

T/QBDA

青岛市大数据发展促进会团体标准

T/QBDA XXXX-2024

民生领域数据分类分级应用指南

(征求意见稿)

2024 - XX - XX 发布

2024 - XX - XX 实施

青岛市大数据发展促进会 发布

目 次

前 言	1
1 范围	3
2 规范性引用文件	3
3 术语定义	3
4 数据分类分级原则	4
5 数据分类框架和方法	5
5.1 数据分类框架	5
5.2 数据分类方法	5
6 数据分级框架和方法	6
6.1 数据分级框架	6
6.2 数据分级方法	7
6.2.1 数据分级要素	7
6.2.2 数据影响分析	8
6.2.3 分级参考规则	9
7 数据分类分级流程	12
7.1 建立数据分类分级组织保障	12
7.2 建立数据分类分级制度保障	12
7.3 数据资源梳理	12
7.4 数据分类	13
7.5 数据分级	13
7.6 数据资产目录	15
7.7 分类分级结果核查	15
7.8 动态更新管理	16
7.9 关键问题	16
8 数据分级安全保护要求	16
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	18
附录 B（资料性）数据分级要素识别常见考虑因素	19
附录 C（资料性）影响对象考虑因素	22

附录 D（资料性） 影响程度参考示例	25
附录 E（资料性） 衍生数据定级参考	28
附录 F（资料性） 动态更新情形参考	29
附录 G（资料性） 民生领域数据分类分级示例	30
附录 H（资料性） 数据分类分级流程示意图	33
附录 I（资料性） 数据分类分级应用场景	36
参 考 文 献	37

前 言

“民生”一词，源自古籍《左传·宣公十二年》，原文“民生在勤，勤则不匮”强调了勤劳对于保障民众生计的重要性。这一术语随着时间的推移逐渐丰富和发展，其内涵不断扩展。在《辞海》中，民生被解释为“人民的生计”，不仅体现了人本思想，还蕴含着深厚的人文关怀。在这个定义中，民生不仅关乎基本的物质需求，如食物、住房和衣着，还包括教育、健康、就业、娱乐和养老等更广泛的生活领域，体现了一个社会关注并满足其成员全面需求的程度。

在现代社会，民生的概念已经超越了物质层面，涵盖了生活形态、文化模式和市民精神等多方面的精神特质。民生、民主和民权互为依托，共同构成社会发展的重要支柱。在数字化经济的背景下，民生领域的重要性更加凸显。民生数据的分类、分级和应用管理不仅是提升公共服务质量的关键，也是推动区域数字经济发展的核心要素。

“领域”和“行业”虽然相关，但含义有所不同。“领域”是一个广泛的概念，涵盖知识、技能和活动等多个方面；而“行业”更具体，指的是进行相似商业活动的机构和个体的集合，具体行业分类，可根据《国民经济行业分类》进行分类。在民生领域，这两者交织在一起，形成了一个涵盖医疗、教育、交通、养老等多个行业的综合体。

本指南基于青岛市北区民生领域公共服务信息化项目而编写，目的是指导相关领域、行业和企业对民生数据的分类、分级以及应用管理方面的实践。这不仅对于促进同类企业或项目的发展具有指导意义，而且对于区域数字经济的发展，尤其是在数据要素方面的研究和应用，也具有重要的参考价值。

本指南由青岛建投聚禾数字科技发展有限公司提出

本指南由青岛市大数据发展促进会归口。

本指南起草单位：。

本指南主要起草人：。

版权声明

根据国家有关法律法规规定，团体标准享有版权，未经许可禁止复制和销售。

未经合法授权，严禁任何单位和个人对标准出版物及相关工作文件进行复制、销售、传播和翻译出版，严禁任何单位或个人将国际标准的任何部分通过电子信息网络或制作成标准数据库用于传播。标准化服务机构和中介机构的检验、鉴定、认证、咨询、评估和培训等活动必须使用正版标准。标准化研究机构馆藏的标准文本必须通过合法渠道购买。

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中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，应急救援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，应急救援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“应急救援数据—灾情数据—受灾区域信息”“应急救援数据—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，确定数据一旦被泄露、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 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 and 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系列字段等。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。

青岛市大数据发展促进条例

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，将网络和信息系统的运维数据、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	网络和信息系统的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；

- 空间精度，如位置定位精度、数字地图精度等；
- 时间精度，如年度、季度、月度、日度等；
- 生产工艺精密度，如集成电路精细度、机械加工精度等；
- 视频图像高清度；
- 遥测遥感精度；
- 仪器仪表精度。

B.3 数据规模考虑因素

数据规模识别的常见考虑因素，例如：

- 数据存储量；
- 企业市值（估值）；
- 设备或装备容量；
- 生产、加工、控制、吞吐、输送、储存能力；
- 资源储量；
- 交易量；
- 群体规模，如用户规模、系统或设备数量、生产加工单元数量、基础设施数量、项目数量等。

B.4 数据深度考虑因素

数据深度识别的常见考虑因素，例如：

- 经济运行情况统计；
- 产业发展态势分析；
- 特定领域、群体或区域的特征分析，如特定人群或用户特征分析；
- 行踪轨迹；
- 主体关系；
- 历史信息；
- 机构背景；
- 产业供应链。

B.5 数据覆盖度考虑因素

数据覆盖度识别的常见考虑因素，例如：

- 领域覆盖分布或密度，如领域覆盖占比、领域覆盖分布、领域覆盖密度等；

- 群体覆盖分布或密度，如群体覆盖占比、群体覆盖分布、人口密度等；
- 区域覆盖分布或密度，如行政区划覆盖度、区域覆盖分支、区域覆盖密度等。
- 时段覆盖分布或密度，如时间段覆盖度、时段覆盖分布、时段覆盖密度等。

B.6 重要性考虑因素重要性识别常见考虑因素，例如：

1. 在数字经济建设中的重要程度，如数字基础设施建设、数据要素市场流通、产业数字化转型、数字化产业竞争力等；
2. 在社会建设中的重要程度，如公共服务数字化、智慧城市、数字生活建设、住建、数字农村等；
3. 在数字政府和政治建设中的重要程度，如政务数据共享、公共数据开放和开发利用、数字化政务服务、监管治理体系建设、政治制度、法律司法等；
4. 在文化建设中的重要程度，如教育、科学、文学艺术、新闻出版、广播电视、卫生体育、图书馆、博物馆、网络空间等各项文化事业；
5. 在生态文明建设中的重要程度，如自然资源、生态环境、交通、水利、气象、林草、地震等；
6. 在国家安全、维护社会稳定等工作的重要程度，如涉外数据对维护和塑造国家安全意义重大。

B.7 安全风险考虑因素

安全风险识别常见考虑因素，例如：

1. 数据泄露风险：数据被窃取、未授权访问、人员盗取等破坏数据保密性风险。
2. 数据篡改风险：数据被未授权修改、注入、仿冒、伪造等破坏数据完整性风险。
3. 数据破坏风险：数据被损毁、数据质量下降、数据访问或使用中断等破坏数据可用性风险。
4. 非法获取数据风险：违反法律、行政法规等有关规定，超范围收集、强制授权、非法获取公民个人信息等违法违规收集数据。
5. 非法利用数据风险：违反法律、行政法规等有关规定，使用、加工、委托处理数据，以及数据被未授权使用、算法歧视等违规滥用风险。
6. 非法共享数据风险：违反法律、行政法规等有关规定，向他人提供、交换、转移、交易、出境、公开数据。

附录 C（资料性）影响对象考虑因素

C.1 国家安全

判断可能影响国家安全的数据，常见考虑因素包括但不限于：

1. 影响国家政权安全、政治制度安全、意识形态安全、民族和宗教政策安全；
2. 影响领土安全、国家统一、边疆安全和国家海洋权益；
3. 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；
4. 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；
5. 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；
6. 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；
7. 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；
8. 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；
9. 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；
10. 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；
11. 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；
12. 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；
13. 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。

C.2 经济运行

判断可能影响经济运行的数据，常见考虑因素包括但不限于：

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。

C.3 社会稳定

判断可能影响社会稳定的数据，常见考虑因素包括但不限于：

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。

C.4 公共利益

判断可能影响公共利益的数据，常见考虑因素包括但不限于：

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。

C.5 组织权益

判断可能影响组织权益的数据，常见考虑因素包括但不限于：

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。

C.6 个人权益

判断可能影响个人权益的数据，常见考虑因素包括但不限于：

1. 可能导致自然人的人格尊严受到侵害；
2. 影响自然人的人身安全；
3. 影响自然人的财产安全；
4. 影响个人在个人信息处理活动中的权利，如选择权、知情权、拒绝权等；
5. 其他影响个人权益的数据。

附录 D（资料性） 影响程度参考示例

针对国家安全、经济运行、社会稳定、公共利益、组织权益、个人权益六个影响对象，产生不同 影响程度的参考示例见表 D. 1。

表 D. 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	关系国家安全重点领域，或者对国土、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、海外利益等任一领域国家安全造成严重威胁
	一般危害	对国土、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、海外利益等任一领域国家安全造成直接威胁
经济运行	特别严重危害	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，或者对行业核心业务、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
	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，或者直接影响行业核心竞争力、关键产业链、核心供应链等

影响对象	影响程度	参考说明
	一般危害	1. 对行业发展、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
社会稳定	特别严重危害	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
	严重危害	1. 直接导致重大突发事件、重大群体性事件等，引起社会矛盾点激化，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公共服务职能 4. 严重影响法治和社会伦理道德规范
	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
公共利益	特别严重危害	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
	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. 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

影响对象	影响程度	参考说明
		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
	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	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
	严重危害	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
	一般危害	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
个人权益	特别严重危害	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。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。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	个人信息主体可能会遭受困扰，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 E（资料性） 衍生数据定级参考

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。数据加工程度维度数据分类见表 E.1。

表 E.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	是指数据的原本形式和内容，未作任何加工处理	如采集的原始数据等
脱敏数据	对敏感数据（如个人信息）采取技术手段进行数据变形处理后的新数据，降低数据敏感性	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	是由多个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	对不同业务目的或群体、区域、领域的数据进行汇聚，进行挖掘或聚合	如多个业务、多个区域、多个领域的数据整合、汇聚等

衍生数据级别可参考待加工的原始数据集级别，综合考虑数据加工对分级要素、影响对象、影响程度的影响，按照第 6 章进行数据分级：

脱敏数据级别可以比原始数据集级别降低；

标签数据级别可以比原始数据集级别降低；

统计数据如涉及大规模群体特征或行动轨迹，应设置比原始数据集级别更高的级别；

融合数据级别要考虑数据汇聚融合结果，如果结果数据是对大量多维数据进行关联、分析或挖掘，汇聚了更大规模的原始数据或分析挖掘出更敏感、更深层的数据，级别可以升高，但如果结果数据降低了标识化程度等，级别可以降低。

附录 F（资料性）动态更新情形参考

数据分类分级完成后，当数据的业务属性、重要程度和可能造成的危害程度的变化时通常需要进行动态更新，动态更新常见情形包括但不限于：

1. 数据内容发生变化，导致原有数据的安全级别不再适用；
2. 数据内容未发生变化，但数据时效性、数据规模、数据应用场景、数据加工处理方式等发生显著变化；
3. 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；
4. 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；
5. 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；
6. 数据进行脱敏或删除关键字段，或者经过去标识化、假名化、匿名化处理；
7. 发生数据安全事件，导致数据敏感性发生变化；
8. 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；
9. 需要对数据安全级别进行变更的其他情形。

附录 G（资料性）民生领域数据分类分级示例

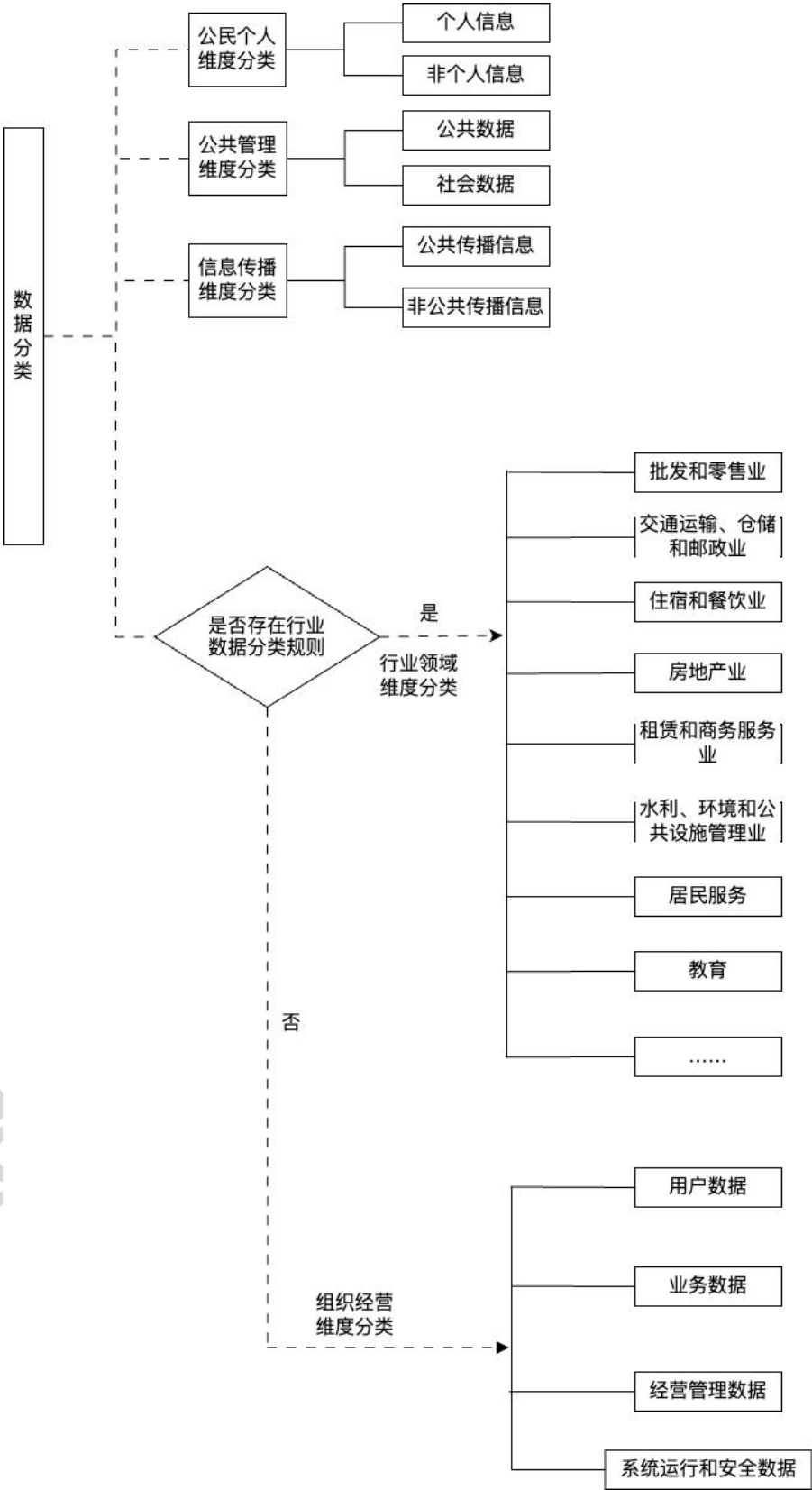
一级分类	二级分类	数据内容示例	数据级别
应急救援管理类	资源保障类数据	应急物资数据、应急救援队伍数据、应急避难场所数据、医疗保障类数据	重要数据
	预案管理类数据	预案数据、备案管理数据、数字化数据、条件类型数据、流程管理数据	重要数据
	自然灾害类数据	自然灾害风险隐患数据、自然灾害风险感知数据、应急资源数据、自然灾害承灾体数据、监测预警数据	重要数据
	安全生产类数据	企业信息数据、危险源信息数据、重点防护目标数据	重要数据
	风险隐患类	风险隐患数、地点信息、位置（经纬度）、行政区划编号、管控要求、责任人、联系电话	重要数据
	值守管理类	应急机构、应急人员、排班信息、值班日志数据、交接班情况数据	重要数据 / 一般数据
	应急研判类	气象数据、水雨情数据、危旧房数据、地质灾害数据、预警信息数据	重要数据
	辅助决策类	救援态势数据、重灾区分析数据、灾区分析数据、影响区范围数据、态势标绘类数据	重要数据
商贸类	应急调度类	应急调度事件数据、应急调度地址信息、地点位置（经纬度）、行政区划信息、责任部门数据	重要数据
	市场数据	市场名称、市场地址、市场摊位信息等	
	用户数据	商户编码、商户名称、摊位信息、身份证、经营范围、手机号、姓名、银行卡号、邮箱等	重要数据
	商品数据	商品引进单号、销售方式、商品名称、商品分类编码、商品分类名称、品牌编码、品牌名称、规格信息、货号、供应商名称等	一般数据
	订单类数据	连锁店编码、销售时间、交易方式、会员编码、	重要数据

		会员 ID、会员卡号、会员名称、退款流水号、退款订单号、收银员编码、收银员、导购员名称等数据	
	库存类数据	仓库名称、实物库存、实物占用库存、实物可用库存、商品库管类型、商品名称、类别名称、类别编码、单价编码等	一般数据
	交易类数据	支付编码商户编码、门店编码、业务系统单号、贸易单号、交易时间、退款信息、充值信息、支付银行信息、支付完成时间、支付方式名称、订单总金额、找零金额、订单号等	重要数据 / 一般数据
泊车管理类	泊车资源信息类	车辆信息数据、车场统计数据、车场基础信息数据、车场泊位信息数据等	一般数据
	设备管理类	设备能力数据、设备事件数据、告警数据、设备授权码数据、设备大类数据、设备抓拍记录数据、设备名录数据、设备心跳记录数据、设备车场关联数据、设备操作日志数据	一般数据
	泊车订单类	卡口抓拍记录数据、订单计费过程明细数据、车停时间数据、计费明细数据、停车订单数据、驶出数据、驶入数据、停车交易数据、订单支付数据、长租数据等	重要数据
	巡检管理数据	巡检考核数据、巡检缴费数据、巡检追缴数据、巡检员空间数据、巡检员绩效统计数据、巡检员签到数据、巡检问题数据	一般数据
	用户消费类	消费用户信息数据、商停类消费数据、长租类消费数据等	重要数据
	基础信息类	区域基本信息类数据、车辆基础信息数据、车场基础信息类数据、车位基础信息类数据等	一般数据
外贸综合交易	出口相关大类	出口产品类数据、出口订单管理类数据、国内采	重要数据 / 一

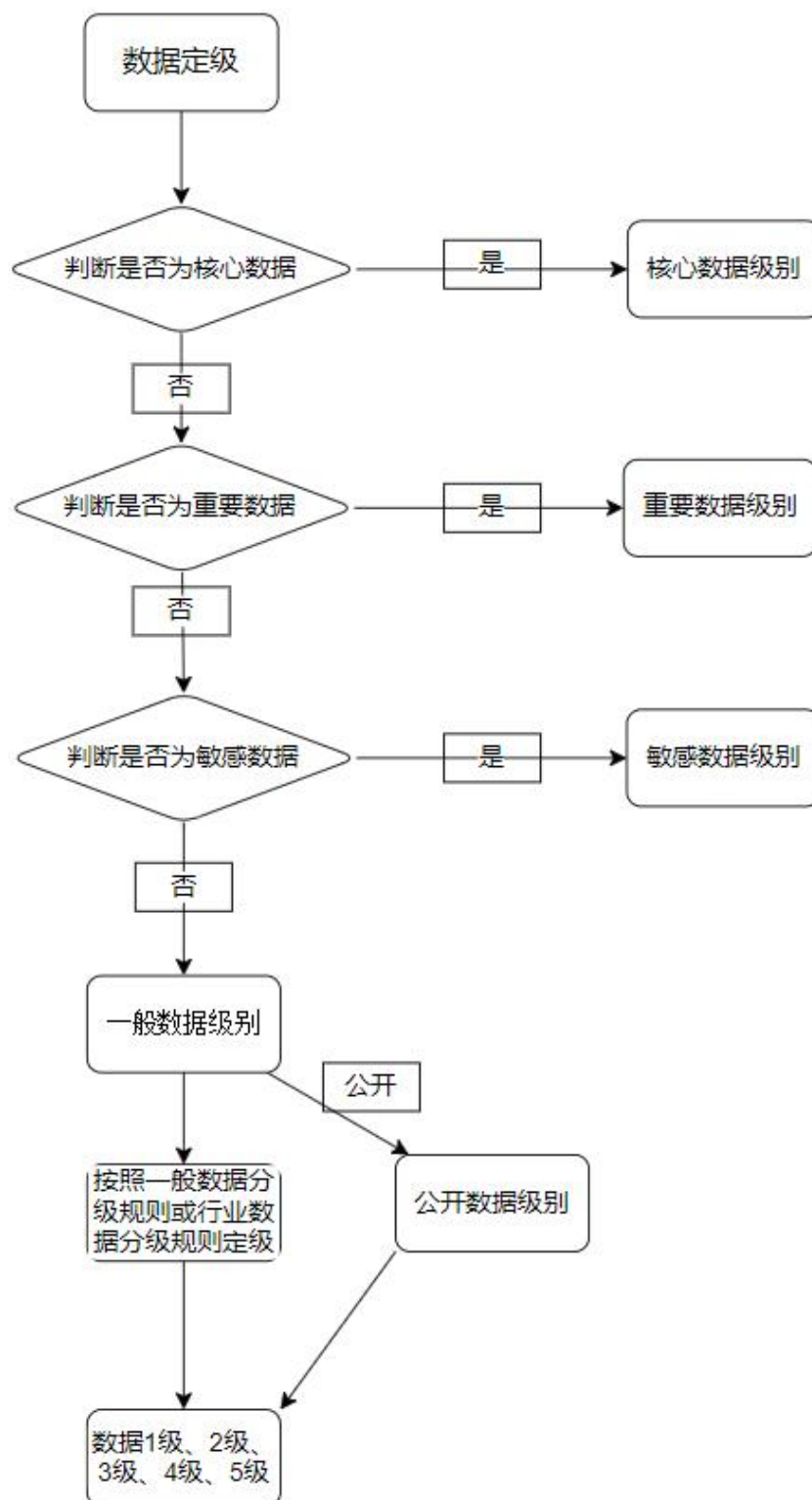
类数据		购类数据、出运管理类数据、国际结算类数据等	般数据
	进口相关大类	进口产品类数据、进口订单管理类数据、海运管理类数据、清关类数据、财务类数据、进口风险类数据等	重要数据 / 一般数据
	交易结算类	外贸交易类数据、收款类数据、平台交易类数据、物流类数据、预订类数据、订单类数据等	重要数据 / 一般数据
	金融管理类	金融服务类数据、金融产品类数据、金融信用保险类数据、供应链金融类数据等	一般数据
	运营管理类	发布资讯类数据、用户信息类数据、外部系统对接数据、区块链技术相关数据、内部系统对接数据、运营分析类数据	重要数据 / 一般数据

附录 H（资料性）数据分类分级流程示意图

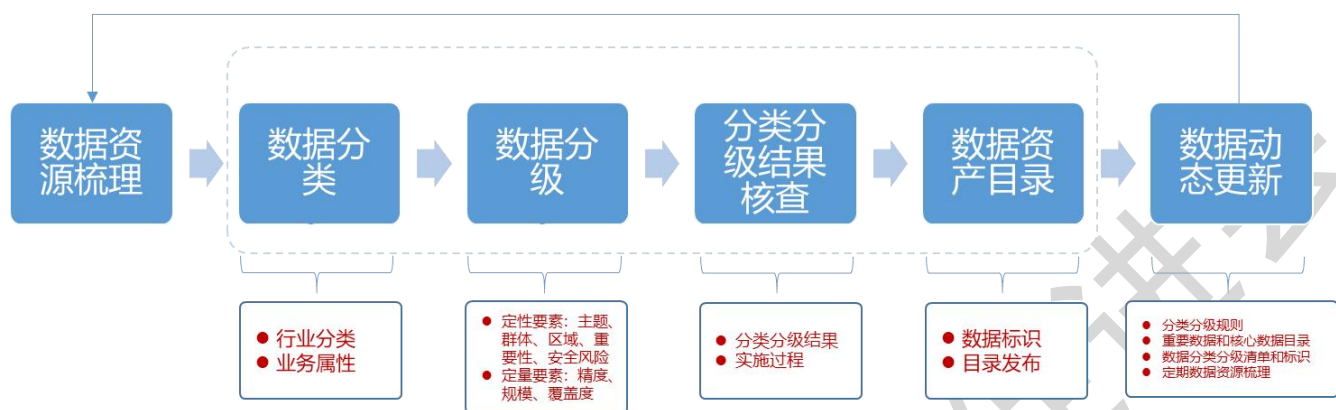
H.1 数据分类流程



H.2 数据定级流程



H.3 数据分类分级流程



附录 I（资料性）数据分类分级应用场景

1. 数据资产管理和价值评估：通过数据分类明确数据资产类目，数据等级作为数据价值评估的支撑要素之一，基于分类分级开展数据资产化管理和价值评估。

2. 根据数据分类分级开展数据安全保护工作，降低数据安全成本提高保障效率。

3. 根据分类分级与第三方机构开展数据合作，包括数据共享与交换，拓展数据要素生态圈。

4. 合规性和隐私保护：根据数据的敏感性级别，制定相应的合规策略和隐私保护措施。例如，对于涉及个人隐私的数据，实施更严格的保护措施。

5. 决策支持系统：使用不同级别和类型的数据支持业务决策。高价值、高可靠性的数据可以用于关键业务决策，而其他数据可用于日常操作和策略规划。

6. 风险管理：通过识别数据类别和等级，评估与数据相关的风险，如数据泄露、滥用等风险，并制定相应的风险缓解措施。

7. 数据治理：制定和实施有效的数据治理策略，包括数据的获取、存储、处理和销毁等方面，以确保数据的质量和一致性。

8. 数据驱动的市场营销：利用不同类型的数据（如消费者行为、偏好等）来制定更有效的市场营销策略。

9. 技术研发：在技术研发中使用不同级别的数据进行模型训练和测试，以提高产品和服务的技术含量和市场竞争力。

10. 客户关系管理：利用分类分级的数据更好地理解 and 满足客户需求，提升客户满意度和忠诚度。

11. 教育和培训：在教育和培训领域，利用分类分级数据来支持课程设计、学习进度跟踪和成效评估。

12. 公共服务和政策制定：政府和公共机构可以利用分类分级数据更好地了解民众需求，制定更有效的公共政策和服务。

参 考 文 献

- [1] 《中华人民共和国数据安全法》
- [2] 《中华人民共和国个人信息保护法》
- [3] 《网络数据安全条例（征求意见稿）》
- [4] 《工业和信息化领域数据安全管理办法（试行）（征求意见稿）》
- [5] 《中央企业商业秘密保护暂行规定》
- [6] GB/T 4754—2017 国民经济行业分类
- [7] GB/T 35273—2020 信息安全技术 个人信息安全规范
- [8] GB/T 37973—2019 信息安全技术 大数据安全管理指南
- [9] GB/T 38667—2020 信息技术 大数据 数据分类指南
- [10] 信息安全技术 重要数据识别指南（征求意见稿）
- [11] JR/T 0158—2018 证券期货业数据分类分级指引
- [12] JR/T 0171—2020 个人金融信息保护技术规范
- [13] JR/T 0197—2020 金融数据安全 数据安全分级指南
- [14] YD/T 3813—2020 基础电信企业数据分类分级方法
- [15] YD/T 3867—2021 基础电信企业重要数据识别指南
- [16] 北京市地方标准《政务数据分级与安全保护规范》
- [17] 贵州省地方标准 DB 52/T 1123—2016《政府数据 数据分类分级指南》
- [18] 上海市公共数据开放分级分类指南（试行）
- [19] 内蒙古自治区地方标准《公共数据分类分级指南》