TC260-PG-20212A

网络安全标准实践指南

—数据分类分级指引

（征求意见稿-v1.0-202109）

全国信息安全标准化技术委员会秘书处

2021 年 9 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。

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、中国电信股份有限公司、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，从国家数据安全管理视角对数据分类分级进行了研究，给出了数据分类分级的原则、框架和规则，可为主管监管部门、数据处理者开展数据分类分级保护工作提供参考。

目　录

1 范围

本实践指南从国家数据安全管理视角，给出了数据分类分级的原则、框架和规则。

本实践指南适用于数据处理者开展数据分类分级保护活动，也可为主管监管部门进行数据分类分级保护管理和监督提供参考。

涉及国家秘密的数据，应遵守保密法律法规的规定，不适用本实践指南。

2 术语定义

2.1 数据

任何以电子或者其他方式对信息的记录。

注1：网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

注2：数据资产，通常包括数据库表、数据文件、数据集、数据项等。数据集是对数据库表、数据文件等进行筛选形成的数据集合，数据项是数据库表的某一列字段，。

2.2 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。

2.3 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，如影响国家安全或公共利益，则可能属于重要数据。

2.4 国家核心数据

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。

2.5 公共数据

公共管理和服务机构在依法履行公共管理和服务职责过程中收集、产生的数据，及其他组织和个人在提供公共服务中收集、产生的涉及公共利益的数据。

注：公共管理和服务机构，通常包括各级党政机关、具有公共管理和服务职能的企事业单位。

2.6 法人数据

组织在生产经营和内部管理过程中收集和产生的数据。

2.7 衍生数据

原始数据经过计算、统计、关联、挖掘或聚合等加工活动而产生的数据。

注：根据数据的加工程度，可将衍生数据分为脱敏数据、标签数据、统计数据、关联数据等。

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：数据分类分级应满足相关法律法规及主管监管部门有关规定要求，优先识别法律法规中规定的数据类别或级别，如识别是否包含国家核心数据、重要数据、个人信息、公共数据。

b）界限明确原则：数据分类分级的各类别、各级别界限明确，每个数据项原则上只属于一个类别、一个级别。

c）就高从严原则：采取就高从严原则对数据进行分类分级，主要表现在：

1) 如果数据集包含多个级别的数据项，应按照数据项的最高级别对数据集进行定级。

2) 数据分类时按照个人信息、公共数据、法人数据的优先次序依次识别，采取就高从严原则对数据进行分类:

- 当数据既属于个人信息又属于公共数据或法人数据时，识别为个人信息;
- 当数据既属于公共数据又属于法人数据时，识别为公共数据。

3) 数据定级时优先识别是否涉及国家核心数据、重要数据，如涉及应按照国家核心数据级别、重要数据级别进行定级。

d) 时效性原则：数据的类别级别可能因时间变化、政策环境变化、安全事件发生或不同业务场景的敏感性变化而发生改变，因此需要对数据分类分级进行定期审核并及时调整。

e) 自主性原则：在国家数据分类分级规则的框架下，根据自身数据管理需要，行业、领域、地方或组织自主细化确定所管辖数据的类目设置和层级划分。

4 数据分类分级框架

本实践指南从国家数据安全管理视角，提出数据分类分级框架，如图 1 所示。

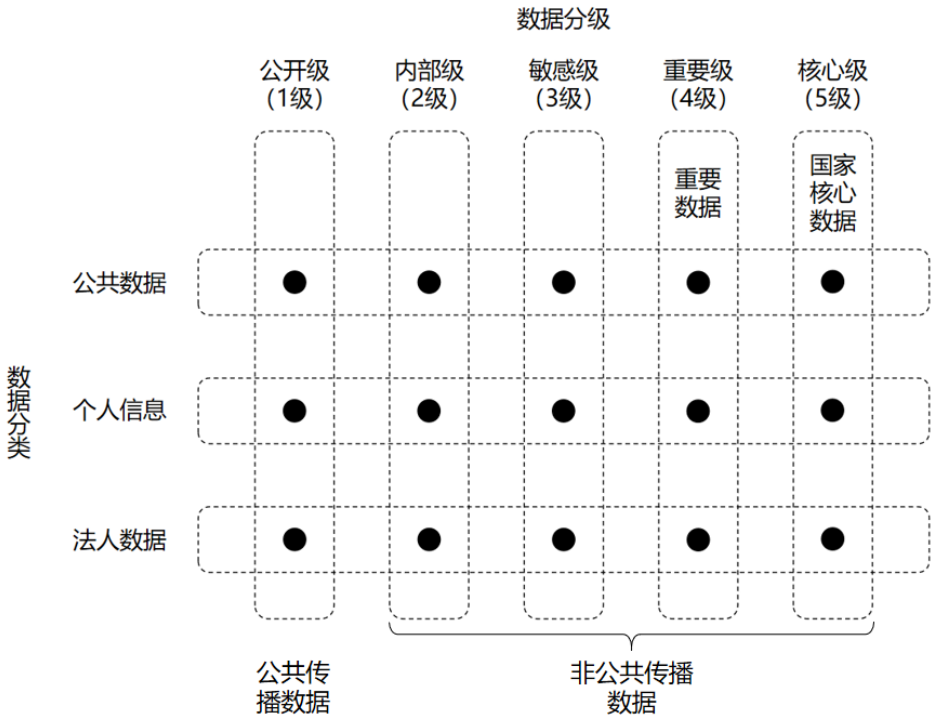

图 1 数据分类分级框架

a）数据分类

从数据主体角度，将数据分为**公共数据、个人信息、法人数据三个类别**，如表 1 所示：

表 1 数据主体视角的数据分类参考

数据分类	类别定义	示例
公共数据	公共管理和服务机构在依法履行公共管理和服务职责过程中收集、产生的数据，及其他组织和个人在提供公共服务中收集、产生的涉及公共利益的数据	如政务数据，及提供供水、供电、供气、供热、公共交通、养老、教育、医疗健康、邮政等公共服务中涉及公共利益的数据等
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，不包括匿名化处理后的信息	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
法人数据	组织在生产经营和内部管理过程中，收集和产生的数据	如业务数据、经营管理数据、系统运行和安全数据等

b）数据分级

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**公开级（1 级）、内部级（2 级）、敏感级（3 级）、重要级（4 级）、核心级（5 级）五个级别**。其中，**重要数据属于重要级（4 级），国家核心数据属于核心级（5 级）**。

表 2 数据分级规则参考示例

数据分级	传播范围	级别定义
公开级（1 级）	公开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	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，但不会危害国家安全、公共利益
内部级（2 级）	内部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	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，或者对公共利益造成轻微危害，但不会危害国家安全
敏感级（3 级）	敏感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	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，或者对公共利益造成一般危害，但不会危害国家安全
重要级（4 级）	重要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	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、组织合法权益造成特别严重危害，可能对公共利益造成严重危害，或者对国家安全造成轻微或一般危害
核心级（5 级）	核心级数据禁止对外共享或传播	数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对国家安全造成严重或特别严重危害，或对公共利益造成特别严重危害

此外，从数据传播视角，也可将数据分为公共传播数据和非公共传播数据。**公共传播数据**是指具有公共传播属性，可对外公开发布、转发传播的数据。公开级数据属于公共传播数据。**非公共传播数据**，是指不具有公共传播属性，仅在授权的限定范围传播或禁止进行传播的数据，如国家秘密、重要数据、商业秘密、个人信息、

有条件或禁止共享开放的公共数据、未经同意的知识产权作品等。内部级、敏感级、重要级、核心级数据均属于非公共传播数据。

5 数据分类规则

5.1 个人信息识别与分类

5.1.1 个人信息识别

判定某项信息是否属于个人信息，可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，可识别为个人信息。

a）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。按照个人信息标识个人的程度，可分为直接标识信息，准标识信息、非标识信息。直接标识信息、准标识信息均属于个人信息。

直接标识信息是指在特定环境下可以单独唯一识别特定自然人的信息。特定环境指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、电子邮件地址、移动电话号码、银行卡号码、车辆识别号码、社会保险号码、唯一设备识别码等。

准标识信息，是指在特定环境下无法单独唯一识别特定自然人，但结合其他信息可以唯一识别特定自然人的信息。常见的准标识信息有：性别、出生日期或年龄、事件日期（例如入院、手术、出院、访问）及地点、职业、婚姻状况、受教育水平、宗教信仰等。

可标识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，那么加工后的信息不再属于个人信息。

b）特定自然人关联信息

即从个人到信息，如已知特定自然人，该自然人的一些固有属性特征（如民族、个人生物识别信息等），以及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），均可识别为个人信息。

5.1.2 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、个人身份信息等多个类别，见附录 A.1。按照个人信息的敏感程度，可分为一般个人信息与敏感个人信息。按照个人信息的私密程度，可分成一般个人信息、私密个人信息。

a）一般个人信息

一般个人信息，是一旦泄露或者非法使用，对自然人个人信息权益造成轻微影响，不易导致自然人的人格尊严受到侵害，或危害自然人人身、财产安全，例如网络身份标识信息。

b）敏感个人信息

敏感个人信息，是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。敏感个人信息分类和示例参

见附录A.2。

判定个人信息是否属于敏感个人信息时，可关注以下三点：

1) 泄露、非法使用信息本身是否会直接侵害信息主体的人格尊严。例如，特定身份、医疗健康、性取向信息、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。
2) 泄露、非法使用信息本身不会直接侵害人格尊严，但由于社会偏见、歧视性待遇而间接侵害自然人的人格尊严以及人身、财产安全。例如，将个人健康生理信息用于保险公司营销和确定个体保费高低；利用个人教育信息推断出学生家庭背景。
3) 泄露、非法使用信息本身不会直接造成危害，但由于被泄露、非法使用进而危害信息主体的人身、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。

c）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。判断私密个人信息的标准为“秘密性”和“私人性”。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。

私密个人信息的判定需要同时满足以下两个条件:

1) 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。

2) 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。

5.2 公共数据识别与分类

5.2.1 公共数据识别

公共数据识别，可优先按照国家、地方制定的电子政务信息目录和公共数据目录进行识别，在相关目录不明确时，可按照数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用，是否可能危害公共利益的角度进行识别，包括但不限于:

a）各级党政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，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）受公共管理和服务机构委托或授权提供公共服务（如水电燃气、公共交通、邮政、教育等）的企业、社团等其他组织，在开展公共服务过程中收集和产生的数据。

d）其他可能影响公共利益的数据，例如:

- 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;

- 影响公共场所的活动秩序、公共交通秩序;
- 影响公共卫生事件;
- 影响公共网络空间秩序;
- 影响人民群众的生活秩序;
- 影响社会成员使用公共设施;
- 影响社会成员获取公开数据资源;
- 影响社会成员接受公共服务;
- 其他影响公共利益的情形。

5.2.2 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，按照公共数据目录进行分类。

c) 如不存在公共数据目录，公共数据可按照服务行业领域进行分类，也可从公共数据开放程度和条件的角度进行分类。

5.3 法人数据识别与分类

5.3.1 法人数据识别

法人数据数据识别，可参考以下原则:

a) 不属于个人信息、公共数据的数据，可识别为法人数据。

b) 法人数据仅用于组织的业务生产、经营管理及信息系统管理，不包括客户的个人信息。

c) 公共管理和服务机构在依法开展公共管理和服务的生产经营活动中收集和产生的数据属于公共数据，不属于法人数据。

d) 在开展公共服务生产经营过程中，收集和产生的涉及公共利益的数据属于公共数据，不属于法人数据。

5.3.2 法人数据分类

法人数据可分为业务数据、经营管理数据、系统运行和安全数据三类。

a) 业务数据

业务数据，是组织在开展业务生产经营过程中收集和产生的数据。业务数据分类，可按照业务所属行业领域的数据分类分级要求，结合自身实际业务运营需要进行细化分类。

b) 经营管理数据

经营管理数据，是组织进行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、经营信息等。

c) 系统运行和安全数据

系统运行和安全数据，是指网络、系统、应用及网络安全数据，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。

6 数据分级规则

6.1 定级要素

数据定级时，需要考虑危害对象、危害程度两个要素。

a）危害对象

危害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）危害程度

危害程度是数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用后，所造成的危害的大小。危害程度从低到高可分为轻微危害、一般危害、严重危害、特别严重危害。

6.2 定级方法

对数据资产进行定级，可参考以下方法步骤:

a）识别是否涉及国家核心数据，如涉及定为核心级（5级）。

b）识别是否涉及重要数据，如存在则将数据资产定为重要级（4级），重要数据识别可按照行业领域的重要数据目录进行判定，如果在相关行业领域重要数据目录不明确时可参考相关国家标准进行判定。

c）个人信息和公共数据的定级符合6.3要求。

d）不涉及国家核心数据、重要数据的数据，需要识别危害主体，分析危害程度，按照表3的数据分级规则综合判定数据级别。

表3 数据定级规则参考

最低级别	危害对象	危害程度	一般特征
5 级	国家安全	严重危害、特别严重危害	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、国民经济命脉、重要民生、重大公共利益
5 级	公共利益	特别严重危害	
4 级	国家安全	轻微危害、一般危害	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
4 级	公共利益	严重危害	
4 级	个人合法权益	特别严重危害	
4 级	组织合法权益	特别严重危害	
3 级	公共利益	一般危害	一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能对公共利益造成一般危害，或对个人、组织合法权益造成严重危害，但不会危害国家安全
3 级	个人合法权益	严重危害	
3 级	组织合法权益	严重危害	
2 级	公共利益	轻微危害	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、组织合法权益造成一般危害，或对公共利益造成轻微危害，但不会危害国家安全
2 级	个人合法权益	一般危害	
2 级	组织合法权益	一般危害	
1 级	个人合法权益	轻微危害	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、组织合法权益造成轻微危害，但不会危害国家安全、公共利益
1 级	组织合法权益	轻微危害	

6.3 特定数据最低安全级别

国家核心数据、重要数据、个人信息、公共数据等特定数据的最低安全级别，可设置如下:

a）国家核心数据的级别不低于 5 级;

b）重要数据的级别不低于 4 级;

c）敏感个人信息不低于 4 级，一般个人信息不低于 3 级，组织内部员工个人信息不低于 2 级，个人标签信息不低于 2 级;

d）有条件开放的公共数据级别不低于 2 级，禁止开放的公共数据不低于 4 级。

6.4 重新定级的情形

数据安全定级完成后，出现下列情形之一时，应重新进行定级:

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。

附录 A 个人信息分类示例

A.1 个人信息分类示例

表 A.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A.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	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	个人身份信息	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
个人生物识别信息	个人生物识别信息	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
网络身份标识信息	网络身份标识信息	个人信息主体账号、IP 地址、Wi-Fi 列表、个人数字证书等
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、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、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
个人教育工作信息	个人教育信息	学历、学位、教育经历、成绩单等
	个人工作信息	个人职业、职位、职称、工作单位、工作经历、培训记录等
个人财产信息	金融账户信息	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

一级类别	二级类别	典型示例和说明
	交易信息	个人信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、流水记录、透支记录、交易状态、交易日志、交易凭证、证券委托、成交、持仓信息、保单信息、理赔信息等
	资产信息	包括但不限于个人收入状况、拥有的不动产状况、拥有的车辆状况、虚拟货币、游戏类兑换码等虚拟财产信息
	借贷信息	借贷业务中产生的信息，包括但不限于信贷记录、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
个人通信信息	个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
联系人信息	联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	个人上网记录	指通过日志储存的个人信息主体操作记录，包括网页浏览记录、软件使用记录、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
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
	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
	精确位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等

一级类别	二级类别	典型示例和说明
个人画像信息	间接用户画像	使用来源于特定自然人以外的个人信息（如其所在群体的数据）形成的该自然人的特征模型
	直接画像信息	直接使用特定自然人的个人信息，形成的该自然人的特征模型
未成年人个人信息	未成年人个人信息	14 岁以下（含）未成年人的个人信息
其他信息	其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、个人运动信息等

A.2 敏感个人信息分类示例

表A.2给出了敏感个人信息的一级类别、二级类别和相关数据示例。

表A.2 敏感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
个人身份信息	个人身份信息	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
个人生物识别信息	个人生物识别信息	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
个人财产信息	金融账户信息	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
	交易信息	个人信息主体在交易过程中产生的各类信息，包括但不限于交易金额、支付记录、流水记录、透支记录、交易状态、交易日志、交易凭证、证券委托、成交、持仓信息、保单信息、理赔信息等
	资产信息	包括但不限于个人收入状况、拥有的不动产状况、拥有的车辆状况、虚拟货币、游戏类兑换码等虚拟财产信息
	借贷信息	借贷业务中产生的信息，包括但不限于信贷记录、征信信息、担保情况等

一级类别	二级类别	典型示例和说明
身份鉴别信息	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
个人健康生理信息	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、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
个人画像信息	直接画像信息	直接使用特定自然人的个人信息，形成的该自然人的特征模型
未成年人个人信息	未成年人个人信息	14 岁以下（含）未成年人的个人信息
个人位置信息	精确位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、网页浏览记录等

附录 B 数据分类分级流程

组织开展数据分类分级，可按照数据资产识别、数据分类确定、数据定级判定、审核标识管理、数据分类分级保护流程实施，如图 2 所示。具体步骤包括但不限于:

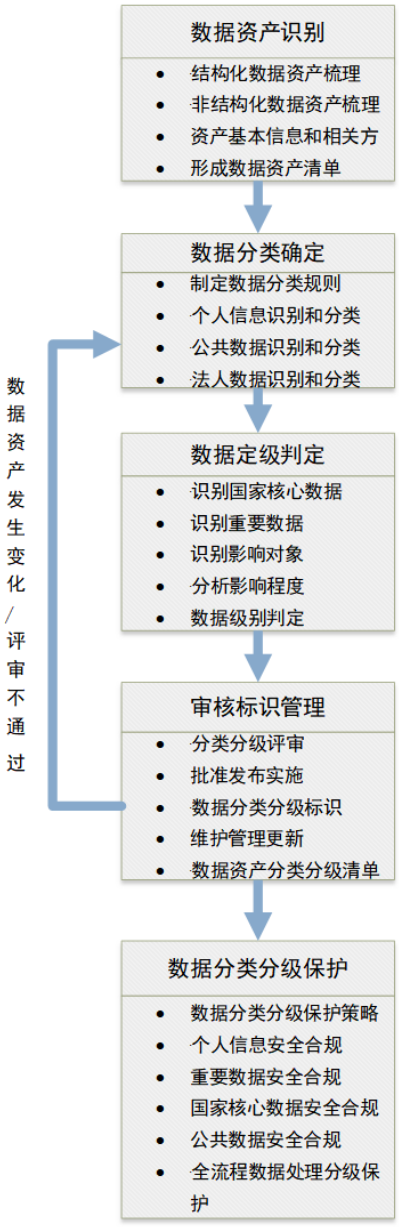

图 2 数据分类分级流程

a）数据资产识别

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）数据分类确定

按照国家和行业数据分类分级要求，结合组织自身实际需要，参考第5章对数据类别进行细分，制定适合组织现状的数据分类规则，形成至少包含一级类别、二级类别的数据分类树。将数据资产清单对应到数据分类树，确定数据资产清单中每个数据项在数据分类树的位置，即确定数据项所属的类别。

c）数据定级判定

按照国家和行业数据分类分级要求，参考第6章的数据定级方法，结合数据资产的颗粒度（如数据库表、数据项、数据文件、数据集等），识别数据资产一旦泄露、篡改、破坏等涉及的危害对象，分析可能造成的危害程度，同时综合考虑数据规模、时效性、数据加工程度等因素，判定数据资产的安全级别。

d）审核标识管理

组织的安全部门、业务部门、数据部门等相关方，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。同时对数据资产进行分类分级标识，并对数据资产和数据分类分级进行维护、管理和定期审核。

e）数据分类分级保护

针对数据资产分类分级结果，按照国家和行业数据分类分级保护要求，制定组织数据分类分级保护策略。国家核心数据、重要数

据、个人信息、公共数据等的数据安全，应符合相关安全合规要求。同时，针对数据安全级别建立覆盖数据收集、存储、传输、使用、加工、提供、公开、删除等全流程数据处理活动的分级保护措施。

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] GB/T 35273—2020 信息安全技术 个人信息安全规范

[4] GB/T 38667—2020 信息技术 大数据 数据分类指南

[5] GB/T 37973—2019 信息安全技术 大数据安全管理指南

[6] 信息安全技术 重要数据识别指南（征求意见稿）

[7] 中央企业商业秘密保护暂行规定

[8] YD/T 3867—2021 基础电信企业重要数据识别指南

[9] YD/T 3813—2020 基础电信企业数据分类分级方法

[10] JR/T 0171—2020 个人金融信息保护技术规范

[11] JR/T 0197—2020 金融数据安全 数据安全分级指南

[12] JR/T 0158—2018 证券期货业数据分类分级指引

[13] 北京市地方标准《政务数据分级与安全保护规范》

[14] 贵州省地方标准 DB 52/T 1123—2016 政府数据 数据分类分级指南

[15] 上海市公共数据开放分级分类指南（试行）

[16]内蒙古自治区地方标准《公共数据分类分级指南》