数据形态提供；二级、三级数据在部门内加工、分析时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态提供；四级数据在部门内加工、分析时，不允许以原始数据形态提供，允许以脱敏数据、统计数据形态经加密处理后提供。

5.6.4　数据内部处理分级管控

数据除了用于共享及对外开放之外，还涉及数据所有者对于数据的处理、分析挖掘等过程，主要对象为内部人员，所有的数据集的使用安全管理过程应按照数据项融合后的最高级别进行，数据内部处理分级管控见表4。

表 4　数据内部处理分级管控要求

数据等级	数据内部处理分级管控
一级	1.可以以原始数据的方式被授权访问。 2.应保证使用被授权的账号进行数据访问，并且该账号可以定位到个人。 3.申请授权时应明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.应对数据加工、分析等处理环节的操作行为建立日志，日志保存期限应不少于 6 个月。 5.在终端上分析、加工数据后，不应保存原始数据。
二级	1.原则上以脱敏数据和统计数据的方式被访问，因业务需要原始数据时，需通过审批。 2.需使用被授权的账号进行数据访问，该账号可以定位到个人。 3.需过审批授权后，进行应用认证和授权处理的方式访问数据。数据申请时明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.应对数据加工、分析等处理环节的操作行为建立日志，日志保存期限应不少于 1 年。 5.当需要导出到终端上分析、加工数据时，需在平台上通过二次审批并下发导出安全策略，分析完成后终端上不允许保留导出数据。 6.远程加工、分析数据时，应严格限制数据加工、分析终端的外部接入 IP 数量和地址。 7.使用网络 DLP 设备对终端进行敏感数据识别和发现；应对加工、分析产生的新数据设置级别标签，分析后的结果应通过风险评估、审核审批之后方可发送给数据需求方。
三级	1.原则上以脱敏数据和统计数据的方式被访问，因业务需要原始数据时，需通过审批，审批级别高于二级数据。 2.需要使用被授权的账号进行数据访问，该账号可以定位到个人。 3.需通过审批授权后，进行应用认证和授权处理的方式访问数据。申请时明确数据加工、分析的目标和范围，确保加工前后数据映射关系。 4.应对数据加工、分析等处理环节的操作行为建立日志，日志保存期限应不少于 3 年。 5.保证数据仅能在内部进行数据加工、分析操作，并采取技术措施禁止远程加工、分析数据。 6.通常情况下不允许导出到终端上分析、加工数据，如分析需要，需在平台上通过二次审批并下发导出安全策略，终端上不允许保留导出数据。 7.使用网络 DLP 设备对终端进行敏感数据识别和发现；应对加工、分析产生的新数据设置级别标签，分析后的结果应通过风险评估、审核审批之后方可发送给数据需求方。
四级	不允许数据处理者直接访问四级数据。

6　监督保障

6.1　职责划分

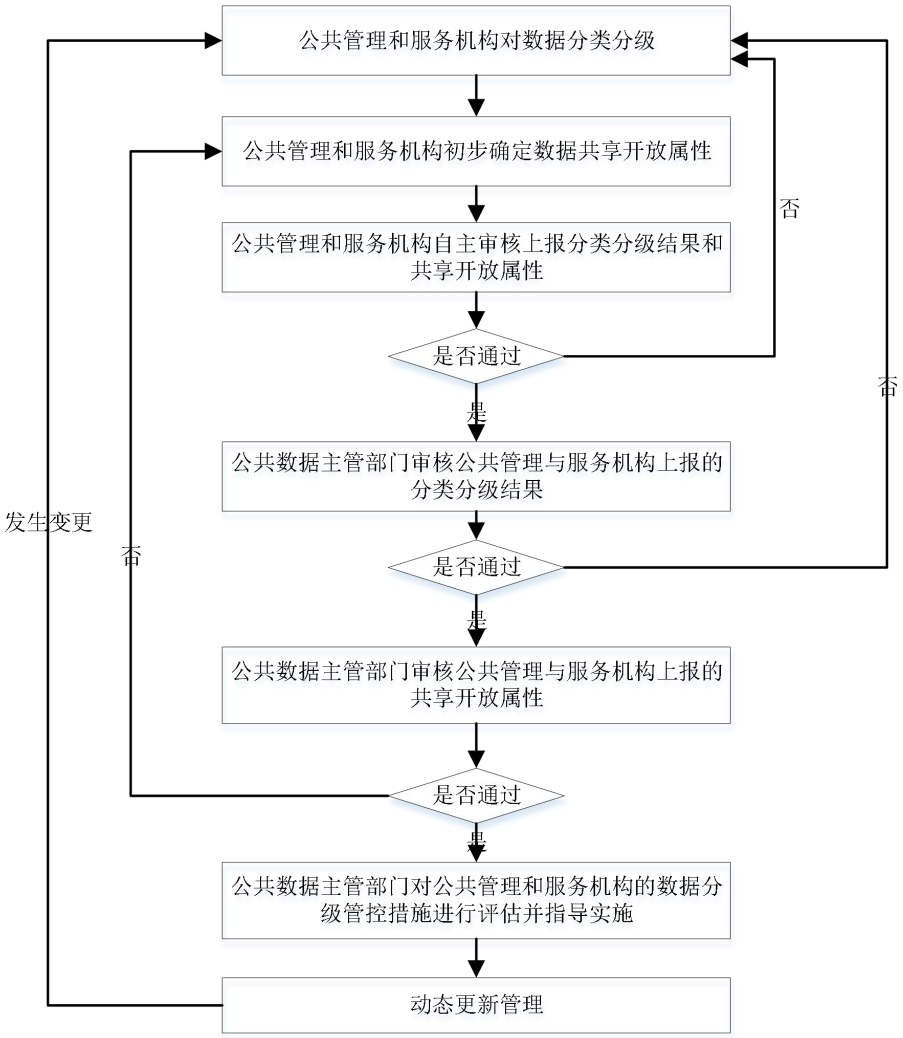
公共数据主管部门负责组织、指导、协调、监督公共数据分类分级规范管理，指导、协调行业主管部门制定公共数据分类分级行业规范并督促落实。

行业主管部门负责牵头制定数据分类分级行业规范，结合行业特点，确定相应的管控措施。协调下属公共管理和服务机构落实分类分级行业规范的工作要求。

各公共管理和服务机构严格执行公共数据分类分级规范，建立工作体系，做好本机构公共数据分类分级，落实管控要求。

6.2　管理流程

分类分级管理流程见图5。



[a] 公共管理和服务机构对数据分类分级。公共管理和服务机构结合自身业务，按照本文件初步判定数据的分类类别和数据敏感等级。

[b] 公共管理和服务机构确定共享及开放属性。公共管理和服务机构根据数据分类分级情况确定数据的共享属性和开放属性，对不予共享数据、有条件共享数据、不予开放数据、有条件开放数据，须说明理由和依据。

[c] 公共管理和服务机构自主审核上报分类分级结果和共享开放属性。应对数据在各维度的初步分类分级结果进行部门内部自主检查，检查通过后提交至本级公共数据主管部门审查。

[d] 公共数据主管部门审核分类分级结果。公共数据主管部门对本级公共管理和服务机构的数据分类分级结果进行初步审查，发现数据分类分级明显错误，应指导数据提供方予以更正。

[e] 公共数据主管部门审核公共管理与服务机构数据共享开放属性。对于敏感级别为三级、四级的数据，若需要共享或开放，公共数据主管部门应与公共管理和服务机构核对确认，经过初审之后，然后进一步复审，复审通过后方可共享或开放。

[f] 公共数据主管部门对公共管理和服务机构的数据分级管控措施进行评估并指导实施。公共管理与服务机构对三四级数据的共享、开放、处理等操作的实施方案需经公共数据主管部门评估、审查、批准后实施。

[g] 动态更新管理。分类分级更新，公共数据主管部门应定期组织对分类分级结果的合理性、有效性进行评估，当数据状态、服务范围等方面发生变化时，及时对分类分级结果进行变更，并记录变更过程。

图 5　分类分级管理流程

6.3 管控要求

公共数据主管部门和公共管理和服务机构对各自负责管理的数据实行全生命周期安全管控，严格落实管控要求，设置专职岗位和人员，建立制定与本部门公共数据相适应的机制、措施、技术、工具，确保公共数据在各生命周期安全可控。

6.4 评价机制

公共数据分类分级工作纳入评价管理，公共数据主管部门制定考核评价机制，对各公共管理和服务机构工作成效进行评价。

对于安全级别较高的数据，不遵守此文件分级要求的行为，包括但不限于分级错误、分级正确但未遵守级别对应的安全管控措施，综合安全事件可控程度、涉及数据量大小和数据项数进行综合评价。

附 录 A
（资料性）
分级要素

分级要素定义见表A.1。

表 A.1 分级要素定义

分级要素	定义
领域	数据描述的业务范畴，数据领域识别可考虑数据描述的行业领域、业务条线、生产经营活动、上下游环节、内容主题等因素。
群体	数据描述的主体或对象集合，数据群体识别可考虑数据描述的特定人群、特定组织、网络和信息系统、资源物资、设备设施等因素。
区域	数据涉及的地区范围，数据区域识别可考虑数据描述的行政区划、特定地区、物理场所等。
精度	数据的精确或准确程度，数据精度越高表示采集数据和真实数据的误差越小。数据精度识别可考虑数值精度、空间精度、时间精度等因素。
规模	数据规模及数据描述的对象范围或能力大小，数据规模识别可考虑数据存储量、群体规模、区域规模、领域规模、生产加工能力等因素。
深度	通过数据统计、关联、挖掘或融合等加工处理，对数据描述对象的隐含信息或多维度细节信息的刻画程度。数据深度识别可考虑数据在刻画描述对象的经济运行、发展态势、行踪轨迹、活动记录、对象关系、历史背景、产业供应链等方面的情况。
覆盖度	数据对领域、群体、区域、时段等的覆盖分布或疏密程度。数据覆盖度识别可考虑对特定领域、特定群体、特定区域、时间段的覆盖占比、覆盖分布等因素。
重要性	数据在经济社会发展中的重要程度。重要性识别可考虑数据在经济建设、社会建设、政治建设、文化建设、生态文明建设等的重要程度。
安全风险	主要识别数据可能遭到泄露、篡改、破坏、非法获取、非法利用、非法共享的风险。

附 录 B
（资料性）
影响对象

影响对象常见考虑因素见表B.1。

表 B.1 影响对象常见考虑因素

影响对象	定义	判定影响的常见考虑因素
国家安全	数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响国家政治、国土、经济、科技、文化、社会、生态、军事、网络、人工智能、核、生物、太空、深海、极地、海外利益等领域国家利益安全。	1.影响领土安全、国家统一、边疆安全和国家海洋权益；2.影响基本经济制度安全、供给侧结构性改革、产业链和供应链安全、粮食安全、能源安全、重要资源安全、系统性金融风险、国际开放合作安全；3.影响我国科技实力、科技自主创新、关键核心技术、国际科技竞争力、科技伦理风险、出口 管制物项；4.影响我国文化自信、社会主义核心价值观、文化软实力、中华优秀传统文化等；5.影响我国社会治理体系、社会治安防控体系、应急管理体系等；6. 影响我国生态环境安全、绿色生态发展、污染防治、生态系统质量和稳定性、生态环境领域 国家治理体系等；7.影响我国国防和军队现代化建设等，或者可被其他国家或组织利用发起对我国的军事打击；8. 影响我国网络空间安全、关键信息基础设施安全、新一代人工智能安全，或者可能被利用实 施对关键信息基础设施、核心技术设备等的网络攻击，可能导致特别重大或重大网络安全和 数据安全事件；9.影响核材料、核设施、核活动情况，或可被利用造成核破坏或其他核安全事件；10.影响国家生物安全治理体系、生物资源和人类遗传资源安全、生命安全和生物安全领域的重大科技成果、疾病防控和公共卫生应急体系安全，或者可能导致重大传染病、重大生物安全风险；11.影响我国在太空、深海、极地等领域的国家利益和国际合作安全；12.影响我国企业海外投资、海外重大项目和人员机构安全、海外能源资源安全、海上战略通道安全，或可被利用实施对我国参与国际经贸、文化交流活动的破坏或对我国实施歧视性禁止、限制或其他类似措施。
经济运行	数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响市场经济运行秩序、宏观经济形势、国民经济命脉等经济利益。	1.影响市场准入、市场行为、市场结构、商品销售、交换关系、生产经营秩序、涉外经济关系等市场经济运行秩序；2.影响社会总供给和总需求、国民经济总产值和增长速度、国民经济中主要比例关系、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宏观经济形势；3.影响行业领域的生产、流通、分配、消费等经济活动，产业链、供应链或经济效益；4.影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业、提供重要公共产品的行业、重大基础设施和重要矿产资源行业等国民经济命脉。
社会稳定	数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能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。	1.导致重大突发事件、群体性事件、社会矛盾激化、暴力恐怖活动、社会治安问题等；2.影响人民群众的民生保障或日常生活秩序，如扶贫、就业、收入、教育、文化体育、健康、养老和社保等民生事项或供电、供气、供水等基本服务保障工程；3.影响各级党政机关依法履行公共管理和服务职能；4.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；5.影响公共场所的活动秩序、公共交通秩序。

表B.1影响对象常见考虑因素（续）

影响对象	定义	判断影响的常见考虑因素
公共利益	数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能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。	1.影响对重大疾病尤其是传染病的预防、监控和治疗，或者可能引发突发公共卫生事件、造成社会公众健康危害；2.影响社会成员使用公共设施；3.影响社会成员获取公开数据资源；4.影响社会成员接受公共服务等方面；5.其他影响公共利益、社会秩序等数据。
组织权益	数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能影响法人和其他组织的生产运营、资本资产、声誉形象、公信力、知识产权等。	1.可能导致组织遭到监管部门处罚、安全事件或法律诉讼；2.影响组织的重要或关键业务生产经营；3.造成组织经济损失；4.破坏组织声誉形象、公信力等；5.影响组织的知识产权、技术损失等；6.其他影响法人、非法人组织合法权益的数据。

附 录 C
（资料性）
影响程度

影响对象的影响程度说明见表C.1。

表 C.1 影响对象的影响程度说明

影响对象	影响程度	参考说明
国家安全	严重危害	1.对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成严重威胁，严重影响海外利益、生物、 太空、极地、深海、人工智能等重点领域安全。 2.对本地区、本部门以及相关行业、领域的重要骨干企业、关键信息基础设施、重要资源等造成严重影响。 3.导致对本地区、本部门以及相关行业、领域大范围停工停产、 大面积网络与服务瘫痪、大量业务处理能力丧失。
	一般危害	1.对政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核安全等构成威胁，影响海外利益、生物、太空、 极地、深海、人工智能等重点领域安全。 2.对本地区、本部门以及相关行业、领域生产、运行和经济利益等造成影响。 3.引发的级联效应明显，影响范围涉及多个行业、区域或者行业内多个企业，或者影响持续时间长，对行业发展、技术进步和产业生态等造成严重影响。
	轻微危害	1.对本地区、本部门以及相关行业、领域生产、运行和经济利益等造成轻微影响。 2.影响持续时间短，对行业发展、技术进步和产业生态等造成一般影响。
	无危害	对国家安全不造成影响。
经济运行	严重危害	1.直接影响涉及国家安全的行业、支柱产业和高新技术产业中的重要骨干企业、提供重要公共产品的行业、重大基础设施和重要矿产资源行业等关系国民经济命脉行业的运行和发展。 2.关系国民经济命脉，严重危害对社会经济发展具有重大影响的部门、企业、资源、区域等的生产运营和经济利益。 3.直接对多个行业领域，或者对行业领域核心业务、重要骨干企业、关键信息基础设施、重要资源等生产运营造成特别严重影响，例如导致大范围停工停产、大面积业务中断、大规模基础设施瘫痪、大量处理能力丧失等。 4.波及一个或多个省市的大部分地区，对经济建设有极其恶劣的负面影响。
	一般危害	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、国民经济总产值和增长速度、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.直接影响行业内多个企业、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、关键产业链、核心供应链等。 3. 波及一个或多个地市的大部分地区对经济建设有重大的负面影响。
	轻微危害	1.对行业领域发展、生产、运行和经济效益等造成一般危害。 2.直接危害市场经济运行秩序，如市场准入、市场行为、市场结构、商品销售、交换关系、生产经营秩序等。 3. 波及一个地市或地市以下的部分地区，对经济建设有一定的负面影响。
	无危害	对经济运行不造成影响。

表C.1影响对象的影响程度说明（续）

影响对象	影响程度	参考说明
社会稳定	严重危害	1.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，引起大范围社会恐慌，对社会稳定造成特别严重危害。
	一般危害	1.直接导致重大突发事件、重大群体性事件等，引起社会矛盾激化，对社会稳定造成严重危害。 2.严重影响人民群众的日常生活秩序。 3.严重影响各级党政机关履行公共管理和服务职能。 4.严重影响法治和社会伦理道德规范。
	轻微危害	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。
	无危害	对社会稳定不造成影响。
公共利益	严重危害	波及一个或多个省市的大部分地区，引起社会动荡，对公共安全和健康有极其恶劣的负面影响，包括但不限于： 1.关系重大公共利益，导致多个省市大部分地区的社会公共资源供应长期、大面积瘫痪，大范围社会成员无法使用公共设施、获取公开数据资源、接受公共服务； 2.可能导致特别重大网络安全和数据安全事件，对公共利益造成特别严重影响，社会负面影响大； 3.可能导致特别重大突发公共卫生事件，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。
	一般危害	波及一个或多个地市的大部分地区引起社会恐慌，危害社会秩序和公共利益，对部分行业、部分组织或者部分人民群众造成影响，包括但不限于： 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.可能导致重大突发公共卫生事件，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，较大范围社会成员无法使用公共设施、获取公开数据资源、接受公共服务。
	轻微危害	波及一个地市或地市以下的部分地区，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。
	无危害	对公共利益不造成影响。

表C.1影响对象的影响程度说明（续）

影响对象	影响程度	参考说明
个人权益	严重危害	个人信息主体可能会遭受重大的、不可消除的、可能无法克服的影响，导致自然人的人身安全、财产安全、健康状况、精神状况、人格尊严、个人名誉等出现严重损害。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。
	一般危害	个人信息主体可能遭受较大影响，个人信息主体克服难度高，消除影响代价较大。导致人身安全、财产安全、健康状况、精神状况、人格尊严、个人名誉等出现损害。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。
	轻微危害	个人信息主体可能会遭受困扰，但尚可以克服。导致人身安全、财产安全、精神状况、人格尊严、个人名誉等出现轻微损害。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。
	无危害	对个人信息合法权益不造成影响，或仅造成微弱危害影响但可被补救或者补偿。
组织权益	严重危害	可能导致组织遭到监管部门严重处罚（包括取消经营资格、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。
	一般危害	可能导致组织遭到监管部门处罚（包括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。
	轻微危害	可能导致个别诉讼事件，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。
	无危害	对组织合法权益不造成影响，或仅造成微弱影响但不会影响国家安全、公共利益、市场秩序或各项业务的正常开展，造成的微弱影响可被补救或者补偿。

附 录 D
（资料性）
数据分类分级示例

D.1 互联网药品信息服务资格审批数据分类分级示例

互联网药品信息服务资格审批数据分类分级示例见表D.1，本示例中仅做分类分级方法的示例，相关分类分级结论并不具有规范要求，数据分类分级实施过程中需结合实际场景需要来考虑。

表 D.1 互联网药品信息服务资格审批数据分类分级示例

数据项（字段）	数据分类	数据分级	共享属性	开放属性
证书编号	卫生健康	一级	无条件共享	无条件开放
网站域名	卫生健康	一级	无条件共享	无条件开放
发证机关	卫生健康	一级	无条件共享	无条件开放
法定代表人	卫生健康	一级	无条件共享	无条件开放
发证日期	卫生健康	一级	无条件共享	无条件开放
有效期至	卫生健康	一级	无条件共享	无条件开放
服务性质	卫生健康	一级	无条件共享	无条件开放
网站负责人	卫生健康	一级	无条件共享	无条件开放
地址和邮编	卫生健康	一级	无条件共享	无条件开放
[a] 互联网药品信息服务资格审批数据分级：本数据中许可经营的组织通过互联网渠道经营，其经营性质决定其数据宜全部公开，所有字段均为一级。整体数据集按照安全级别最高字段定为一级。 [b] 互联网药品信息服务资格审批数据分级：本数据中许可经营的组织通过互联网渠道经营，其经营性质决定其数据宜全部公开，所有字段均为一级。整体数据集按照安全级别最高字段定为一级。				

D.2 个人公积金信息分类分级示例

个人公积金信息分类分级示例见表D.2，本示例中仅做分类分级方法的示例，相关分类分级结论并不具有规范要求，数据分类分级实施过程中需结合实际场景需要来考虑。

表 D.2 个人公积金信息分类分级示例

数据项（字段）	数据分类	数据分级	共享属性	开放属性
身份证号码	城乡住房	四级	有条件共享 /不予共享	不予开放
姓名	城乡住房	三级	有条件共享 /不予共享	不予开放
公积金账号	城乡住房	三级	有条件共享 /不予共享	有条件开放 /不予开放
公积金缴存基数	城乡住房	二级	无条件共享/有条件共享	有条件开放
公积金缴存比例	城乡住房	二级	无条件共享/有条件共享	有条件开放
公积金个人账户余额	城乡住房	三级	有条件共享 /不予共享	有条件开放 /不予开放
公积金个人应缴额	城乡住房	三级	有条件共享 /不予共享	有条件开放 /不予开放
公积金单位应缴额	城乡住房	三级	有条件共享 /不予共享	有条件开放 /不予开放
[a] 个人公积金数据分类按照主题分类，属于城乡住房。 [b] 个人公积金数据分级本数据各个数据项（字段）分级有差异。 [c] 本数据中 “身份证号码”和“姓名”共同出现时即可获取公民个人特定身份信息，属于敏感个人信息，参考《中华人民共和国个人信息保护法》要求，按照就高从严原则，可定为四级。				

附 录 E
（资料性）
敏感数据参考清单

E.1 个人一般信息和敏感信息参考清单

个人一般信息和敏感信息参考清单供分类分级工作参考，实际分类分级工作中需根据现实场景需要，结合本规范分类分级标准，综合判定。个人一般信息和敏感信息参考清单见表E.1。

表 E.1 个人一般信息和敏感信息参考清单

个人信息类别		个人信息示例	敏感程度
一级类别	二级类别		
特定身份	个人基本资料	姓名，出生年月日，性别，民族，国籍，籍贯，婚姻状况，婚史，兴趣爱好，手机号码，家庭固话号码，家庭关系，工作单位，个人受教育和培训情况相关信息（如学历、学位、入学日期、毕业日期、学校、院系、专业、成绩单、资质证书、培训记录）等。	敏感
	个人身份信息	可直接标识自然人身份的信息，如身份证、户口本、军官证、护照、驾驶证、行驶证、工作证、出入证、社保卡、居住证、澳台通行证等证件号码、证件生效日期、证件到期日期、证件照片或影印件等。	敏感
	网络身份标识	信息可直接标识网络或通信用户身份的信息及账户相关资料信息（金融账户除外），包含但不限于：用户账号，用户ID，即时通信账号（微信、飞信、QQ等），网络社交用户账号（抖音、微博、邮箱等），用户头像，昵称，个性签名，IP 地址，账户开立时间等。	一般
	身份鉴别信息	用于身份鉴别的数据，如账户登录密码、银行卡密码、支付密码、账户查询密码、交易密码、银行卡有效期、银行卡片验证码（CVN和CVN2）、USBKEY、动态口令、U盾（网银、手机银行密保工具信息）、短信验证码、密码提示问题答案、手机客服密码、个人数字证书、随机令牌等。	敏感
	个人设备信息	可变更的唯一设备识别码：Android ID，IDFA，IDFV，OAID等；不可变更的唯一设备识别码：IMEI，IMSI，MEID，设备MAC地址，硬件序列号，ICCID等。	一般
	个人标签信息	于个人上网记录等各类个人信息加工产生的用于对个人用户分类分析的描述信息，包括但不限于：App偏好，关系标签，终端偏好，内容偏好等标签信息。	一般
个人生物识别信息	个人生物识别信息	生物识别原始信息（如样本、图像等）和比对信息（如特征值、模板等），包含但不限于：人脸，指纹，步态，声纹，基因，虹膜，笔迹，掌纹，耳廓，眼纹等。	敏感

表E.1　个人一般信息和敏感信息参考清单（续）

个人信息类别		个人信息示例	敏感程度
一级类别	二级类别		
个人财产信息	金融账户	金融账户及账户相关信息，包含但不限于：银行卡号，银行卡磁道数据（或芯片等效信息），银行卡有效期，电子银行账号，支付宝账号，微信支付账号，证券账户，基金账户，保险账户，公积金账户，公积金联名账号，账户开立时间，开户机构，账户余额，支付标记信息，账户登录密码，查询密码，支付密码，交易密码，收入，余额，消费支出等。	敏感
	个人交易信息	交易过程中产生的交易信息和消费记录，包含但不限于：交易订单，交易金额，支付记录，透支记录，交易状态，交易日志，交易凭证，账单，证券委托，成交，持仓信息，保单信息，理赔信息等。	敏感
	个人借贷信息	个人在借贷过程中产生的信息，包含但不限于：个人借款信息，贷款额，还款信息，欠款信息，信贷记录，担保情况，其他征信信息等。	敏感
	动产不动产信息	个人所持有的土地、房产等不动产信息，个人所持有的飞机、船舶、汽车、机器设备、农业用具、牲畜、企业产品、材料等。	敏感
行踪轨迹	地理位置	能具体定位到个人的地理位置数据，包括但不限于：家庭住址，通信地址，常驻地址，定位信息，车辆轨迹信息，工作单位地址，住宿信息，出入境记录等。	敏感
	个人上网记录	个人在业务服务过程中的操作记录和行为数据，包括但不限于：网页浏览记录，软件使用记录，点击记录，Cookie，发布的社交信息，点击记录，收藏列表，搜索记录等。	一般
个人通信及社交信息	个人通信信息	通信记录，包括但不限于：短信，彩信，话音，电子邮件，即时通信等通信内容（如文字、图片、音频、视频、文件等），及描述个人通信的元数据（如通话时长）等。	敏感
	联系人信息	描述个人与关联方关系的信息，包括但不限于：通讯录，好友列表，群列表，电子邮件地址列表，家庭关系，工作关系，社交关系等。	一般
医疗健康	健康状况信息	与个人身体健康状况相关的一般信息，包含但不限于：体重，身高，体温，肺活量，血压，血型，步数，步频，运动时长，运动距离，运动方式，运动心率等。	一般
	个人医疗信息	个人因生病医治等产生的相关记录，包含但不限于：就诊医院，疾病名称，临床表现，检查报告，诊断结果，病症，住院志，医嘱单，检验报告，体检报告，手术及麻醉记录，护理记录，用药记录，药物食物过敏信息，生育信息，以往病史，诊治情况，家族病史，现病史，传染病史，吸烟史等。	敏感
宗教信仰	宗教信仰	信仰宗教名称。	敏感
未成年人个人信息	未成年人个人信息	14岁以下（含）未成年人的个人信息。	敏感
其他信息	其他信息	种族、性取向、未公开的违法犯罪记录等。	敏感

E.2 组织敏感信息参考清单

组织敏感信息参考清单供分类分级工作参考，实际分类分级工作中需根据现实场景需要，结合本规范分类分级标准，综合判定。组织敏感信息参考清单见表E.2。

表 E.2 组织敏感数据参考清单

敏感数据类别	敏感数据
账户信息	支付账号（账户），证券账户，保险账户，登录密码，查询密码，交易密码，企业借款信息，企业还款信息，企业欠款信息，账户收入，账户余额，账户消费支出。
业务信息	交易金额，交易证件扫描件，业务合同扫描件，签名影像，交易录音，交易视频。
项目管理	信息化项目、信息系统的规划文档等数据，制度文档、质量管控文档等数据，信息系统设计方案、源代码等数据。
综合管理	市场营销活动及其有关的各项业务管理文档等数据，资金统筹管理活动有关文档等数据，人力资源管理活动有关文档等数据，品牌管理活动有关文档等数据，业务发展规划过程中记录的数据，如一定时期内对业务发展方向、发展速度与质量、发展点及业务发展能力的重大选择和策略等，管理层人员信息，员工信息，人事档案信息。
财务信息	预算执行，周转金拨付，年终并账，会计记录，账簿，金融资产，流动资产，长期投资，固定资产，无形资产，递延资产，流动负债，非流动负债，所有者权益，税务信息（包括税款形成、申报、缴纳以及发票管理等过程中产生的各类数据）。
动产不动产	持有的土地、房产等不动产信息，持有的飞机、船舶、汽车、机器设备、农业用具、牲畜、企业产品、材料等动产信息。

附 录 F
（资料性）
数据分级管控要求

数据全生命周期包括数据采集、传输、存储、处理、共享、开放、销毁等阶段对四个级别数据实施差异化管控要求见表F.1。

表 F.1 数据全生命周期分级管控

数据生命周期	一级数据	二级数据	三级数据	四级数据
数据采集	1.公共数据采集应遵循合法、正当、必要和诚信原则。 2.公共数据采集需遵循真实性原则。 3.应明确数据采集的目的、用途和范围，规范数据采集的流程和方法。 4.应明确数据的最小颗粒度到具体字段级别，对采集账号权限管理，根据对数据字段的需求，依据权限最小化原则分配采集账号权限，并通过管控措施实现账号认证和权限分配，不得采集提供服务所必需以外数据。 5.明确数据采集的渠道及外部数据源，要求敏感数据提供方说明数据来源，并对信息来源的合法性进行确认。 6.依据全省统一的技术标准和规范在法定职权范围内采集、核准与提供公共数据，对于同一项数据有多个来源的情况，进行多源比对和校正。	在满足一级管控要求基础上，满足以下要求。 1.采取必要的技术手段对采集的数据进行校验，以保证其完整性和一致性。 2.需实施数据采集过程的数据防泄漏安全技术措施，防止数据在采集过程中的泄露，如数据加密、采集链路加密、敏感字段脱敏等。	在满足二级管控要求基础上，满足以下要求。 1.待采集数据采取数据访问控制等保护措施。	在满足三级管控要求基础上，满足以下要求。 1.应对外部收集的数据和数据源进行识别和记录，即通过数据溯源的机制保证数据管理人员能够追踪其加工和计算的数据来源。
数据传输	1.加强数据线下交互的过程管控，对数据线下交互建立审核机制及操作流程，要求对线下交互数据采取加密、脱敏、物理封装等防护手段，防止数据被违规复制、传播、破坏等。 2.在网络边界上针对数据流向做好隔离封堵的限制。 3.能够校验数据在传输过程中的完整性。	在满足一级管控要求基础上，满足以下要求。 1.应建立安全的数据传输通道，例如VPN，专线等。 2.应对数据进行来源正确性检测。 3.应对传输通道两端进行主体身份鉴别和认证。	在满足二级管控要求基础上，满足以下要求。 1.应对数据进行加密传输，加密算法应符合国家密码管理的相关法律法规要求。	在满足三级管控要求基础上，满足以下要求。 1.应使用数据源(如水印、溯源)等技术，对数据泄露风险及行为进行追踪，如定位到责任人等。

表 F.1　数据全生命周期分级管控（续）

数据生命周期	一级数据	二级数据	三级数据	四级数据
数据存储	1.公共数据应保存在可信或可控的信息系统或物理环境中。 2.应对存储系统的账号权限进行最小权限管理。 3.应建立本地数据备份与恢复机制，定期进行数据的备份。	在满足一级管控要求基础上，满足以下要求。 1.应对存储系统的访问进行鉴权、日志记录、审计。 2.硬件冗余，保证系统高可用性。 3.建立数据异地备份与恢复机制，定期进行数据的备份。	在满足二级管控要求基础上，满足以下要求。 1.重要的敏感数据应进行加密存储。 2.建立数据实时备份机制。	在满足三级管控要求基础上，满足以下要求。 1.应建立异地灾备中心，提供业务应用的实时无缝切换。
数据处理	1.设置身份标识与鉴别机制。 2.对数据操作行为进行日志记录、审计与分析。 3.依据权限最小化原则分配账号权限，通过管控技术手段统一实现账号认证和权限分配；不同用户只能访问与自己职责对应的数据。 4.应建立数据分析挖掘的操作过程，输出结果的安全审查、合规风险评估和数据使用授权流程。 5.对于系统间和后台数据的转移、导出行为，应通过管理和技术手段予以严格控制。	在满足一级管控要求基础上，满足以下要求。 1.供开发人员使用的测试数据必须经过模糊化处理。 2.对获取数据和本地下载等的敏感操作行为，应进行二次操作审批。	在满足二级管控要求基础上，满足以下要求。 1.应采用口令、密码、生物识别等两种以上鉴别技术同时对用户进行身份鉴别。 2.对敏感数据访问应进行模糊化或脱敏处理。 3.数据进行对外查询、展现、统计等操作时，必须经过模糊化处理。 4.介质中的数据必须进行加密保护。	在满足三级管控要求基础上，满足以下要求。 1.需要满足多人操作管理，确保单人无法拥有重要数据的完整操作权限。 2.应持续对账号进行风险监控，动态授权。
数据共享	1.建立数据共享目录，明确数据的共享范围和使用属性。 2.无条件共享。	1.应建立数据共享目录，明确数据的共享范围和使用属性。 2.对共享数据的使用申请进行严格审批和授权。 3.建立数据共享的唯一通道，定义数据共享的字段、传输方式、服务接口，并对数据共享过程进行日志记录和审计。	在满足二级管控要求基础上，满足以下要求。 1.数据共享前应进行脱敏处理。 2.对数据共享全链路各环节风险进行监控。	1.一般情况不允许共享。 2.若需共享应采取一事一议制，经相关责任人审核授权后，进行脱敏降级后共享。

表F.1　数据全生命周期分级管控（续）

数据生命周期	一级数据	二级数据	三级数据	四级数据
数据开放	1.建立数据开放目录，明确数据的开放范围和使用属性。 2.无条件开放。	1.建立数据开放目录，明确数据的开放范围和使用属性。 2.数据主管部门审批后有条件开放。 3.根据需求场景情况对安全风险较高场景实施数据脱敏。 4.应对开放数据实时监控，发现频繁查询请求、抓取等异常动作时对请求阻断。	在满足二级管控要求基础上，满足以下要求。 1.对数据开放全链路各环节的权限最小化控制，如进行白名单控制；记录请求访问日志；对异常进程监控。	禁止开放
数据销毁	1.建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。 2.业务终止时自行决定数据是否需要销毁，宜采用删除、覆写法等方式进行数据销毁。	1.建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制。 2.业务终止时采用删除、覆写法等方式销毁有关数据。	1.建立数据销毁的审批机制，设置销毁相关监督角色，监督操作过程，并对审批和销毁过程进行记录控制。 2.应以不可逆的方式销毁有关数据。可使用国家权威机构认证的设备对存储介质进行销毁，或联系专业机构执行销毁工作。	同第三级管控要求。