1 范围

本指南给出了民生领域数据分类分级的原则、流程和方法。

本指南适用于区县级政治及地理范围内的民生相关企业和政府，指导企业开展数据分类分级工作，也可为主管监管部门进行数据分类分级管理提供参考。

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 10113-2003 分类与编码通用术语

GB/T 25069—2022 信息技术 安全技术 术语

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 35273-2020 信息安全技术 个人信息安全规范

DB 3301/T 0322.3-2020 数据资源管理 第3部分 政务数据分类分级

YD/T 3813-2020 基础电信企业数据分类

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

3 术语定义

民生领域 People's livelihood field

特指区县级政治及地理范围内，涵盖医疗、教育、交通、养老等多个行业的综合体。

民生领域数据 Data on people's livelihood

在民生相关领域，以电子或其他方式记录的关于信息的任何形式，这些信息涉及与人民日常生活、福祉和基本需求密切相关的各个方面。

注：民生领域数据可能包括：

a) 批发和零售业：供应商、客户、产品、支付交易、供应链等数据。

b) 交通运输、仓储和邮政业：车辆、停车位、运输合同、路线等数据。

c) 住宿和餐饮业：顾客、菜单、结账单、房间等数据。

d) 居民服务、修理和其他服务业：服务组织、服务订单、零件数据、维修记录等数据。

e) 租赁和商务服务业：租赁设备、租赁协议、监控设备、监控视频等数据。

f） 金融业：客户、账户、贷款、投资产品、交易记录等数据。

g） 房地产业：房屋、建筑商、购房合同、物业等数据。

h） 水利、环境和公共设施管理业：水库、河流、水质报告、污染指数等数据。

i） 教育：学生、教师、课程、成绩、教材等数据。

j） 卫生和社会工作：医生、患者、病例、药品、药方等数据。

k） 文化、体育和娱乐业：书籍、展览、版权、赛事观看率等数据。

4 数据分类分级原则

民生领域数据在进行分类分级及应用管理等活动时应坚持贯彻如下原则：

a） 实用性

应符合普遍认知，从可用、实用、好用出发，不应设置无效、无意义的类目或级别，类目和级别不应过粗或过细。

b） 科学性

按照科学系统化的方法进行数据属性、特征进行分类分级，规则级别相对明确、稳定，不宜模棱两可、频繁变更。

c） 安全性

数据安全关系民生，安全性应贯穿数据全生命周期，数据分类分级是数据安全的基础，同时数据安全要求进行数据分类分级、数据应用管理等活动中时刻关注安全性。

d） 开放性

民生领域数据涉及行业门类众多，数据分类分级应开放、兼容，夯实稳定基础并且兼具开放、包容、扩展。

e） 多元性

民生数据基于其领域宽广性，进行分类分级等数据活动时应坚持多元、多样，自主、灵活。

f）动态更新原则

根据数据的业务属性、重要性和可能造成的危害程度的变化，对数据分类分级、重要数据目录等进行定期审核更新。

5 数据分类框架和方法

5.1 数据分类框架

数据按照先行业分类、再业务属性分类的思路进行分类。

a) 按照业务所属行业，将民生数据分为批发和零售数据 ，交通运输数据、仓储和邮政数据，住宿和餐饮数据，金融数据，房地产数据，租赁和商务服务数据，水利、环境和公共设施管理数据，居民服务、修理和其他服务数据，教育数据，卫生和社会工作数据，文化、体育和娱乐数据。

b) 根据本行业业务属性，对行业数据进行细化分类。常见业务属性包括但不限于：

(1) 业务领域：按照业务范围或业务种类进行细化分类；

(2) 责任部门：按照数据管理部门或职责分工进行细化分类；

(3) 描述对象：按照数据描述对象进行细化分类；

(4) 上下游环节：按照业务运营活动的上下游环节进行细化分类；

(5) 数据主题：按照数据的内容主题进行细化分类；

(6) 数据用途：按照数据使用目的进行细化分类；

(7) 数据处理：按照数据处理者类型或数据处理活动进行细化分类；

(8) 数据来源：按照数据来源进行细化分类。

c) 如涉及法律法规有专门管理要求的数据类别（如个人信息），应按照有关规定或标准对个人信息、敏感个人信息进行识别和分类。

5.2 数据分类方法

开展数据分类时，应根据所属行业数据管理和使用需求，结合本行业已有的数据分类基础，灵活选择业务属性将数据逐级细化分类。行业数据分类方法重点考虑以下内容：

a) 明确数据范围：按照行业主管（监管）部门职责，明确本行业本领域管理的数据范围。

b) 细化业务分类：对本行业本领域业务进行细化分类，包括：

(1) 结合部门职责分工，明确行业或业务条线分类；

注 1：例如，民生领域数据，按照部门职责分成应急救灾类、交通管理类、商贸管理类、外贸交易类等类别。

(2) 按照业务范围、运营模式、业务流程等，细化行业或明确各业务条线的关键业务分类；

注 2：例如，应急救灾类可分为资源保障类、预案管理类、自然灾害类、安全生产类、应急管理基础类、风险隐患类、应急事件类、应急通讯类、应急人员类、应急调度类、应急指挥类、辅助决策类等。

c） 业务属性分类：按需选择数据描述对象、数据主题、责任部门、上下游环节、数据用途、数据处理、数据来源等业务属性特征，采用线分类法对关键业务的数据进行细化分类。附录 A 给出了基于数据描述对象的行业数据分类参考示例。

d） 确定分类规则：梳理分析各关键业务的数据分类结果，根据行业数据管理和使用需求，确定行业数据分类规则，例如：

(1) 可采取“业务条线—关键业务—业务属性分类”的方式给出数据分类规则；

注 3：例如，应急救灾数据按照数据描述对象，可分为灾情数据、救援数据、物资调配数据、系统运行和安全数据等，灾情数据可细分为受灾区域信息、灾害类型、灾害影响等，救援数据可细分为救援队伍信息、救援设备信息、救援进展等，数据类别标识为“应急救灾数据－灾情数据－受灾区域信息”“应急救灾数据－救援数据－救援队伍信息”等。

(2) 也可对关键业务的数据分类结果进行归类分析，将具有相似主题的数据子类进行归类。

注 4：例如，民生领域数据也可按照数据处理、上下游环节等业务属性进行分类，首先按照数据处理者类型分为政府机构数据、企业机构数据、公民个人数据等民生领域数据，再将政府机构数据分为公共事务数据、商业服务数据、医疗健康数据和个人数据等，然后按照数据主题将生产数据分为政务数据、公共安全数据、社会公共服务数据等。

6 数据分级框架和方法

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、破坏或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成的危害程度，将数据从高到低分为核心、重要、敏感、一般、公开 5 个级别。

a） 核心数据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能直接危害政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。

b） 重要数据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，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。

c） 敏感数据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能对个体或组织有一定影响，但对国家安全和公共利益的影响较小。

d） 一般数据一旦被泄露、篡改、破坏或者非法获取、非法利用、非法共享，仅影响小范围的组织或公民个体合法权益。

e） 公开数据即使被泄露、篡改、破坏或者非法获取、非法利用、非法共享，但对所有影响对象都没有影响。

6.2 数据分级方法

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，然后开展数据影响分析，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。

6.2.1 数据分级要素

影响数据分级的要素，包括数据主题、群体、区域、精度、规模、深度、覆盖度、重要性、安全风险等，其中主题、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，常见考虑因素见附录 B。

a） 主题：是指数据描述的业务范畴，数据主题识别可考虑数据描述的行业、业务条线、生产经营活动、上下游环节、内容主题等因素。

b） 群体：是指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。

c） 区域：是指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。

d） 精度：是指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。

e） 规模：是指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。

f） 深度：是指通过数据统计、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。

g） 覆盖度：是指数据对领域、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。

h） 重要性：是指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。

i） 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。

j） 可访问性：指数据的获取和利用的便捷程度，包括数据的共享方式、访问权限和使用限制等因素。数据可访问性识别可考虑数据的开放程度、权限管理、隐私保护等情况。

6.2.2 数据影响分析

6.2.2.1 影响对象

影响对象是指数据一旦遭到泄露、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。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，常见考虑因素见附录 C。

a） 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。

b） 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。

c） 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。

d） 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。

e） 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、声誉形象、公信力、知识产权等。

f） 个人权益：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，可能直接影响自然人的人身权、财产权以及其他合法权益。

6.2.2.2 影响程度

影响程度是指数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用、非法共享，可能造成的影响程度。影响程度从高到低可分为特别严重危害、严重危害、一般危害。对不同影响对象进行影响程度判断时，采取的基准不同。如果影响对象是组织或个人权益，则以本单位或本人的总体利益作为判断影响程度的基准。如果影响对象是国家安全、经济运行、社会稳定或公共利益，则以国家、社会或行业的整体利益作为判断影响程度的基准。对不同影响对象的影响程度具体说明见附录 D。

a) 当影响对象是国家安全时，如果可能直接影响政治安全，应将影响程度确定为特别严重危害，如果关系国家安全重点领域，应将影响程度确定为严重危害。

b) 当影响对象是经济运行时，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。

c) 当影响对象是社会稳定时，如果关系重要民生，应将影响程度设置为特别严重危害。

d) 当影响对象是公共利益时，如果关系重大公共利益，应将影响程度设置为特别严重危害，如果可能直接危害公共健康和安全，应将影响程度设置为严重危害。

6.2.3 分级参考规则

在分级要素识别、数据影响分析的基础上，可参考以下规则确定数据级别。

a) 满足以下任一条件的数据，可考虑确定为核心数据：

(1) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能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（如关系国家安全重点领域）；

(2) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能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) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能直接对社会稳定造成特别严重危害（如关系重要民生）；

(4) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能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、群体或区域具有较高覆盖度，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益的重要数据；

(6) 达到较高精度、较大规模或一定深度，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益的重要数据；

(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，可考虑确定为重要数据：

(1) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能直接对国家安全造成一般危害；

(2) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能直接对经济运行造成严重危害或一般危害；

(3) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能直接对社会稳定造成严重危害；

(4) 数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，可能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、公共健康和安全的特定领域、特定群体或特定区域；

(6) 数据达到一定精度、规模或深度，可能直接影响国家安全、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) 满足以下任一条件的数据，可定级为敏感数据：

(1) 数据包含个人隐私信息，如健康记录、个人财务信息等，一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，可能对个体隐私权造成显著影响；

(2) 数据包含组织的商业秘密，如未公开的研发信息、战略计划等，一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，可能对组织的竞争地位或市场价值造成显著影响；

(3) 数据包含可能对个体或组织声誉有显著影响的信息，一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，可能对个体社会形象或组织品牌造成显著影响；

(4) 数据泄露可能给相关个体或组织带来经济损失或其他形式的损害，影响其正常运营或生活质量；

(5) 数据被非法获取或非法利用可能导致个体或组织权益受损，但并未达到危害国家安全、经济运行、社会稳定、公共健康和安全的程度。

d) 满足以下任一条件的数据，可定级为一般数据：

(1) 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，仅可能对社会稳定造成一般危害；

(2) 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，仅可能对公共利益造成一般危害；

(3) 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，仅影响组织合法权益；

(4) 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，仅影响公民合法权益；

(5) 经国家有关部门、各行业各领域主管（监管）部门和各地区、各部门等评估，均未被确定为核心数据和重要数据的数据。

e) 满足以下任一条件的数据，可定级为公开数据：

满足以下条件的数据，可定级为公开数据：

(1) 数据已被官方或组织明确标定为公开信息，且其内容旨在供公众获取和使用；

(2) 数据的内容不包含任何个人隐私、商业秘密或其他敏感信息；

(3) 数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用、非法共享，对社会稳定、公共利益、组织合法权益或公民合法权益均无任何危害；

(4) 数据内容不涉及任何可能影响个体、组织或国家安全的信息；

(5) 数据公开性质已经过相关部门评估确认，且无需任何形式的保密或限制性措施。

表 1 数据分级确定参考规则

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	核心数据	重要数据	公开数据
经济运行	核心数据	重要数据	重要数据	公开数据
社会稳定	核心数据	重要数据	敏感数据	公开数据
公共利益	核心数据	重要数据	敏感数据	公开数据
组织权益、个人权益	敏感数据	一般数据	一般数据	公开数据

7 数据分类分级流程

7.1 建立数据分类分级组织保障

数据分类分级工作的开展应有组织保障。

a) 应明确数据分类分级的决策机构和最高责任人。决策机构负统筹和决策职责，决策数据分类分级工作的目标、内容、标准规范等。决策机构的最高责任人对数据分类分级工作负全面领导责任。

b) 应明确数据分类分级的牵头部门。牵头部门负责牵头推动数据分类分级工作的开展，牵头部门负责按照决策机构议定的工作目标和要求开展数据分类分级工作，牵头制定企业数据分类分级管理办法、制度、流程、标准规范，协调解决分类分级工作中的问题，牵头进行数据分类分级工作的评价。

c) 应明确数据分类分级的实施部门，实施部门负责本部门数据分类分级的具体实施工作，具体包括：按照牵头部门制定的制度、流程、规范等梳理本部门的数据资源，并提交给牵头部门。实施部门包括各业务部门和信息技术部门，业务部门包括财务、人力资源等关键部门。

7.2 建立数据分类分级制度保障

数据分类分级工作的开展需要有制度保障，应明确：

a)数据分类分级的总体要求；

b)数据分类分级的相关制度、规范、标准、工作流程等的制定、发布、维护和更新的机制以及评审和修订周期；

c)数据分类分级管理相关绩效考评和评价机制；

d)数据资产分类分级清单的确立、审核、修订周期和原则；

e)数据分类分级保护的总体原则和目标；

f)操作人员的操作规程。

7.3 数据资源梳理

牵头部门应牵头全面梳理企业内部的所有数据资源，业务部门和技术部门配合数据梳理工作，梳理的内容包括以电子形式记录的数据表、数据项、数据文件等，明确数据梳理的要求，包括数据内容描述、数据量、保存位置、保存期限、数据处理情况（数据处理目的、数据处理所涉及的信息系统）、数据对外提供情况（共享转让、公开披露、数据出境）、数据生命周期各环节安全措施配套情况等内容。

a） 应对重要支撑信息系统的业务流程进行分析，绘制业务流程图。

b） 应根据业务流程，梳理每个业务节点所产生的数据资源。

c） 应明确业务节点的数据资源的访问对象、访问权限、处理单元、存储单元、传输单元等。

应对每个部门的所有数据资源进行逻辑汇聚，对所有部门的数据集合，进行合并然后统一列表，形成数据资源列表。

7.4 数据分类

按照数据分类分级有关要求，参考第 5 章建立自身的数据分类框架和方法，对数据进行分类。数据处理者进行数据分类时，应遵守国家和行业数据分类规则，数据分类流程主要包括以下步骤：

a） 确定数据处理者业务涉及的行业；

b） 按照业务所属行业的数据分类规则，对该业务运营过程中收集和产生的数据进行分类；

c） 识别是否存在法律法规或主管监管部门有专门管理要求的数据类别（如个人信息），对个人信息、敏感个人信息进行区分标识；

d） 如果存在行业域数据分类规则未覆盖的数据类型，可以从组织经营角度结合自身数据管理和使用需要对数据进行分类。

7.5 数据分级

按照数据分类分级有关要求，参考第 6 章建立数据分级框架和方法，并对数据进行分级。

a） 数据分级步骤

可参考以下步骤开展数据分级。

(1) 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、跨行业数据等。

注：数据项是数据不可分割的最小单位，通常表现为数据库表某一列字段等。数据集是由多个数据项组成的集合，如数据库表、数据文件等。跨行业数据是指跨行业流动的数据，及多个行业数据融合加工的数据。

(2) 分级要素识别：按照 6.2.1 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。

(3) 数据影响分析：结合数据分级要素识别情况，分析数据一旦遭到泄露、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（见 6.2.2.1）和影响程度（见 6.2.2.2）。

(4) 综合确定级别：按照 6.2.3 的分级参考规则，综合确定数据级别。

b) 综合确定级别

在分级要素识别、数据影响分析的基础上，按照 6.2.3 分级参考规则综合确定数据级别。

(1) 综合确定级别时，可按照重要数据、核心数据、一般数据的顺序进行确定：

①首先进行重要数据定级评估，可参考重要数据识别相关标准，重点评估数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，是否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，如果符合 6.2.3 中 （1）则进一步评估数据是否为核心数据；

②核心数据定级评估可在识别为重要数据的基础上，重点评估数据一旦被泄露、篡改、损毁或者非法获取、非法使用、非法共享，是否可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。如果符合 6.2.3 中 （2）则将数据确定为核心数据，如果不符合则将数据确定为重要数据；

③重要数据、核心数据之外的数据可确定为一般数据，一般数据定级评估可参考 6.2.3 中（3）进行评估。

(2) 数据集级别可在数据项级别的基础上，按照就高从严的原则，可以将数据集包含数据项的最高级别作为数据集默认级别，但同时也要考虑分级要素（如数据规模）变化可能需要调高级别。

注：数据集中数据项级别与数据集级别不一定相同，具体要根据该数据项的影响对象和影响程度进行判断。

(3) 衍生数据级别可按照就高从严原则，在原始数据级别的基础上进行分级，同时综合考虑加工后的数据深度等分级要素对国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益的影响，对数据级别进行调整，衍生数据级别确定可参考附录 E。

(4) 跨行业数据分级，原则上可按照数据来源的行业数据分级规则确定级别，如果存在跨行业数据融合加工，需考虑跨行业对数据分级要素的影响，按照衍生数据确定级别。

(5) 根据数据重要程度和可能造成的危害程度的变化，可对数据级别进行动态更新，动态更新情形可参考附录 F。

c) 行业分级规则

各行业各领域在遵循数据分级框架的基础上，结合行业数据分级要素识别、数据影响分析和综合确定级别等实践经验，制定本行业本领域数据分级规则，重点可以考虑明确以下内容。

(1) 给出本行业本领域重要数据目录或识别细则，明确哪些数据可确定为重要数据，包括但不限于：

①本行业本领域哪些特定领域、特定群体、特定区域，以及达到什么精度、什么规模的数据，可能直接关系国家安全、经济发展、社会稳定、公共健康和安全；

②本行业本领域达到什么深度的衍生数据，可能直接关系国家安全、经济发展、社会稳定、公共健康和安全。

(2) 提出本行业本领域核心数据目录建议，明确哪些数据建议确定为核心数据，包括但不限于：

①本行业本领域对特定领域、特定群体、特定区域具有什么覆盖度，以及达到什么精度、什么规模、什么覆盖度的重要数据，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益；

②本行业本领域达到什么深度的衍生数据，可能直接影响政治安全、国家安全重点领域、国民经济命脉、重要民生、重大公共利益。

(3) 明确本行业本领域一般数据范围。

注：行业也可以根据工作需要对一般数据进行细化分级。

7.6 数据资产目录

对数据分类分级结果进行审核和完善，最后批准发布实施，对数据进行分类分级标识，形成数据分类分级清单和重要数据、核心数据目录。

7.7 分类分级结果核查

根据实际数据的应用场景，核查验证分类分级结果及实施过程是否合规，包括但不限于数据表、过程记录、方法内容等。 。

7.8 动态更新管理

根据数据重要程度和可能造成的危害程度变化，对数据分类分级规则、重要数据和核心数据目录、数据分类分级清单和标识等进行动态更新管理。

7.9 关键问题

a) 根据数据分类分级的原则，数据分类相对稳定不变，数据等级需要根据数据的体量、政策和实际情况定期动态调整，以确保定级的准确性和数据安全性。

b) 数据分级后涉及级别变更，基本如下：

(1) 级别提升：数据的数量增多、体量增大、数据涉及行业、部门、人员等范围扩大；数据价值较之前有明显增加；发生特定事件后的数据重要性和敏感性提升等。

(2) 级别降低：数据已被公开或披露；数据时效性变差价值降低；数据进行脱敏或删除关键字段；发生特定事件后的数据重要性和敏感性降低等。

c) 多源数据融合的问题：在多元化的业务场景中，数据可能来源于多个系统或平台。如何确保这些数据能够准确无误地进行分类和级别设定是一大挑战。

d) 法律和合规的挑战：在某些国家或地区，关于数据的分类和处理可能存在严格的法律和规定。如何确保数据分类分级工作既满足业务需求，又符合相关的法律规定，是一个需要重点关注的问题。

8 数据分级安全保护要求

根据数据资源的分类分级情况，在数据生命周期的各个环节配套差异化的安全保护措施，应遵循如下管控要点。

a) 根据数据分类分级管理制度对数据进行分类分级标识。对于在数据库中存储的高安全级别数据（如核心数据），标记应细化至数据库表的字段级，其他级别数据采用的标记宜细化到数据库表的字段级。若出现任何没有分级标识的数据，其默认安全控制等级为最高安全等级。

b) 原则上未经过脱敏处理的数据不可降级使用，若确有需要，应执行严格的授权审批流程，并对降级使用数据进行全过程审计。数据使用完毕后，恢复至原安全级别。

c) 数据传输过程中，若涉及高安全级别数据（如核心数据）应对数据报文进行加密，并采取措施（如数字签名、MAC 等），以保证数据传输的机密性和完整性。

d) 在使用数据或披露前，涉及高安全级别数据的，应采用数据脱敏技术，确保数据使

用、对外披露等场景的脱敏。

e） 对于个人敏感信息的安全管控，还应满足《GB/T 35273-2020 信息安全技术 个人信息安全规范》中对个人敏感信息的安全管控要求。

附录 A（资料性）基于数据描述对象的行业数据分类参考示例

表 A.1 从数据描述对象角度，将行业数据分为用户数据、业务数据、经营管理数据、系统运行和安全数据，具体分类方法可参考如下：

1. 从便于保护用户数据角度，将个人和组织用户的数据单独划分出来作为用户数据，同时识别用户数据涉及的个人信息、敏感个人信息，并按照国家有关规定或标准对个人信息进行细化分类（个人信息分类见附录 H）；

2. 从便于行业管理业务数据的维度，将业务的研发、生产、运营过程中收集和产生的非用户类数据划分为业务数据，并按照业务属性对业务数据进一步细分；

3. 从保护组织机构的商业秘密、知识产权等维度，将组织机构经营和内部管理数据划分为一类；

4. 从便于网络安全运维管理角度，将网络和信息系统运维数据、网络安全数据划分为一类。

表 A.1 行业数据分类参考示例

数据类别	类别定义	示例
用户数据	在开展业务服务过程中从个人用户或组织用户收集的数据，以及在业务服务过程中产生归属于用户的数据	如个人用户信息（即个人信息）、组织用户信息（如组织基本信息、组织账号信息、组织信用信息等）
业务数据	在业务的研发、生产、运营过程中收集和产生的非用户类数据	参考业务所属的行业数据分类分级，结合自身业务特点进行细分，如产品数据、合同协议等
经营管理数据	在组织机构经营和内部管理过程中收集和产生的数据	如经营战略、财务数据、并购及融资信息等
系统运行和安全数据	网络和信息系统运维及网络安全数据	如网络和信息系统的配置数据、网络安全监测数据、备份数据、日志数据、安全漏洞信息等

附录 B（资料性）数据分级要素识别常见考虑因素

B.1 数据主题、群体、区域考虑因素

数据的主题、群体、区域识别常见考虑因素，包括但不限于：

——数据领域识别的常见考虑因素，例如：

- 行业；
- 业务类目；
- 生产经营活动；
- 上下游环节；
- 内容主题；
- 与国家安全、经济运行、社会稳定、公共利益相关的领域等。

——数据群体识别的常见考虑因素，例如：

- 特定人群；
- 特定团体、单位、组织；
- 特定网络、信息系统、数据中心；
- 特定资源、原材料、物资；
- 特定元器件设备；
- 特定项目；
- 特定基础设施；
- 与国家安全、经济运行、社会稳定、公共利益相关的群体等。

——数据区域识别的常见考虑因素，例如：

- 行政区划；
- 特定地区；
- 地理环境；
- 重要场所；
- 网络空间；
- 与国家安全、经济运行、社会稳定、公共利益相关的区域等。

B.2 数据精度考虑因素

数据精度识别的常见考虑因素，例如：

- 数值精度，如统计指标的精度等；