ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 43697—2024

数据安全技术　数据分类分级规则

Data security technology—Rules for data classification and grading

2024-03-15 发布　　2024-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
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 …… 2
5.1　数据分类框架 …… 2
5.2　数据分类方法 …… 3
6　数据分级规则 …… 3
6.1　数据分级框架 …… 3
6.2　数据分级方法 …… 4
6.3　数据分级要素 …… 4
6.4　数据影响分析 …… 4
6.5　级别确定规则 …… 5
6.6　综合确定级别 …… 6
7　数据分类分级流程 …… 7
7.1　行业领域数据分类分级流程 …… 7
7.2　处理者数据分类分级流程 …… 7
附录 A（资料性）　基于描述对象与数据主体的数据分类参考 …… 8
附录 B（资料性）　个人信息分类示例 …… 9
附录 C（资料性）　数据分级要素识别常见考虑因素 …… 11
附录 D（资料性）　安全风险常见考虑因素 …… 13
附录 E（资料性）　影响对象考虑因素 …… 14
附录 F（资料性）　影响程度参考示例 …… 16
附录 G（规范性）　重要数据识别指南 …… 18
附录 H（资料性）　一般数据分级参考 …… 20
附录 I（资料性）　衍生数据分级参考 …… 22
附录 J（资料性）　动态更新情形参考 …… 23
参考文献 …… 24

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。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国电子技术标准化研究院、中国科学技术大学、国家计算机网络应急技术处理协调中心、国家信息技术安全研究中心、中国信息安全测评中心、中国网络空间研究院、中国网络安全审查技术与认证中心、国家工业信息安全发展研究中心、国家信息中心、北京市政务信息安全保障中心(北京信息安全测评中心)、公安部第三研究所、中国信息通信研究院、清华大学、中国人民公安大学、中国科学院软件研究所、交通运输部科学研究院、杭州安恒信息技术股份有限公司、三六零数字安全科技集团有限公司、北京抖音信息服务有限公司、北京快手科技有限公司、中国核能行业协会、中国石油化工集团有限公司、中国银联股份有限公司、中国邮政储蓄银行股份有限公司、阿里巴巴(北京)软件服务有限公司、蚂蚁科技集团股份有限公司、华为技术有限公司、北京百度网讯科技有限公司、中国移动通信集团有限公司、中国电信集团有限公司、北京爱奇艺科技有限公司、数库(上海)科技有限公司、北京奇虎科技有限公司、深信服科技股份有限公司、启明星辰信息技术集团股份有限公司、奇安信科技集团股份有限公司。

本文件主要起草人：姚相振、左晓栋、胡影、周晨炜、吴梦婷、陈琦、周亚超、上官晓丽、卢磊、任英杰、陈特、晏慧、杨晨、杨晓伟、李文婷、卓子寒、邢潇、杨韬、李敏、段静辉、许静慧、李媛、任卫红、金波、胡振泉、耿贵宁、单博深、许皖秀、张敏、晏敏、都婧、杨光、姜伟、杨帅锋、孙岩、刘蓓、郭明多、张夕夜、曹京、芦天亮、杨骁涵、杨博龙、落红卫、王昕、郝春亮、朱雪峰、沙睿、蒋楠、郭延玲、刘磊、田鑫、张放、朱晨红、彭骏涛、孙勇、白晓媛、彭晋、常新苗、李实、王海棠、钟舒翔、张骁、张妍婷、江为强、范东媛、杨立宝、许琛超、樊庆君、张宇光、蓝宇娜、张屹、陆忠明、叶润国、宋博韬、姚卓、宋晓鹏、刘前伟、安锦程。

引　言

2021 年 9 月 1 日，《中华人民共和国数据安全法》正式施行，明确规定“国家建立数据分类分级保护制度”，提出“根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、损毁、泄露或者非法获取、非法使用，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，对数据实行分类分级保护”。

开展数据分类分级保护工作，首先需要对数据进行分类分级，识别涉及的重要数据和核心数据，然后建立相应的数据安全保护措施。本文件在国家数据安全工作协调机制指导下，根据《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》及有关规定，给出了数据分类分级的通用规则，用于指导各行业领域、各地区、各部门和数据处理者开展数据分类分级工作。

数据安全技术　数据分类分级规则

1　范围

本文件规定了数据分类分级的原则、框架、方法和流程，给出了重要数据识别指南。

本文件适用于行业领域主管（监管）部门参考制定本行业本领域的数据分类分级标准规范，也适用于各地区、各部门开展数据分类分级工作，同时为数据处理者进行数据分类分级提供参考。

本文件不适用于涉及国家秘密的数据和军事数据。

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

3　术语和定义

GB/T 25069—2022 界定的以及下列术语和定义适用于本文件。

3.1

数据　data

任何以电子或者其他方式对信息的记录。

3.2

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。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

3.3

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。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

3.4

一般数据　general data

核心数据、重要数据之外的其他数据。

3.5

个人信息　personal information

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。

3.6

敏感个人信息　sensitive personal information

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。

3.7

行业领域数据　industry sector data

在某个行业领域内依法履行工作职责或开展业务活动中收集和产生的数据。

3.8

公共数据　public data

各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据。

3.9

组织数据　organization data

组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据。

3.10

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。

3.11

数据处理者　data processor

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

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）　科学实用原则：从便于数据管理和使用的角度，科学选择常见、稳定的属性或特征作为数据分类的依据，并结合实际需要对数据进行细化分类。

b）　边界清晰原则：数据分级的各级别边界清晰，对不同级别的数据采取相应的保护措施。

c）　就高从严原则：采用就高不就低的原则确定数据级别，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。

d）　点面结合原则：数据分级既要考虑单项数据分级，也要充分考虑多个领域、群体或区域的数据汇聚融合后的安全影响，综合确定数据级别。

e）　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　数据分类规则

5.1　数据分类框架

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。

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。常见业务属性包括但不限于：

1）　业务领域：按照业务范围、业务种类或业务功能进行细化分类；

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：按照数据描述的对象进行细化分类；

注 1：按照描述对象分为用户数据、业务数据、经营管理数据、系统运维数据，见附录 A 的 A.1。

4） 流程环节：按照业务流程、产业链环节进行细化分类；

注 2：能源数据按照流程环节分为探勘、开采、生产、加工、销售、使用等数据。

5） 数据主体：按照数据主体或属主进行细化分类；

注 3：按照数据主体分为公共数据、组织数据、个人信息，见 A.2。

6） 内容主题：按照数据描述的内容主题进行细化分类；

7） 数据用途：按照数据处理目的、用途进行细化分类；

8） 数据处理：按照数据处理活动或数据加工程度进行细化分类；

9） 数据来源：按照数据来源、收集方式进行细化分类。

c） 如涉及法律法规有专门管理要求的数据类别（如个人信息等），应按照有关规定和标准进行识别和分类。

注 4：个人信息分类示例见附录 B，敏感个人信息识别和分类见敏感个人信息国家标准。

5.2 数据分类方法

数据分类可根据数据管理和使用需求，结合已有数据分类基础，灵活选择业务属性将数据细化分类。具体参考以下步骤开展行业领域数据分类。

a） 明确数据范围：按照行业领域主管（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，明确行业领域或业务条线的分类；

注 1：工业领域数据，按照部门职责分成原材料、装备制造、消费品、电子信息制造、软件和信息技术服务等类别。

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

注 2：原材料分为钢铁、有色金属、石油化工等；装备制造分为汽车、船舶、航空、航天、工业母机、工程机械等。

c） 业务属性分类：选择合适的业务属性，对关键业务的数据进行细化分类。

d） 确定分类规则：梳理分析各关键业务的数据分类结果，根据行业领域数据管理和使用需求，确定行业领域数据分类规则，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：钢铁数据按照数据描述对象，分为用户数据、业务数据、经营管理数据、系统运维数据等，业务数据细分为研发设计数据、控制信息、工艺参数等，其中研发设计数据类别能标识为“工业数据-原材料数据-钢铁数据-业务数据-研发设计数据”。

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：工业领域数据也按照数据处理、流程环节等业务属性进行分类，首先按照数据处理者类型分为工业企业工业数据、平台企业工业数据，再将工业企业工业数据分为研发数据、生产数据、运维数据、管理数据、外部数据，然后按照数据主题将生产数据分为控制信息、工况状态、工艺参数、系统日志等。

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 数据分级方法

数据分级是为了保护数据安全，具体可参考以下步骤进行数据分级。

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、跨行业领域数据等。

注 1：数据项通常表现为数据库表某一列字段等。数据集是由多个数据记录组成的集合，如数据库表、数据库一行或多行记录集合、数据文件等。

注 2：跨行业领域数据是指某个行业领域收集或产生的数据流转到另一个行业领域，以及两个或两个以上行业领域的数据融合加工产生的数据。

b) 分级要素识别：结合自身数据特点，按照 6.3 识别数据涉及的分级要素情况。

c) 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、损毁或者非法获取、非法使用、非法共享，可能影响的对象（见 6.4.1）和影响程度（见 6.4.2）。

d) 综合确定级别：按照 6.5 和 6.6，综合确定数据级别。

6.3 数据分级要素

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。数据分级应首先识别以下数据分级要素情况，具体考虑因素见附录 C。

a) 领域：数据描述的业务或内容范畴。数据领域可识别数据描述的行业领域、业务条线、流程环节、内容主题等因素。

b) 群体：数据主体或描述对象集合。数据群体可识别数据描述的人群、组织、网络和信息系统、资源物资等因素。

c) 区域：数据涉及的地区范围。数据区域可识别数据描述的行政区划、特定地区等因素。

d) 精度：数据的精确或准确程度。数据精度可识别数值精度、空间精度、时间精度等因素。

e) 规模：数据规模及数据描述的对象范围或能力大小。数据规模可识别数据存储量、群体规模、区域规模、领域规模、生产加工能力等因素。

f) 深度：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。数据深度可识别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：数据对领域、群体、区域、时段等的覆盖分布或疏密程度。数据覆盖度可识别对领域、群体、区域、时间段的覆盖占比、覆盖分布等因素。

h) 重要性：数据在经济社会发展中的重要程度。重要性可识别数据在经济建设、政治建设、文化建设、社会建设、生态文明建设等方面的重要程度。

6.4 数据影响分析

6.4.1 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，见附录 D。影响对象通常包括国家安全、经济运行、社会秩序、公共利益、组织权益、个人权益，判断影响对象的常见考虑因素见附录 E。

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) 社会秩序：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：影响自然人的人身权、财产权、隐私权、个人信息权益等个人权益。

6.4.2 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。开展数据影响分析时，应按照以下规则确定影响程度，影响程度参考示例见附录 F。

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。

6.5 级别确定规则

核心数据、重要数据、一般数据的确定规则如下，数据级别与影响对象、影响程度的对应关系见表 1。

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、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） 经行业领域主管（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。

表 1 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
国家安全	核心数据	核心数据	重要数据
经济运行	核心数据	重要数据	一般数据
社会秩序	核心数据	重要数据	一般数据
公共利益	核心数据	重要数据	一般数据
组织权益、个人权益	一般数据	一般数据	一般数据
注：如果影响大规模的个人或组织权益，影响对象可能不只包括个人权益或组织权益，也可能对国家安全、经济运行、社会秩序或公共利益造成影响。			

6.6 综合确定级别

在分级要素识别、数据影响分析的基础上，按照以下规则确定数据级别。

a） 应按照 6.5 规定的数据级别确定规则，识别核心数据、重要数据和一般数据。

b） 重要数据的识别，在符合 6.5b）的基础上应按照附录 G 执行。

c） 如待分级数据涉及多个要素、多个影响对象或影响程度，应按照就高从严原则确定数据级别。

d） 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，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：数据集中各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。

e） 在 6.1 规定的数据分级框架下，如还需对一般数据进行细化分级保护，可参考附录 H 对一般数据进行分级。

f） 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，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、社会秩序、公共利益、组织权益、个人权益的影响进行确定，具体见附录 I。

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

h） 根据数据重要程度和可能造成的危害程度的变化，应对数据级别进行动态更新，更新情形见附录J。

7 数据分类分级流程

7.1 行业领域数据分类分级流程

行业领域主管（监管）部门在遵循国家有关规定要求的基础上，可参考以下步骤开展行业领域数据分类分级工作。

a） 制定行业标准规范：按照国家数据分类分级保护有关要求，参照本文件制定本行业本领域的数据分类分级标准规范，重点可明确以下内容：

1） 明确行业数据分类细则，确定数据分类所依据的业务属性，给出按照业务属性划分的数据类别；

2） 分析行业领域数据的领域、群体、区域、精度、规模、深度、重要性等分级要素，明确本行业本领域重要数据识别细则，确定哪些数据可确定为重要数据；

3） 明确本行业本领域核心数据识别细则，提出哪些数据建议确定为核心数据；

4） 明确本行业本领域一般数据范围。

b） 开展数据分类分级：行业领域主管（监管）部门，根据本行业本领域的数据分类分级标准规范，组织本行业本领域数据处理者开展数据分类分级工作，指导数据处理者准确识别、及时报送重要数据和核心数据目录信息。

7.2 处理者数据分类分级流程

数据处理者进行数据分类分级时，应在遵循国家和行业领域数据分类分级要求的基础上，参考以下步骤开展数据分类分级工作。

a） 数据资产梳理：对数据资产进行全面梳理，确定待分类分级的数据资产及其所属的行业领域。

b） 制定内部规则：按照行业领域数据分类分级标准规范，结合处理者自身数据特点，参考本文件制定自身的数据分类分级细则：

1） 如行业领域主管部门已制定行业领域数据分类分级规则，处理者应结合自身实际参考本文件的数据分类分级方法，按照行业领域数据分类分级规则细化执行；

2） 如所属行业领域没有行业主管部门认可的数据分类分级标准规范的，或存在行业领域规范未覆盖的数据类型，按照本文件进行数据分类分级；

3） 如果业务涉及多个行业领域，可在参考本文件的基础上，分别按照各个行业领域的数据分类分级标准规范细化执行。

c） 实施数据分类：对数据进行分类，并对公共数据、个人信息等特殊类别数据进行识别和分类。

d） 实施数据分级：对数据进行分级，确定核心数据、重要数据和一般数据的范围。

注：由于一般数据涵盖范围较广，数据处理者结合组织自身安全需求，参考附录H对一般数据进行细化分级。

e） 审核上报目录：对数据分类分级结果进行审核，形成数据分类分级清单、重要数据和核心数据目录，并对数据进行分类分级标识，按有关程序报送目录。

f） 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，动态更新情形见附录J。

附 录 A
（资料性）
基于描述对象与数据主体的数据分类参考

A.1 基于描述对象的数据分类参考

从数据描述对象角度，可将数据分为用户数据、业务数据、经营管理数据、系统运维数据四个类别，数据分类参考示例见表 A.1。

表 A.1 基于描述对象的数据分类参考示例

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的归属于用户的数据	如个人信息、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	数据处理者在单位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、并购融资信息、人力资源数据、市场营销数据等
系统运维数据	网络和信息系统运行维护、日志记录及网络安全数据	如网络设备和信息系统的配置数据、日志数据、安全监测数据、安全漏洞数据、安全事件数据等

A.2 基于数据主体的数据分类参考

从数据主体角度，可将数据分为公共数据、组织数据、个人信息三个类别，数据分类参考示例见表 A.2。

表 A.2 基于数据主体的数据分类参考示例

数据分类	类别定义	示例
公共数据	各级政务部门、具有公共管理和服务职能的组织及其技术支撑单位，在依法履行公共事务管理职责或提供公共服务过程中收集、产生的数据	如政务数据，在供水、供电、供气等公共服务运营过程中收集和产生的数据等
组织数据	组织在自身生产经营活动中收集、产生的不涉及个人信息和公共利益的数据	如不涉及个人信息和公共利益的业务数据、经营管理数据、系统运维数据等
个人信息	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	如个人身份信息、个人生物识别信息、个人财产信息、个人通信信息、个人位置信息、个人健康生理信息等

附 录 B
（资料性）
个人信息分类示例

表 B.1 参考 GB/T 35273—2020 给出了个人信息的一级类别、二级类别和典型数据示例。

表 B.1 个人信息分类参考示例

一级类别	二级类别	典型示例和说明
个人基本资料	个人基本资料	自然人基本情况信息，如个人姓名、生日、年龄、性别、民族、国籍、籍贯、政治面貌、婚姻状况、家庭关系、住址、个人电话号码、电子邮件地址、兴趣爱好等
个人身份信息	个人身份信息	可直接标识自然人身份的信息，如身份证、军官证、护照、驾驶证、工作证、社保卡、居住证、港澳台通行证等证件号码、证件照片或影印件等。其中特定身份信息属于敏感个人信息，具体参见敏感个人信息国家标准
个人生物识别信息	生物识别信息	个人面部识别特征、虹膜、指纹、基因、声纹、步态、耳廓、眼纹等生物特征识别信息，包括生物特征识别原始信息（如样本、图像）、比对信息（如特征值、模板）等
网络身份标识信息	网络身份标识信息	可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），如用户账号、用户标识符（用户 ID）、即时通信账号、网络社交用户账号、用户头像、昵称、个性签名、互联网协议地址（IP 地址）等
个人健康生理信息	健康状况信息	与个人身体健康状况相关的个人信息，如体重、身高、体温、肺活量、血压、血型等
	医疗健康信息	个人因疾病诊疗等医疗健康服务产生的相关信息，如医疗就诊记录、生育信息、既往病史等，具体范围参见敏感个人信息国家标准
个人教育工作信息	个人教育信息	个人教育和培训的相关信息，如学历、学位、教育经历、学号、成绩单、资质证书、培训记录、奖惩信息、受资助信息等
	个人工作信息	个人求职和工作的相关信息，如个人职业、职位、职称、工作单位、工作地点、工作经历、工资、工作表现、简历、离退休状况等
个人财产信息	金融账户信息	金融账户及鉴别相关信息，如银行、证券等账户的账号、密码等，具体参见敏感个人信息国家标准
	个人交易信息	交易过程中产生的交易信息和消费记录，如交易订单、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
	个人资产信息	个人实体和虚拟财产信息，如个人收入状况、房产信息、存款信息、车辆信息、纳税额、公积金缴存明细、银行流水、虚拟财产（如虚拟货币、虚拟交易、游戏类兑换码等）等
	个人借贷信息	个人在借贷过程中产生的信息，如个人借款信息、还款信息、欠款信息、信贷记录、征信信息、担保情况等
身份鉴别信息	身份鉴别信息	用于个人身份鉴别的数据，如账号口令、数字证书、短信验证码、密码提示问题等

表 B.1　个人信息分类参考示例（续）

一级类别	二级类别	典型示例和说明
个人通信信息	个人通信信息	通信记录，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
联系人信息	联系人信息	描述个人与关联方关系的信息，如通讯录、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、父母或监护人信息、配偶信息等
个人上网记录	个人操作记录	个人在业务服务过程中的操作记录和行为数据，包括网页浏览记录、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、服务使用时间、下载记录等
	业务行为数据	用户使用某业务的行为记录（如游戏业务：用户游戏登录时间、最近充值时间、累计充值额度、用户通关记录）等
个人设备信息	可变更的唯一设备识别码	Android ID、广告标识符（IDFA）、应用开发商标识符（IDFV）、开放匿名设备标识符（OAID）等
	不可变更的唯一设备识别码	国际移动设备识别码（IMEI）、移动设备识别码（MEID）、设备媒体访问控制（MAC）地址、硬件序列号等
	应用软件列表	用户在终端上安装的应用程序列表，如每款应用软件的名称、版本等
个人位置信息	粗略位置信息	仅能定位到行政区、县级等的位置信息，如地区代码、城市代码等
	行踪轨迹信息	与个人所处地理位置、活动地点和活动轨迹等相关的信息，具体范围参见敏感个人信息国家标准
	住宿出行信息	个人住宿信息，及乘坐飞机、火车、汽车、轮船等交通出行信息等
个人标签信息	个人标签信息	基于个人上网记录等加工产生的个人用户标签、画像信息，如行为习惯、兴趣偏好等
个人运动信息	个人运动信息	步数、步频、运动时长、运动距离、运动方式、运动心率等
其他个人信息	其他个人信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录等

附 录 C
（资料性）
数据分级要素识别常见考虑因素

C.1 数据领域、群体、区域考虑因素

数据的领域、群体、区域识别常见考虑因素，包括但不限于以下内容。

——数据领域识别的常见考虑因素，例如：

- 行业领域；
- 业务条线、业务类目；
- 生产经营活动；
- 流程环节；
- 内容主题；
- 与国家安全、经济运行、社会秩序、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：

- 人群；
- 团体、单位、组织；
- 网络、信息系统、数据中心；
- 资源、原材料、物资；
- 元器件、设备；
- 项目；
- 基础设施；
- 与国家安全、经济运行、社会秩序、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、社会秩序、公共利益相关的区域等。

C.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。

C.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。

C.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；
——领域、群体或区域的特征分析，如人群或用户特征分析；
——行踪轨迹；
——对象关系；
——历史信息；
——产业供应链。

C.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、区域覆盖分布、区域覆盖密度等；
——时段覆盖分布或密度，如时间段覆盖度、时间段覆盖分布、时间段覆盖密度等。

C.6 数据重要性考虑因素

数据重要性识别常见考虑因素，例如：
a) 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；
b) 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；
c) 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；
d) 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；
e) 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；
f) 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。

附 录 D
（资料性）
安全风险常见考虑因素

数据影响分析通常考虑以下安全风险。

a） 数据泄露：数据窃取、未授权访问数据、违规导出数据等破坏数据保密性风险。

b） 数据篡改：未授权修改、注入、仿冒、伪造数据等破坏数据完整性风险。

c） 数据损毁：也称数据破坏，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。

d） 非法获取数据：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风险。

e） 非法使用数据：也称非法利用数据，违反法律、行政法规等有关规定，使用、加工、委托处理数据。

f） 非法共享数据：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 E
（资料性）
影响对象考虑因素

E.1 国家安全

判断数据是否可能影响国家安全，常见考虑因素包括但不限于：

a） 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；
b） 影响领土安全、国家统一、边疆安全和国家海洋权益；
c） 影响基本经济制度安全、供给侧结构性改革、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；
d） 影响国家科技实力、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；
e） 影响社会主义核心价值观、文化软实力、中华优秀传统文化等；
f） 影响国家社会治理体系、社会治安防控体系、应急管理体系等；
g） 影响生态环境安全、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；
h） 影响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；
i） 影响电磁空间、网络空间安全、关键信息基础设施安全、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；
j） 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；
k） 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；
l） 影响在太空、深海、极地等领域的国家利益和国际合作安全；
m） 影响海外重大项目和人员机构安全、海外能源资源安全、海上战略通道安全等。

E.2 经济运行

判断数据是否可能影响经济运行，常见考虑因素包括但不限于：

a） 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；
b） 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；
c） 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；
d） 影响行业领域或地区的经济发展、业务生产、技术进步、产业生态等。

E.3 社会秩序

判断数据是否可能影响社会秩序，常见考虑因素包括但不限于：

a） 影响社会稳定，可能引发社会恐慌，导致重大突发事件、群体性事件、暴力恐怖活动、社会治安问题等；

b) 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、文体、健康、养老、社保等民生事项或供电、供气、供水等基本服务保障工程；
c) 影响国家机关、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；
d) 影响各级政务部门依法履行公共管理和服务职能；
e) 影响司法领域的公正、公信或权威性；
f) 影响公共场所的活动秩序、公共交通秩序。

E.4 公共利益

判断数据是否可能影响公共利益，常见考虑因素包括但不限于：
a) 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；
b) 影响社会成员使用公共设施；
c) 影响社会成员获取公开数据资源；
d) 影响社会成员接受公共服务等方面；
e) 其他影响公共利益、社会秩序的数据。

E.5 组织权益

判断数据是否可能影响组织权益，常见考虑因素包括但不限于：
a) 导致组织遭到监管部门处罚、安全事件或法律诉讼；
b) 影响组织的重要或关键业务生产经营；
c) 造成组织经济损失；
d) 破坏组织声誉形象、公信力等；
e) 影响组织的知识产权、商业秘密、技术损失等；
f) 影响组织的公平竞争利益；
g) 其他影响法人、非法人组织合法权益的数据。

E.6 个人权益

判断数据是否可能影响个人权益，常见考虑因素包括但不限于：
a) 影响个人私人活动、私有领域、私密部位等个人隐私；
b) 影响自然人的人格尊严；
c) 影响自然人的人身安全；
d) 影响自然人的财产安全；
e) 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；
f) 其他影响个人权益的数据。

附 录 F
（资料性）
影响程度参考示例

表 F.1 给出了不同影响对象对应的影响程度参考示例。

表 F.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

表 F.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 1 000 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 G
（规范性）
重要数据识别指南

重要数据识别应在符合 6.5b)的基础上，考虑如下因素：

a) 直接影响领土安全和国家统一，或反映国家自然资源基础情况，如未公开的领陆、领水、领空数据；

b) 可被其他国家或组织利用发起对我国的军事打击，或反映我国战略储备、应急动员、作战等能力，如满足一定精度指标的地理数据或与战略物资产能、储备量有关的数据；

c) 直接影响市场经济秩序，如支撑关键信息基础设施所在行业、领域核心业务运行或重要经济领域生产的数据；

d) 反映我国语言文字、历史、风俗习惯、民族价值观念等特质，如记录历史文化遗产的数据；

e) 反映重点目标、重要场所物理安全保护情况或未公开地理目标的位置，可被恐怖分子、犯罪分子利用实施破坏，如描述重点安保单位、重要生产企业、国家重要资产（如铁路、输油管道）的施工图、内部结构、安防情况的数据；

f) 关系我国科技实力、影响我国国际竞争力，或关系出口管制物项，如反映国家科技创新重大成果，或描述我国禁止出口限制出口物项的设计原理、工艺流程、制作方法的数据，以及涉及源代码、集成电路布图、技术方案、重要参数、实验数据、检测报告的数据；

g) 反映关键信息基础设施总体运行、发展和安全保护情况及其核心软硬件资产信息和供应链管理情况，可被利用实施对关键信息基础设施的网络攻击，如涉及关键信息基础设施系统配置信息、系统拓扑、应急预案、测评、运行维护、审计日志的数据；

h) 涉及未公开的攻击方法、攻击工具制作方法或攻击辅助信息，可被用来对重点目标发起供应链攻击、社会工程学攻击等网络攻击，如政府、军工单位等敏感客户清单，以及涉及未公开的产品和服务采购情况、未公开重大漏洞情况的数据；

i) 反映自然环境、生产生活环境基础情况，或可被利用造成环境安全事件，如未公开的与土壤、气象观测、环保监测有关的数据；

j) 反映水资源、能源资源、土地资源、矿产资源等资源储备和开发、供给情况，如未公开的描述水文观测结果、耕地面积或质量变化情况的数据；

k) 反映核材料、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，如涉及核电站设计图、核电站运行情况的数据；

l) 关系海外能源资源安全、海上战略通道安全、海外公民和法人安全，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，如描述国际贸易中特殊物项生产交易以及特殊装备配备、使用和维修情况的数据；

m) 关系我国在太空、深海、极地等战略新疆域的现实或潜在利益，如未公开的涉及对太空、深海、极地进行科学考察、开发利用的数据，以及影响人员在上述领域安全进出的数据；

n) 反映生物技术研究、开发和应用情况，反映族群特征、遗传信息，关系重大突发传染病、动植物疫情，关系生物实验室安全，或可能被利用制造生物武器、实施生物恐怖袭击，关系外来物种入侵和生物多样性，如重要生物资源数据、微生物耐药基础研究数据；

o) 反映全局性或重点领域经济运行、金融活动状况，关系产业竞争力，可造成公共安全事故或影响公民生命安全，可引发群体性活动或影响群体情感与认知，如未公开的统计数据、重点企业商业秘密；

p) 反映国家或地区群体健康生理状况，关系疾病传播与防治，关系食品药品安全，如涉及健康医

疗资源、批量人口诊疗与健康管理、疾控防疫、健康救援保障、特定药品实验、食品安全溯源的数据；

q） 其他可能影响国土、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、人工智能等安全的数据；

注 1：影响国家安全的考虑因素见 E.1。

r） 其他可能对经济运行、社会秩序或公共利益造成严重危害的数据。

注 2：对经济运行、社会秩序、公共利益造成严重危害的参考示例见表 F.1。

具备以上因素之一的数据，可被识别为重要数据。

附 录 H
（资料性）
一般数据分级参考

H.1 一般数据分 4 级参考

按照数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对经济运行、社会秩序、公共利益或个人、组织合法权益等造成的危害程度，将一般数据从低到高分为 1 级、2 级、3 级、4 级共四个级别。

a） 1 级数据：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，不会对个人权益、组织权益等造成危害。1 级数据具有公共传播属性，可对外公开发布、转发传播，但也需考虑公开的数据量及类别，避免由于类别较多或者数量过大被用于关联分析。

b） 2 级数据：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，对个人权益、组织权益造成一般危害。2 级数据通常在组织内部、关联方共享和使用，相关方授权后可向组织外部共享。

c） 3 级数据：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，对个人权益、组织权益造成严重危害。3 级数据仅可由授权的内部机构或人员访问，如果要将数据共享到外部，需要满足相关条件并获得相关方的授权。

d） 4 级数据：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，对个人权益、组织权益造成特别严重危害，或对经济运行、社会秩序、公共利益造成一般危害。4 级数据按照批准的授权列表严格管理，仅能在受控范围内经过严格审批、评估后才可共享或传播。

H.2 一般数据分 3 级参考

按照数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对经济运行、社会秩序、公共利益或个人、组织合法权益等造成的危害程度，将一般数据从低到高分为 1 级、2 级、3 级共三个级别。

a） 1 级数据：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，对个人权益、组织权益造成一般危害或无危害。

b） 2 级数据：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，对个人权益、组织权益造成严重危害。

c） 3 级数据：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，对个人权益、组织合法权益造成特别严重危害，或者对经济运行、社会秩序、公共利益造成一般危害。

H.3 一般数据分 2 级参考

按照数据一旦遭到泄露、篡改、损毁或者非法获取、非法使用、非法共享，对经济运行、社会秩序、公共利益或个人、组织合法权益等造成的危害程度，将一般数据从低到高分为 1 级、2 级。

a） 1 级数据：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，对个人权益、组织权益造成一般、严重危害或无危害。

b） 2 级数据：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，对个人权益、组织权益造成特别严重危害，或者对经济运行、社会秩序、公共利益造成一般危害。

H.4 最低参考级别

一般数据分级应对个人信息、公共数据等特定类型数据设置合理的数据级别，特定类型数据最低参

考级别如下。

a) 在一般数据分 4 级框架下,特定类型一般数据的最低参考级别为:
   1) 敏感个人信息不低于 4 级,一般个人信息不低于 2 级;
   2) 组织内部员工个人信息不低于 2 级;
   3) 去标识化的个人信息不低于 2 级;
   4) 个人标签信息不低于 2 级;
   5) 有条件开放/共享的公共数据级别不低于 2 级,禁止开放/共享的公共数据不低于 4 级。
b) 在一般数据 3 级框架下,特定类型一般数据的最低参考级别为:
   1) 敏感个人信息不低于 3 级,一般个人信息不低于 2 级;
   2) 有条件开放/共享的公共数据级别不低于 2 级,禁止开放/共享的公共数据不低于 3 级。
c) 在一般数据 2 级框架下,敏感个人信息不低于 2 级,禁止开放/共享的公共数据不低于 2 级。

附 录 I
（资料性）
衍生数据分级参考

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，见表 I.1。

表 I.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	如去标识化的个人信息等
标签数据	对用户行为进行画像分析，生成用户标签数据描述用户属性特征	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原始数据级别，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：

——脱敏数据级别可比原始数据级别降低；

——标签数据级别可比原始数据级别降低或升高；

——统计数据级别可比原始数据级别降低或升高；

注：例如，反映国民经济运行总体情况、行业领域产业发展态势、影响国家宏观调控能力的未公开统计数据，设置比原始数据级别更高的级别；又如，原始数据包含大量原始明细数据，而衍生数据是不敏感的统计特征，设置比原始数据级别更低的级别。

——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 J
（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：

a） 数据规模变化，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、数据应用场景、数据加工处理方式等发生显著变化；

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） 数据进行脱敏或删除关键字段，或者经过去标识化、匿名化处理；

g） 发生数据安全事件，导致数据敏感性发生变化；

h） 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；

i） 需要对数据安全级别进行变更的其他情形。

参 考 文 献

[1] GB/T 21063.4 政务信息资源目录体系 第4部分:政务信息资源分类
[2] GB/T 35273—2020 信息安全技术 个人信息安全规范
[3] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
[4] GB/T 42012—2022 信息安全技术 即时通信服务数据安全要求
[5] GB/T 42013—2022 信息安全技术 快递物流服务数据安全要求
[6] GB/T 42014—2022 信息安全技术 网上购物服务数据安全要求
[7] GB/T 42015—2022 信息安全技术 网络支付服务数据安全要求
[8] GB/T 42016—2022 信息安全技术 网络音视频服务数据安全要求
[9] GB/T 42017—2022 信息安全技术 网络预约汽车服务数据安全要求
[10] JR/T 0197—2020 金融数据安全 数据安全分级指南
[11] 中华人民共和国数据安全法
[12] 中华人民共和国网络安全法
[13] 中华人民共和国个人信息保护法