ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术　网络数据分类分级要求

Information security technology — Requirements for classification and grading of network data

（征求意见稿）

（本稿完成时间：2022 年 9 月 14 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－XX－XX 发布　　XXXX－XX－XX 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

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。

本文件由全国信息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、中国网络安全审查技术与认证中心、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、中国人民公安大学、阿里巴巴（北京）软件服务有限公司、北京字节跳动科技有限公司、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、北京快手科技有限公司、中移动信息技术有限公司、中国电信集团有限公司、北京爱奇艺科技有限公司、联通数字科技有限公司、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、亚信科技（成都）有限公司等。

本文件主要起草人：姚相振、胡影、周晨炜、上官晓丽、任英杰、左晓栋、卓子寒、邢潇、杨韬、段静辉、许静慧、李媛、任卫红、唐前进、曹京、张夕夜、芦天亮、彭俊涛、孙勇、杨骁涵、白晓媛、常新苗、李实、王海棠、钟书翔、落红卫、范东媛、杨立宝、许琛超、樊庆君、蓝宇娜、张屹、廖双晓、叶润国、宋博韬、姚卓、宋晓鹏、刘前伟、安锦程等。

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、破坏、泄露或者非法获取、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，对数据实行分类分级保护”。

开展数据分类分级保护工作时，首先需要对数据进行分类和分级，然后对不同类别不同级别的数据建立相应的全流程数据安全保护措施。本文件根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》及国家数据分类分级保护有关规定，给出了数据分类分级的原则和方法，用于指导各行业、各领域、各地方、各部门和数据处理者开展数据分类分级工作。涉及国家秘密的数据和军事数据不适用于本文件。

信息安全技术　网络数据分类分级要求

1　范围

本文件给出了数据分类分级的原则和方法，包括数据分类分级基本原则、数据分类框架和方法、数据分级框架和方法等。

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，也适用于各地方、各部门开展本地区、本部门的数据分类分级工作，同时还可为数据处理者进行数据分类分级提供参考。

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 25069—2022　信息安全技术　术语

3　术语与定义

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数据，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。

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、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。

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，不包括匿名化处理后的信息。

3.6

行业领域数据 industry sector data

在某个行业领域依法履行工作职责或业务运营活动中收集和产生的数据。

3.7

组织数据 organization data

组织在自身的业务生产、经营管理和信息系统运维过程中收集和产生的数据。

3.8

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。

4 基本原则

在遵循国家数据分类分级保护要求的基础上，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：数据分类应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：数据分级的主要目的是为了数据安全，各个数据级别应做到边界清晰，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分级，当多个因素可能影响数据分级时，按照可能造成的最高影响对象和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对数据重要性、安全风险等的影响，通过定量与定性相结合的方式综合确定数据级别。
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 数据分类框架和方法

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) 按照业务所属行业领域，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、科学数据等行业领域数据。
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 行业领域数据分类方法

行业领域开展数据分类时，应根据行业领域数据管理和使用需求，结合本行业本领域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。行业领域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分类；
   注 1：例如，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：例如，原材料可分为钢铁、有色金属、石油化工等；装备制造可分为汽车、船舶、航空、航天、工业母机、工程机械等。
c) 业务属性分类：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领域数据分类参考示例。
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：例如，钢铁数据按照数据描述对象，可分为用户数据、业务数据、经营管理数据、系统运行和安全数据等，用户数据可细分为个人身份信息、网络身份标识信息、个人上网记录等，业务数据可细分为研发设计数据、控制信息、工艺参数等，数据类别标识为“工业数据-原材料数据-钢铁数据-用户数据-个人身份信息”、“工业数据-原材料数据-钢铁数据-业务数据-研发设计数据”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，工业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。

5.3 数据处理者数据分类流程

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领域；
b) 按照业务所属行业领域的数据分类规则，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) 如果存在行业领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。

6 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、一般三个级别。各行业各领域应在遵循数据分级框架的基础上，明确本行业本领域数据分级规则，并对行业领域数据进行定级。

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) 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。

7 数据分级确定方法

7.1 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。

7.2 数据分级要素

影响数据分级的要素，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，常见考虑因素见附录B。

a） 领域：是指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。
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。

7.3 数据影响分析

7.3.1 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。

7.3.2 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、社会或行业领域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。

7.4 分级参考规则

影响对象、影响程度与数据级别的关系如表 1 所示。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) 经行业领域主管（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。

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
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	重要数据
社会稳定	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

7.5 数据分级流程

7.5.1 数据分级步骤

可参考以下步骤开展数据分级。

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：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。跨行业领域数据是指跨行业领域流动的数据，及多个行业领域数据融合加工的数据。

b) 分级要素识别：按照 7.2 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) 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 7.3.1）和影响程度（见 7.3.2）。

d) 综合确定级别：按照 7.4 的分级参考规则，综合确定数据级别。

7.5.2 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7.4分级参考规则综合确定数据级别。

a) 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 7.4 中 a）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 7.4 中 b）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 7.4 中 c）进行评估。

b) 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。

c) 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。

d) 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，需考虑跨行业领域对数据分级要素的影响，按照衍生数据确定级别。

f) 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。

7.5.3 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，结合行业领域数据分级要素识别、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。

a) 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。

b) 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。

c) 明确本行业本领域一般数据范围。

注：行业领域也可以根据工作需要对一般数据进行细化分级。

8 数据分类分级实施流程

数据分类分级可参考图1所示流程实施，主要步骤包括：

a) 数据资产梳理：对数据资产进行全面梳理，包括以物理或电子形式记录的数据库表、数据项、数据文件等结构化和非结构化数据资产，明确数据资产基本信息和相关方，形成数据资产清单。

b) 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规则，对数据进行分类，同时对个人信息、敏感个人信息进行识别和分类。

c) 数据分级：按照数据分类分级有关要求，参考第 6、7 章建立自身的数据分级规则，并对数据进行分级。

注：由于一般数据涵盖范围较广，数据处理者可结合组织自身需求，对一般数据进行细化分级，本文件附录 G 给出了一般数据分级的参考规则。

d) 审核上报目录：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，按有关程序报送重要数据和核心数据目录等。

e) 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，动态更新情形参加附录 F。

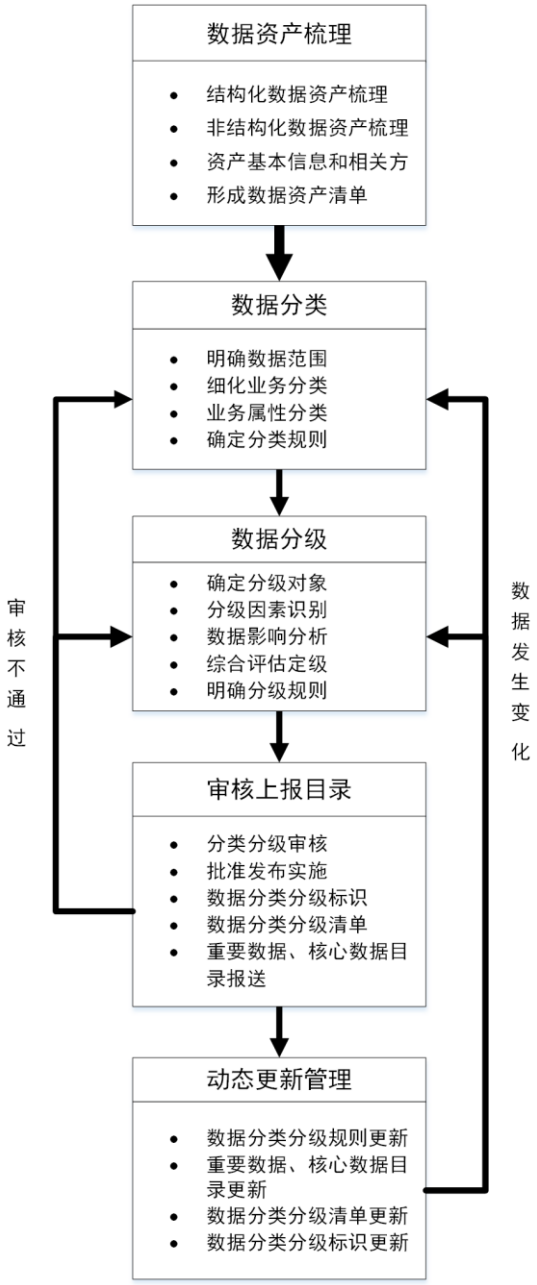

图 1 数据分类分级实施流程

附 录 A
（资料性）
基于数据描述对象的行业领域数据分类参考示例

表A.1从数据描述对象角度，将行业领域数据分为用户数据、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：

a) 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）；
b) 从便于行业领域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；
c) 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；
d) 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 行业领域数据分类参考示例

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：

——数据领域识别的常见考虑因素，例如：

- 行业领域；
- 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：
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；
c） 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；
d） 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；
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。

B.7 安全风险考虑因素

安全风险识别常见考虑因素，例如：

a) 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。
b) 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。
c) 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。
d) 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。
e) 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。
f) 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：

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、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；
d) 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；
e) 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；
f) 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；
g) 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；
h) 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；
i) 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；
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) 影响我国在太空、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：

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。
d） 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：

a） 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；
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；
c） 影响各级党政机关依法履行公共管理和服务职能；
d） 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；
e） 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：
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：
a) 可能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、技术损失等；
f) 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：
a) 可能导致自然人的人格尊严受到侵害；
b) 影响自然人的人身安全；
c) 影响自然人的财产安全；
d) 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；
e) 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
	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，或者直接影响行业领域核心竞争力、关键产业链、核心供应链等
	一般危害	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
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
	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

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 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 7 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：

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、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、假名化、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。

附 录 G
（资料性）
一般数据分级参考

G.1 一般数据分 4 级参考

按照数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对社会稳定、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、破坏或者非法获取、非法利用，不会对个人权益、组织合法权益造成危害。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、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成一般危害。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、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成严重危害。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、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成特别严重危害，或可能对公共利益、社会稳定造成一般危害。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。

G.2 一般数据分 3 级参考

按照数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对社会稳定、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、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成一般危害；

b) 2 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成严重危害；

c) 3 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织合法权益造成特别严重危害，或者可能对公共利益、社会稳定造成一般危害。

G.3 一般数据分 2 级参考

按照数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，对社会稳定、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、破坏或者非法获取、非法利用，可能对个人权益、组织权益造成一般或严重危害；

b） 2 级数据：数据一旦遭到泄露、篡改、破坏或者非法获取、非法利用，可能对个人权益、组织权益造成特别严重危害，或者可能对公共利益、社会稳定造成一般危害；

G.4 最低参考级别

一般数据分级要考虑敏感个人信息等特定类型数据的敏感性，特定类型数据最低参考级别包括：

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如下：

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，匿名化个人信息不低于1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/共享的公共数据或政务数据不低于4级。

b） 在一般数据 3 级框架下，敏感个人信息不低于 3 级，禁止开放/共享的公共数据或政务数据不低于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/共享的公共数据或政务数据不低于2级。

附 录 H
（资料性）
个人信息分类示例

表H.1给出了个人信息的一级类别、二级类别和相关数据示例。

表 H.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、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、出入证、社保卡、居住证、港澳台通行证等证件号码、证件有效期、证件照片或影印件等
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），如人脸、指纹、步态、声纹、基因、虹膜、笔迹、掌纹、耳廓、眼纹等
网络身份标识信息	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），如用户账号、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、IP 地址、账户开立时间等
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一般信息，如体重、身高、体温、肺活量、血压、血型等
	个人医疗信息	个人因生病医治等产生的相关记录，如病症、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
个人教育工作信息	个人教育信息	个人受教育和培训情况相关信息，如学历、学位、教育经历（如入学日期、毕业日期、学校、院系、专业等）、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	个人求职和工作情况相关信息，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、简历等
个人财产信息	金融账户信息	金融账户及账户相关信息，如银行卡号、支付账号、银行卡磁道数据（或芯片等效信息）、银行卡有效期、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、支付标记信息等
	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（含余额、基数、缴纳公司、公积金中心、状态等）、银行流水、虚拟财产（虚拟货币、虚拟交易、游戏类兑换码等）、个人社保与医保存缴金额等

一级类别	二级类别	典型示例和说明
	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
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、访问时间（含登录时间、退出时间）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、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
	应用软件列表	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
	精确位置信息	能具体定位到个人的地理位置数据，包括经纬度、住宿信息、小区代码、基站号、基站经纬度坐标等
	个人出行信息	乘坐飞机、火车、汽车、轮船等交通信息，行踪轨迹等
个人标签信息	个人标签信息	基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，如 App 偏好、关系标签、终端偏好、内容偏好等标签信息
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
注：个人画像，是由多个用户个人标签组成的数据集。		