TC260-PG-20212A

网络安全标准实践指南

—网络数据分类分级指引

(v1.0-202112)

全国信息安全标准化技术委员会秘书处

2021 年 12 月

本文档可从以下网址获得：

www.tc260.org.cn/

全国信息安全标准化技术委员会

NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

声　明

本《实践指南》版权属于信安标委秘书处，未经秘书处书面授权，不得以任何方式抄袭、翻译《实践指南》的任何部分。凡转载或引用本《实践指南》的观点、数据，请注明“来源：全国信息安全标准化技术委员会秘书处”。

技术支持单位

本《实践指南》得到中国电子技术标准化研究院、中国移动通信集团有限公司、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、成都卫士通信息产业股份有限公司、亚信科技（成都）有限公司、北京百度网讯科技有限公司、北京奇虎科技有限公司、联通大数据有限公司、北京明朝万达科技股份有限公司、天翼电子商务有限公司、蚂蚁科技集团股份有限公司、深信服科技股份有限公司、北京爱奇艺科技有限公司、杭州安恒信息技术股份有限公司、北京字节跳动科技有限公司、阿里巴巴（北京）软件服务有限公司、OPPO广东移动通信有限公司、中国电信集团有限公司、北京数安行科技有限公司、顺丰速运有限公司、深圳市腾讯计算机系统有限公司、北京小桔科技有限公司、京东科技控股股份有限公司、闪捷信息科技有限公司、内蒙古自治区大数据中心等单位的技术支持。

摘　要

为贯彻落实《中华人民共和国数据安全法》中“国家建立数据分类分级保护制度”要求，保障国家安全、公共利益、个人和组织的合法权益，本实践指南依据法律法规和政策标准要求，给出了网络数据分类分级的原则、框架和方法，可用于指导数据处理者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。

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

目　录

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

1 范围

本实践指南给出了网络数据分类分级的原则、框架和方法。

本实践指南适用于指导数据处理者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 术语定义

2.1 网络数据

简称数据，是指任何以电子方式对信息的记录。

注：数据分类分级的对象通常是数据项、数据集。数据项是数据库表的某一列字段。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。

2.2 重要数据

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益的数据。

注1：重要数据不包括国家秘密。

注2：重要数据一般不包括个人信息和企业内部管理信息，但达到一定规模的个人信息或者基于海量个人信息加工形成的衍生数据，如其一旦遭到篡改、破坏、泄露或者非法获取、非法利用可能危害国家安全、公共利益，也应满足重要数据保护要求。

2.3 核心数据

即国家核心数据，是指关系国家安全、国民经济命脉、重要民生、重大公共利益等的数据。

2.4 一般数据

一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人、组织合法权益造成危害，但不会危害国家安全、公共利益的数据。

2.5 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，不包括匿名化处理后的信息。

2.6 公共数据

国家机关和依法经授权、受委托履行公共管理和服务职能的组织（以下统称公共管理和服务机构），在依法履行公共管理职责或提供公共服务过程中收集、产生的数据。

注1：公共管理和服务机构，包括各级政务机关、事业单位，其他依法经授权或受委托管理公共事务的组织，以及供水、供电、供气、公共交通、教育、卫生健康、社会福利、环境保护等提供公共服务的组织。

注2：本实践指南给出的公共数据是广义概念，实际使用时也存在狭义的公共数据，即仅将提供公共服务的组织在公共服务过程中收集产生的数据作为公共数据，将政务机关履职过程中收集产生的数据作为政务数据。

注3：公共数据通常不包括组织专有的知识产权数据和商业秘密。

2.7 公共传播信息

也称公共信息，数据处理者在提供公共服务过程中收集、产生的具有公共传播特性的信息。

2.8 组织数据

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。

2.9 衍生数据

原始数据经过统计、关联、挖掘或聚合等加工活动而产生的数据。

2.10 商业秘密

不为公众所知悉、具有商业价值并经权利人采取相应保密措施的技术信息、经营信息等商业信息。

3 数据分类分级原则

数据分类分级按照数据分类管理、分级保护的思路，依据以下原则进行划分:

a）**合法合规原则**：数据分类分级应遵循有关法律法规及部门规定要求，优先对国家或行业有专门管理要求的数据进行识别和管理，满足相应的数据安全管理要求。

b）**分类多维原则**：数据分类具有多种视角和维度，可从便于数据管理和使用角度，考虑国家、行业、组织等多个视角的数据分类。

c）**分级明确原则**：数据分级的目的是为了保护数据安全，数据分级的各级别应界限明确，不同级别的数据应采取不同的保护措施。

d）**就高从严原则**：数据分级时采用就高不就低的原则进行定级，例如数据集包含多个级别的数据项，按照数据项的最高级别对数据集进行定级。

e）**动态调整原则**：数据的类别级别可能因时间变化、政策变化、安全事件发生、不同业务场景的敏感性变化或相关行业规则不同而发生改变，因此需要对数据分类分级进行定期审核并及时调整。

4 数据分类分级框架

4.1 数据分类框架

数据分类具有多种视角和维度，其主要目的是便于数据管理和使用。本实践指南采用面分类法，从国家、行业、组织等视角给出了多个维度的数据分类参考框架。常见的数据分类维度，包括但不限于:

a）**公民个人维度**：按照数据是否可识别自然人或与自然人关联，将数据分为个人信息、非个人信息。

b）**公共管理维度**：为便于国家机关管理数据、促进数据共享开放，将数据分为公共数据、社会数据。

注：b）给出的分类是按照广义的公共数据进行分类，如果从狭义的公共数据角度，数据也可分为政务数据、公共数据、社会数据。

c）**信息传播维度**：按照数据是否具有公共传播属性，将数据分为公共传播信息、非公共传播信息。

d）**行业领域维度**：按照数据处理涉及的行业领域，将数据分为工业数据、电信数据、金融数据、交通数据、自然资源数据、卫生健康数据、教育数据、科技数据等，其他行业领域可参考 GB/T 4754—2017《国民经济行业分类》。

e）**组织经营维度**：在遵循国家和行业数据分类分级要求的基础上，数据处理者也可按照组织经营维度，将个人或组织用户的数据单独划分出来作为用户数据，用户数据之外的其他数据从便于业务生产和经营管理角度进行分类。附录 A 给出了组织经营维度的数据分类参考示例，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。

数据处理者进行数据分类时，可在遵循国家和行业数据分类要求的基础上，采用面分类法从多个维度进行分类，对不同维度的数据类别进行标识，每个维度的数据分类也可采用线分类法进行细分。

4.2 数据分级框架

按照《中华人民共和国数据安全法》要求，根据数据一旦遭到篡

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，将数据从低到高分成**一般数据、重要数据、核心数据共三个级别**。

上述三个级别是从国家数据安全角度给出的数据分级基本框架。由于一般数据涵盖数据范围较广，采用同一安全级别保护可能无法满足不同数据的安全需求。因此建议数据处理者优先按照基本框架进行定级，在基本框架定级的基础上也可结合行业数据分类分级规则或组织生产经营需求，对一般数据进行细化分级，本实践指南6.3给出了一般数据分级的参考规则。

核心数据、重要数据的识别和划分，按照国家和行业的核心数据目录、重要数据目录执行，目录不明确时可参考有关规定或标准，本实践指南不对重要数据、核心数据的识别和划分进行阐释。

5 数据分类方法

5.1 数据分类流程

数据处理者进行数据分类时，应优先遵循国家、行业的数据分类要求，如果所在行业没有行业数据分类规则，也可从组织经营维度进行数据分类，数据分类流程如图 1 所示。

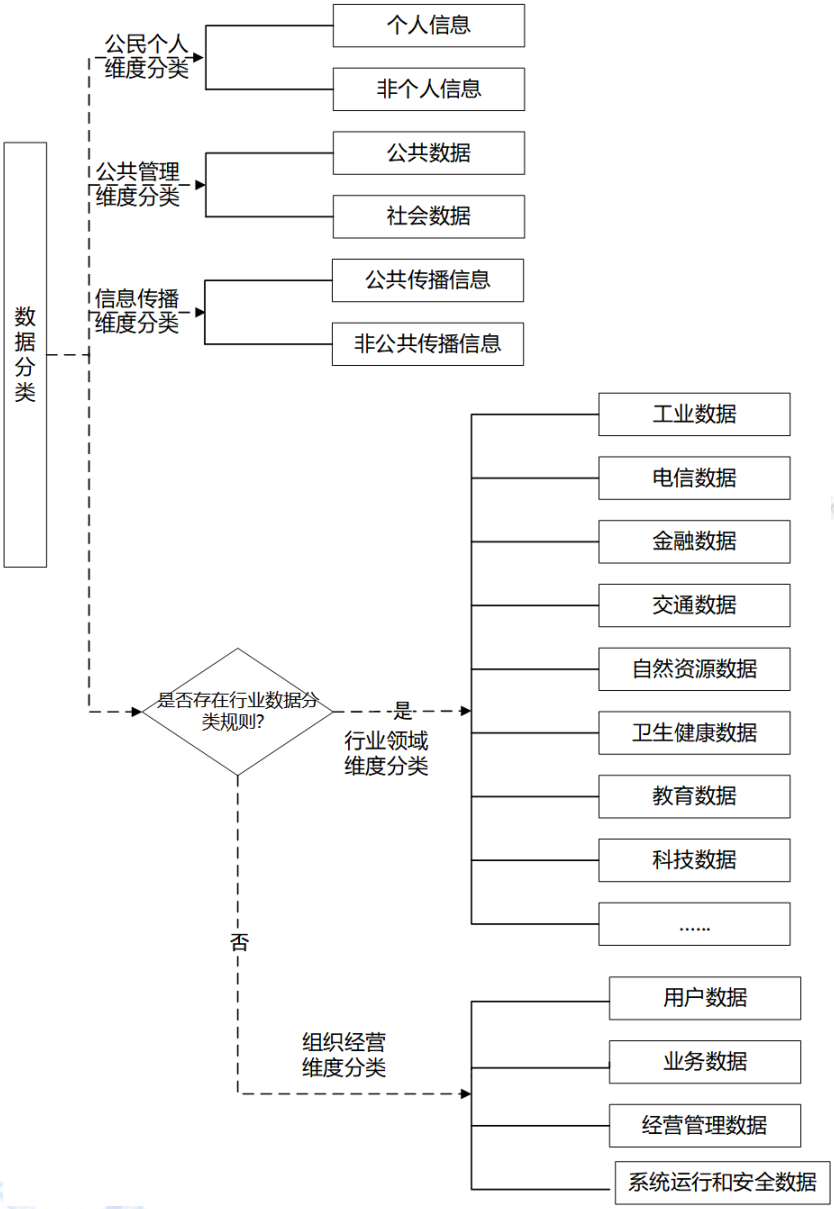

图 1 数据分类流程

具体数据分类步骤包括:

a）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，并对识别的数据类别进行区分标识，包括但不限于:

1) 从公共个人维度识别是否存在个人信息，个人信息识别见5.2.1;

2) 从公共管理维度识别是否存在公共数据，公共数据识别见5.3.1;

3) 从信息传播维度识别是否存在公共传播信息，公共传播信息识别见 5.4.1。

b）从行业领域维度，确定待分类数据的数据处理活动涉及的行业领域。

1) 如果该行业领域存在行业主管部门认可或达成行业共识的行业数据分类规则，应按照行业数据分类规则对数据进行分类；

2) 如果该行业领域不存在行业数据分类规则，可从组织经营维度结合自身数据管理和使用需要对数据进行分类，参考示例见附录 A；

3) 如果数据处理涉及多个行业领域，建议分别按照各行业的数据分类规则对数据类别进行标识。

c）完成上述数据分类后，数据处理者可采用线分类法对类别进一步细分，其中个人信息分类见 5.2.2 和附录B.1，公共数据分类见 5.3.2，公共传播信息分类见 5.4.2，行业领域数据分类参考示例见附录 C。

5.2 个人信息识别与分类

5.2.1 个人信息识别

通过分析特定自然人与信息之间的关系，符合下述情形之一的信息，可判定为个人信息。

a）**可识别特定自然人：**即从信息到个人，依据信息本身的特殊性可识别出特定自然人，包括单独或结合其他信息识别出特定自然人。

按照个人信息标识特定自然人的程度，可分为直接标识信息、准标识信息。

直接标识信息，是指在特定环境下可单独唯一识别特定自然人的信息。特定环境即个人信息使用的具体场景，如在一个具体的学校，通过学号可以直接识别出一个具体的学生。常见的直接标识信息有：姓名、公民身份号码、护照号、驾照号、详细住址、电子邮件地址、移动电话号码、银行账户、社会保障号码、唯一设备识别码、车辆识别码、健康卡号码、病历号码、学号、IP 地址、网络账号等。

准标识信息，是指在特定环境下无法单独唯一标识特定自然人，但结合其他信息可以唯一标识特定自然人的信息。常见的准标识信息，如性别、出生日期或年龄、国籍、籍贯、民族、职业、婚姻状况、受教育水平、宗教信仰、收入状况等。

个人信息通过去标识化等处理后，如果达到无法识别特定自然人且不能复原的匿名化效果，那么处理后的信息不再属于个人信息。

b）**与特定自然人关联：**即从个人到信息，如已知特定自然人，由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、网页浏览记录等），可识别为个人信息。

5.2.2 个人信息分类

按照涉及的自然人特征，个人信息可分为个人基本资料、个人身份信息等 16 个类别，具体分类示例见附录 B.1。

a）个人基本资料：个人基本情况信息，如个人姓名、生日、年龄、性别、民族、国籍、籍贯等。

b）个人身份信息：个人身份标识和证明信息，如身份证、军官证、护照、驾驶证、工作证、出入证、社保卡等证件信息。

c）个人生物识别信息：个人生物特征识别原始信息和比对信息，如人脸、指纹、步态、声纹、基因、虹膜等生物识别信息。

d）网络身份标识信息：网络身份标识和账户相关资料信息，如用户账号、用户 ID、即时通信账号、头像、昵称、IP 地址等。

e）个人健康生理信息：个人医疗就诊和健康状况信息，包括病症、住院志等个人医疗信息，和身高、体温等个人健康状况信息。

f）个人教育工作信息：个人教育培训、工作求职信息，包括学历、学位等个人教育信息，及个人职业、工作单位等个人工作信息。

g）个人财产信息：个人实体和虚拟财产信息，包括银行卡号等金融账户信息，交易订单等个人交易信息，收入状况、房产信息、虚拟财产等个人资产信息，及借款信息、还款信息等个人借贷信息。

h）身份鉴别信息：用于鉴别用户身份的数据，如账户登录密码、银行卡密码、支付密码、账户查询密码、交易密码等。

i）个人通信信息：个人通信数据和内容，如通信记录，短信、彩信、话音、电子邮件、即时通信等通信内容等。

j）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、电子邮件地址列表等。

k）个人上网记录：个人在使用业务服务过程中的操作记录和行为数据，如网页浏览记录、软件使用记录、点击记录等。

l）个人设备信息：个人设备标识信息和应用安装信息，不包括设备型号、品牌、厂商、屏幕分辨率等设备基本信息。

m）个人位置信息：描述能精确或粗略定位到个人的地理位置数据，包括精确位置信息、粗略位置信息等。

n）个人标签信息：根据个人上网日志等各类个人信息构建的，用于对个人用户分类分析的描述信息，如兴趣爱好、App 偏好等。

o）个人运动信息：描述个人运动活动或状态的信息，如步数、运动时长等。

p）其他个人信息：作为上述个人信息的补充，如宗教、个人违法记录等。

5.3 公共数据识别与分类

5.3.1 公共数据识别

符合以下任一情形的数据，可识别为公共数据。

a）各级政务机关在依法履行公共管理和服务职能过程中收集和产生的数据；

b）具有公共管理和服务职能的企事业单位和社会团体，在依法履行公共管理和服务职能过程中收集和产生的数据；

c）提供公共服务的组织，在开展公共服务（如供水、供电、供热、供气、教育、医疗、公共交通、通信、邮政、养老、环保等）过程中收集和产生的数据；

d）在为国家机关提供服务，参与公共基础设施、公共服务系统建设运维管理，利用公共资源提供服务过程中收集、产生的数据。

5.3.2 公共数据分类

公共数据分类，可参考以下规则实施:

a）政务数据的分类，优先按照国家或当地的电子政务信息目录进行分类，也可参考 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》等相关电子政务国家标准执行;

b）如存在公共数据目录，按照公共数据目录规则进行分类;

c）如不存在公共数据目录，公共数据可按照主题、部门或行业领域进行分类，也可从数据共享、开放角度进行分类。

注：公共数据从共享、开放角度，可分成无条件共享/开放数据、有条件共享/开放数据、禁止共享/开放数据。

5.4 公共传播信息识别与分类

5.4.1 公共传播信息识别

公共传播信息可通过判断信息是否具有公共传播属性进行识别，公共传播属性可参考以下任一原则判断:

a）已合法公开的信息;

b）以广泛传播为目的发布，接收者不特定;

c）在传播过程中事实上被广泛传播的信息;

d）即时通信服务平台的非个人通信信息，按照公共传播信息有关规定进行管理。

5.4.2 公共传播信息分类

公共传播信息分类，从信息传播类型角度可分为以下类别:

a）公开发布信息;

b）可转发信息;

c）无明确接收人信息。

6 数据分级方法

6.1 分级要素

数据分级主要从数据安全保护的角度，考虑影响对象、影响程度两个要素进行分级。

a）**影响对象：**是指数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后受到危害影响的对象，包括国家安全、公共利益、个人合法权益、组织合法权益四个对象。

b）**影响程度：**是指数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后，所造成的危害影响大小。危害程度从低到高可分为轻微危害、一般危害、严重危害。表 3 给出了针对各个危害对象的危害程度描述。

表3 影响对象的影响程度描述

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

影响对象	影响程度	参考说明
国家安全	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
公共利益	严重危害	波及到一个或多个省市的大部分地区，引起社会动荡，对经济建设有极其恶劣的负面影响
	一般危害	波及到一个或多个地市的大部分地区引起社会恐慌，对经济建设有重大的负面影响
	轻微危害	波及到一个地市或地市以下的部分地区，扰乱社会秩序，对经济建设有一定的负面影响
	无危害	对公共利益不造成影响
个人合法权益	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，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
	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。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。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，或仅造成微弱影响但可忽略不计
组织合法权益	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

6.2 基本分级规则

本实践指南 4.2 的数据分级框架给出了数据分级基本框架，将数据从低到高分成一般数据、重要数据、核心数据三个级别。各级别与影响对象、影响程度的对应关系如表 4 所示。

表4 数据安全基本分级规则

基本级别	影响对象			
	国家安全	公共利益	个人合法权益	组织合法权益
核心数据	一般危害、严重危害	严重危害	—	—
重要数据	轻微危害	一般危害、轻微危害	—	—
一般数据	无危害	无危害	无危害、轻微危害、一般危害、严重危害	无危害、轻微危害、一般危害、严重危害

6.3 一般数据分级规则

按照数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，对个人、组织合法权益造成的危害程度，将一般数据从低到高分为 **1 级、2 级、3 级、4 级共四个级别**，具体分级规则见表 5:

a）1 级数据：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，不会对个人合法权益、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：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成轻微危害。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：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成一般危害。3 级数据仅能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：数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对个人合法权益、组织合法权益造成严重危害，但不会危害国家安全或公共利益。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。

表5 一般数据分级规则

安全级别	影响对象	
	个人合法权益	组织合法权益
4 级数据	严重危害	严重危害
3 级数据	一般危害	一般危害
2 级数据	轻微危害	轻微危害
1 级数据	无危害	无危害

6.4 定级方法

6.4.1 定级流程

数据处理者按照基本分级框架（见4.2、6.2）和一般数据分级规则（见6.3）对数据进行定级时，可参考如图2所示流程实施。

数据定级的具体步骤包括：

a）按照国家和行业领域的核心数据目录、重要数据目录，依次判定是否核心数据、重要数据，如是则按照就高从严原则定为核心数据级、重要数据级，其他数据定为一般数据；

b）国家和行业核心数据、重要数据目录不明确时，可参考核心数据、重要数据认定的规定或标准，分析数据一旦遭到篡改、破坏、

泄露或者非法获取、非法利用的危害对象和危害程度，参照 6.2 的表 4 进行基本定级，确定核心数据、重要数据和一般数据级别；

c）按照 6.3 一般数据分级规则或者所属行业共识的数据分级规则对一般数据进行定级，确定一般数据细分级别。部分行业领域与本实践指南的分级对应关系如附录 B.4 所示。

d）如果数据属于个人信息，应识别敏感个人信息、一般个人信息，按照 6.4.2 对个人信息进行定级。

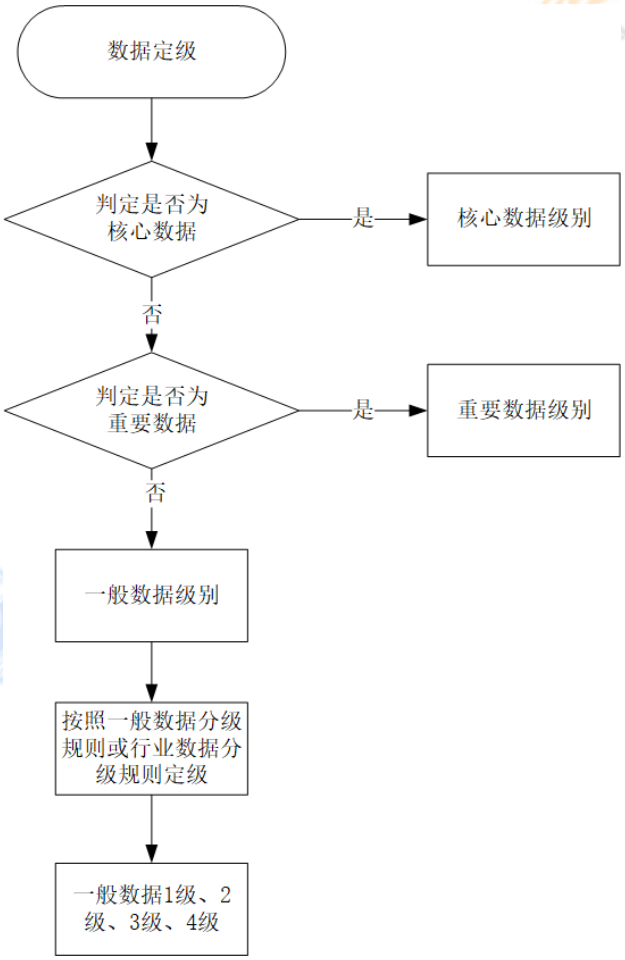

图2 数据定级流程

以上定级方法主要针对数据项，如针对数据集定级，建议在确定数据集中数据项级别的基础上，按照就高从严原则确定数据集的级别。

6.4.2 个人信息定级

根据《中华人民共和国个人信息保护法》要求，按照个人信息一旦泄露或者非法使用，对个人合法权益造成的危害程度，个人信息可分为一般个人信息、敏感个人信息。一般个人信息是指一旦泄露或者非法使用，对自然人个人信息权益造成轻微或一般影响，不易导致自然人的人格尊严、人身安全、财产安全受到侵害，例如网络身份标识信息。敏感个人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。附录 B.2 给出了可能属于敏感个人信息的参考示例。

个人信息定级，可优先判定是否属于敏感个人信息，如果属于敏感个人信息，则定为一般数据 4 级。如果属于一般个人信息，则按照一般数据分级规则，分析影响程度确定属于哪个级别。

其中，敏感个人信息判定，可通过分析个人信息遭到泄露或者非法利用对个人信息主体权益可能造成的影响，符合以下任一影响的可判定为敏感个人信息：

a）个人信息遭到泄露或者非法使用，可能直接侵害个人信息主体的人格尊严。例如，特定身份、医疗健康、犯罪记录等信息属于一旦泄露即侵害人格尊严的敏感个人信息。

b）个人信息遭到泄露或者非法使用，不会直接侵害个人信息主体的人格尊严，但可能由于社会偏见、歧视性待遇而间接侵害个人信

息主体的人格尊严。例如因个人种族、宗教信仰、性取向遭到歧视性待遇。

c）个人信息遭到泄露或者非法使用，可能直接或间接危害个人信息主体的人身、财产安全。例如，泄露、非法使用家庭住址、家属关系等家庭相关信息，可能会为入室抢劫或绑架等犯罪所利用；个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡等。

6.4.2 最低参考级别

特定类型一般数据的最低参考级别如下：

a）敏感个人信息不低于 4 级，一般个人信息不低于 2 级；

b）组织内部员工个人信息不低于 2 级；

c）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。

6.4.3 衍生数据定级

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 6。

表 6 数据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	对数据（如个人信息）按照脱敏规则进行数据变形处理后的新数据。	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

数据类别	类别定义	数据示例
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	即群体性综合性数据，是由多个用户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	对不同业务目的或地域的数据汇聚，进行挖掘或聚合	如多个业务、多个地市的数据整合、汇聚等

原始数据可按照上文介绍的方法进行定级，衍生数据级别原则上依据就高从严原则，对照加工的原始数据集级别进行定级，同时按照数据加工程度也可进行升级或降级调整。

a）脱敏数据级别可比原始数据集级别降低，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。

b）标签数据级别可比原始数据集级别降低，个人标签信息不低于 2 级。

c）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。

d）融合数据级别要考虑数据汇聚融合结果，如果结果数据汇聚了更多的原始数据或挖掘出更敏感的数据，级别需要升高，但如果结果数据降低了标识化程度等，级别可以降低。

6.5 重新定级

6.5.1 重新定级情形

数据安全定级完成后，出现下列情形之一时，应重新定级:

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）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；

g）需要对数据安全级别进行变更的其他情形。

6.5.2 数据变化的定级参考

数据发生变化导致安全级别变化的规则（见表 7），包括但不限于：

表 7 数据安全级别变化示例

措施或情形	安全级别变化
数据体量增加到特定规模导致社会重大影响	升级
达到国家有关部门规定精度的数据	升级
关联多个业务部门数据	升级
大量多维数据进行关联	升级
发生特定事件导致数据敏感性增强	升级
数据已被公开或披露	降级
数据进行脱敏或删除关键字段	降级
数据进行去标识化、假名化、匿名化	降级
数据发生特定事件导致数据失去敏感性	降级

注：处理100万人以上个人信息的数据处理者，按照重要数据处理者进行管理，应满足重要数据保护要求。

7 数据分类分级实施流程

数据处理者在开展数据分类分级时，可按照图 3 所示流程实施，具体步骤包括:

图 3 数据分类分级实施流程

a）数据资产梳理：对组织的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：参考 4.1 和第 5 章从多个维度，建立自身的数据分类规则，参考 5.1 的数据分类流程对数据进行分类。

c）数据分级：参考 4.2 和第 6 章建立自身的数据分级规则，按照 6.4 对数据进行定级。

d）审核标识管理：对数据资产分类分级结果进行评审和完善，最后批准发布实施，形成数据资产分类分级清单。并对数据资产和数据分类分级进行维护、管理和定期审核。重新定级情形可参考 6.5。

e）数据分类分级保护：依据国家给出的关于核心数据、重要数据、个人信息、公共数据等安全要求，以及行业领域给出的数据分类分级保护要求，建立数据分类分级保护策略，按照核心数据严格管理、重要数据重点保护、个人信息安全合规和一般数据分级保护的思路，对数据实施全流程分类分级管理和保护。

附录 A 组织经营维度数据分类参考示例

表 A.1 按照组织经营维度，将组织数据分为用户数据、业务数据、经营管理数据、系统运行和安全数据。

表A.1 组织经营维度的数据分类参考示例

数据类别	类别定义	示例
用户数据	组织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	组织在业务生产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	组织在机构经营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 个人信息分类示例

B.1 个人信息分类示例

表 B.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、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

一级类别	二级类别	典型示例和说明
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。
	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、

一级类别	二级类别	典型示例和说明
		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，包括行踪轨迹、经纬度、住宿信息、小区代码、基站号、基站经纬度坐标等
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。

B.2 敏感个人信息分类示例

表B.2给出了可能构成敏感个人信息的示例。

表B.2 敏感个人信息参考示例

类别	典型示例和说明
特定身份	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
生物识别信息	个人基因、指纹、声纹、掌纹、眼纹、耳廓、虹膜、面部识别特征、步态等
金融账户	金融账户及金融账户相关信息，包括但不限于支付账号、银行卡磁道数据（或芯片等效信息）、证券账户、基金账户、保险账户、其他财富账户、公积金账户、公积金联名账号、账户开立时间、开户机构、账户余额以及基于上述信息产生的支付标记信息等
医疗健康	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、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、传染病史等
行踪轨迹	基于实时地理位置形成的个人行踪和行程信息，例如实时精准定位信息、GPS 车辆轨迹信息、出入境记录、住宿信息（定位到街道、小区甚至更精确位置的数据）等
未成年人个人信息	14 岁以下（含）未成年人的个人信息
身份鉴别信息	用于验证主体是否具有访问或使用权限的信息，包括但不限于登录密码、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）、口令、动态口令、口令保护答案、短信验证码、密码提示问题答案、随机令牌等
其他敏感个人信息	种族、性取向、婚史、宗教信仰、未公开的违法犯罪记录等

B.3 私密个人信息识别参考

按照个人信息的私密程度，个人信息也可分成私密个人信息、非私密个人信息。私密个人信息，是个人信息中不愿为他人知晓的个人隐私信息。

私密个人信息的判定，需要同时满足“秘密性”和“私人性”两个条件:

a）该信息为私人所享有，信息主体有权决定是否对该信息进行公开;

b）从社会公众的一般认知和价值认识综合权衡，该信息一旦泄露，会侵害个人的隐私权，但通常不会危害他人及公共利益。

在考虑场景的前提下，常见的私密个人信息有: 身体缺陷、女性三围、心理特征、个人感情生活、性取向、未公开的违法犯罪记录、个人身体私密部位信息、个人私密录音等。

附录 C 部分行业数据分类分级参考示例

C.1 工业数据分类参考

《工业数据分类分级指南（试行）》（工信厅信发〔2020〕6 号）是由工业和信息化部于 2020 年 2 月发布，提出了工业数据分类分级的方法以及分级管理要求，适用于工业和信息化主管部门、工业企业、平台企业等开展工业数据分类分级工作。

《工业数据分类分级指南（试行）》中定义的工业数据是工业领域产品和服务全生命周期产生和应用的数据，包括但不限于工业企业在研发设计、生产制造、经营管理、运维服务等环节中生成和使用的数据，以及工业互联网平台企业（以下简称平台企业）在设备接入、平台运行、工业 App 应用等过程中生成和使用的数据。工业数据的分类示例如表 C.1 所示。

表C.1 工业数据分类参考示例

一级子类	二级子类	三级子类
工业企业工业数据	研发数据域	研发设计数据
		开发测试数据
	生产数据域	控制信息
		工况状态
		工艺参数
		系统日志
	运维数据域	物流数据
		产品售后服务数据
	管理数据域	系统设备资产信息
		客户与产品信息
		产品供应链数据
		业务统计数据
	外部数据域	与其他主体共享的数据

一级子类	二级子类	三级子类
平台企业工业数据	平台运营数据域	物联采集数据
		知识库模型库数据
		研发数据
	企业管理数据域	客户数据
		业务合作数据
		人事财务数据

C.2 电信数据分类参考

YD/T 3813—2020《基础电信企业数据分类分级方法》提出了基础电信企业数据分类分级的原则，明确了分类分级方法和工作流程，并给出了基础电信企业数据的分类分级示例。

《基础电信企业数据分类分级方法》所规定的数据范围包括基础电信企业生产经营和管理活动中产生、采集、加工、使用和管理的网络数据和非网络数据。根据基础电信企业业务运营管理和数据安全管理特点，将企业数据分为用户相关数据和企业自身相关数据两大类，表 C.2 给出了这两大类数据的详细分类示例。

表C.2 基础电信企业数据分类参考示例

一级子类	二级子类	三级子类	四级类别
用户相关数据	用户身份相关数据	用户身份相关数据	自然人身份标识、网络身份标识、用户基本资料、实体身份证明、用户私密资料
	用户服务内容数据	服务内容和资料数据	服务内容数据、联系人信息
	用户服务衍生数据	用户服务使用数据	业务订购关系、服务记录和日志、消费信息和账单、位置数据、违规记录数据
		设备信息	终端设备标识、终端设备资料
	用户统计分析类数据	用户使用习惯和行为分析数据	

一级子类	二级子类	三级子类	四级类别
		用户上网行为相关统计分析数据	
企业自身相关数据	网络与系统的建设与运行维护类数据	规划建设类数据（分发布前后）	网络规划类、投资计划类、项目管理类
		网络与系统资源类数据	公共资源类数据、传输资源类数据、承载网资源、核心网资源、接入网资源、IT 系统资源、云资源
		网络与系统运维类数据	信令、路由信息、网段、网址、VLAN 划分、设备监测、告警、信令监测、流量监测、运维日志、运维系统账号密码等、系统运行状况统计分析
		网络安全管理类数据	安全审计记录、网络安全应急预案、违法有害信息监测、核心区域监控、网络威胁数据
	业务运营类数据	业务运营服务数据	产品信息、渠道信息、客户服务信息、营销信息
		公开业务运营服务数据	
	企业管理数据	发展战略与重大决策	发展战略、重大决策与重要会议
		业务发展类	市场策略、营销管理、资费管理、产品发展策略
		技术研发类	技术管理、技术研究报告、专利工作
		运行管理类	
		生产经营类	财务预算、业绩披露、考核相关信息、生产经营数据
		综合管理类	人力资源、财务信息、办公自动化、采购
	其他数据	合作方提供数据	

C.3 金融数据分类参考

金融行业中，以 JR/T 0171—2020《个人金融信息保护技术规范》、JR/T 0197—2020《金融数据安全 数据安全分级指南》和 JR/T 0158—2018《证券期货业数据分类分级指引》三个行业标准对金融数据分类分级给出了具体指导。

JR/T 0171—2020《个人金融信息保护技术规范》中规定的个人金融信息是指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。个人金融信息的分类分级可以参考该标准提出的方法执行。标准同时给出了个人金融信息生命周期技术要求和管理要求。

JR/T 0158—2018《证券期货业数据分类分级指引》中针对证券期货行业经营和管理活动中产生、采集、加工、使用或管理的网络数据或非网络数据提出了分类分级的原则、方法和流程，并给出了 6 种行业内典型机构的数据分类分级模板。

JR/T 0197—2020《金融数据安全 数据安全分级指南》是在 JR/T 0171—2020 和 JR/T 0158—2018 基础上的进一步拓展，将数据分类分级的范围扩大至金融数据。该标准中定义的金融数据是金融业机构开展金融业务、提供金融服务以及日常经营管理所需或产生的各类数据。标准内容包括金融数据的定级原则、定级要素、定级规则和定级流程，并在附录中提出了金融数据安全的分类示例，如表 C.3 所示。

表C.3 金融数据分类参考示例

一级子类	二级子类	三级子类
客户	个人	个人自然信息、个人身份鉴别信息、个人资讯信息、个人关系信息、个人行为信息、个人标签信息
	单位	单位基本信息、单位身份鉴别信息、单位资讯信息、单位关系信息、单位行为信息、单位标签信息
业务	账户信息	账户信息
	法定数字货币钱包信息	基本信息
	合约协议	合同通用信息、存款业务信息、贷款业务信息、中间业务信息、资金业务信息、投资理财业务信息、信用卡业务信息、非银行支付业务信息、商户签约信息、保险业务信息、再保险业务信息、信托业务信息、金融资产管理公司业务信息
	金融监管和服务	反洗钱业务信息、国库业务信息、货币金银业务信息、存款保险业务信息、身份核查业务信息、征信管理业务信息、非银行支付机构非现场监管业务信息、支付结算业务信息、LEI 管理业务信息、机构管理业务信息、再贷款业务信息、利率报备业务信息、房地产监测分析业务信息、舆情监测业务信息、行政预审批业务信息、跨境收付业务信息、金融消费权益保护业务信息、金融稳定分析业务信息
	交易信息	交易通用信息、保险收付费信息
经营管理	营销服务	产品信息、渠道信息、营销信息
	运营管理	安防管理信息、业务运维信息、客户服务信息、单证管理信息、合作单位信息、音影像信息
	风险管理信息	风险偏好信息、风险管控信息
	技术管理	项目管理信息、系统管理信息
	综合管理	战略规划信息、招聘信息、员工信息、机构信息、财务信息、资产负债信息、行政信息、内控合规信息
监管	数据报送	监管报送信息
	数据收取	评级、处罚与违规信息、监管统计及预警信息、外部审计信息

C.4 部分行业数据分级对应关系参考

工业、电信、金融行业的数据分级规则，与本实践指南提出的基本分级框架（见 4.2、6.2）和一般数据分级规则（见 6.3）的对应关系参考说明，如表 C.4 所示。

表C.4 部分行业数据分级对应关系参考

行业领域	规则来源	行业数据分级	对应的本指南数据分级
工业	《工业数据分类分级指南（试行）》	工业数据三级	核心数据级
		工业数据二级	重要数据级
		工业数据一级	一般数据级
电信	YD/T 3813—2020《基础电信企业数据分类分级方法》	第一级	一般数据 1 级
		第二级	一般数据 2 级
		第三级	一般数据 3 级
		第四级	一般数据 4 级
	YD/T 3867—2021《基础电信企业重要数据识别指南》	重要数据	重要数据级
金融	JR/T 0197—2020《金融数据安全 数据安全分级指南》	5 级	重要数据级
		4 级	一般数据 4 级
		3 级	一般数据 3 级
		2 级	一般数据 2 级
		1 级	一般数据 1 级
	JR/T 0171—2020《个人金融信息保护技术规范》	C3	一般数据 4 级
		C2	一般数据 3 级、4 级
		C1	一般数据 1 级、2 级

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] 《网络数据安全管理条例（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》