ICS 35.240.01
CCS L 67

DB33

浙　江　省　地　方　标　准

DB33/T 2351—2021

数字化改革 公共数据分类分级指南

Digital reform—

Guidelines for public data classification and grading

2021－07－05 发布　　2021－08－05 实施

浙江省市场监督管理局　　发布

目　　次

前　言

本标准按照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。

请注意本标准的某些内容可能涉及专利，本标准的发布机构不承担识别这些专利的责任。

本标准由浙江省大数据发展管理局提出并归口。

本标准起草单位：浙江省大数据发展中心、浙江省标准化研究院、数字浙江技术运营有限公司、浙江省数据安全服务有限公司、联通数字科技有限公司。

本标准主要起草人：金加和、赵程遥、施筱玲、徐峰、林文都、孟一丁、叶春雷、蒋纳成、党铮铮。

本标准首次发布。

数字化改革 公共数据分类分级指南

1 范围

本标准规定了公共数据分类分级的一般要求、维度与方法。

本标准适用于公共数据的分类分级管理。公共管理和服务机构使用相关企业、第三方平台等数据的分类分级管理可参考执行。

本标准不适用于涉密公共数据的分类分级管理。

2 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 4754-2017 国民经济行业分类

GB/T 10113-2003 分类与编码通用术语

GB/T 25069-2010 信息安全技术 术语

GB/T 35295-2017 信息技术 大数据 术语

GB/T 38667-2020 信息技术 大数据 数据分类指南

3 术语和定义

GB/T 10113-2003、GB/T 25069-2010、GB/T 35295-2017和GB/T 38667-2020界定的以及下列术语与定义适用于本标准。

3.1

公共数据 public data

国家机关、法律法规规章授权的具有管理公共事务职能的组织（以下统称公共管理和服务机构）在依法履行职责和提供公共服务过程中获取的数据资源以及法律法规规章规定纳入公共数据管理范围的其他数据资源。

3.2

数据分类 data classification

按照公共数据具有的某种共同属性或特征（包括数据对象、重要程度、共享属性、开放属性、应用场景等），采用一定的原则和方法进行区分和归类，以便于管理和使用公共数据。

3.3

数据分级 date grading

按照公共数据遭到破坏（包括攻击、泄露、篡改、非法使用等）后对国家安全、社会秩序、公共利益以及个人、法人和其他组织的合法权益（受侵害客体）的危害程度对公共数据进行定级，为数据全生命周期管理的安全策略制定提供支撑。

4 数据分类

4.1 一般要求

4.1.1 应按照公共数据的多维特征及其相互间存在的逻辑关联进行科学、系统的分类。

4.1.2 使用的词语或短语应能准确表达数据类目的实际内容、内涵和外延，相同概念的用语应保持一致。

4.1.3 应结合现实需求，符合用户对公共数据区分和归类的普遍认知。每个类目下都有公共数据，不设没有意义的类目。

4.1.4 应保持与国家、地方、行业法律法规关于公共数据分类分级的标准和要求相一致，原则上同一分类维度内，同一条公共数据只分入一个类目。

4.2 分类维度

4.2.1 数据管理维度

应从元数据角度对公共数据资源目录中的数据进行数据管理维度分类，主要包括：

——数据产生频率；

——数据产生方式；

——数据结构化特征；

——数据存储方式；

——数据质量要求。

4.2.1.1 数据产生频率

根据数据产生的频率（单位时间内产生的数据量或达到指定数据量的频率）对数据进行分类，数据产生与更新的单位周期可分为：每秒、分、时、天、周、月、季度、半年、年，不定期，不更新等。

4.2.1.2 数据产生方式

根据公共数据产生方式可分为：人工采集数据、信息系统产生数据、感知设备产生数据，原始数据、二次加工数据等。

4.2.1.3 数据结构化特征

根据公共数据的结构化特征可分为：结构化数据、半结构化数据和非结构化数据。

4.2.1.4 数据存储方式

根据公共数据储存方式可分为：关系型数据库存储数据、键值数据库存储数据、列式数据库存储数据、图数据库存储数据、文档数据库存储数据等。

4.2.1.5 数据质量要求

根据数据完整性、时效性、准确性等维度的质量要求对数据进行分类。

4.2.2 业务应用维度

对公共数据资源目录中的数据进行业务应用维度分类，主要包括：

——数据产生来源；

——数据所属行业；

——数据应用领域；

——数据使用频率；

——数据共享属性；

——数据开放属性。

其中数据产生来源、数据所属行业应按照GB/T 38667-2020中6.3 业务应用视角相关要求，具体行业领域分类可参照GB/T 4754-2017中第3章和第5章的相关要求。

4.2.2.1 数据应用领域

根据数据应用领域分类体现公共数据对数字化改革的支撑作用，可分为：党政机关整体智治、数字政府、数字经济、数字社会、数字法治等领域。

4.2.2.2 数据使用频率

根据数据使用的频率进行分类，综合考虑数据的访问频次和分析引用层面可分为：冷数据、温数据、热数据。

——冷数据类包括离线的，长期存档的，很少被访问和使用的数据；

——温数据类包括经常被访问和使用的数据；

——热数据类包括是需要被计算节点频繁访问的在线类数据。

4.2.2.3 数据共享属性

根据数据共享属性可分为：无条件共享类、受限共享类和不共享类。

a) 可以提供给所有公共管理和服务机构共享使用的，为无条件共享数据。

b) 可以部分提供或者按照特定要求提供给相关公共管理和服务机构共享使用的，为受限共享数据。列入受限共享数据的，数据提供单位应当明确共享条件。

c) 不宜提供给其他公共管理和服务机构共享使用的，为不共享数据。列入不共享数据的，应当有明确的法律、法规、规章依据和国家、省有关要求。

d) 列入受限共享和不共享的数据，可以经脱敏、脱密等处理后向公共管理和服务机构提供，法律、法规另有规定的除外。

4.2.2.4 数据开放属性

根据数据开放属性可分为：禁止开放类、受限开放类、无条件开放类。其中，

a) 禁止开放类包括：

1) 开放后危及国家安全、公共安全、经济安全和社会稳定的；

2) 涉及商业秘密、个人隐私的；

3) 因数据获取协议或者知识产权保护等禁止开放的；

4) 法律、法规规定不得开放的。

b) 受限开放类包括：

1) 涉及商业秘密、个人隐私，其指向的特定公民、法人或者其他组织同意开放，且法律、法规未禁止的；

2) 开放将严重挤占公共基础设施资源，影响公共数据处理效率的；

3) 开放安全风险难以评估的；

4) 依法经脱敏、脱密等处理的禁止开放类公共数据，符合受限开放的，应列为受限开放类公共数据。

c) 无条件开放类包括：

1) 除禁止开放类与受限开放类公共数据以外的其他公共数据；

2) 已脱敏、脱密等处理的禁止开放类与受限开放类公共数据，符合无条件开放的，可列为无条件开放类公共数据。

4.2.3 安全保护维度

从数据的重要程度等对公共数据资源目录中的数据进行安全保护维度分类，包括：

——核心数据：对公共管理和服务机构履行社会管理职能或从事经营活动极其重要的公共数据；

——重要数据：公共管理和服务机构收集、产生、控制的不涉及国家秘密，但与国家安全、经济发展、社会稳定，以及公共利益密切相关的公共数据；

——一般数据：公共管理和服务机构履行社会管理职能或从事经营活动等一系列活动中产生的可存储的公共数据，不包括核心数据和重要数据。

4.2.4 数据对象维度

对公共数据资源目录中的数据进行数据对象维度分类，包括：

——个人：指自然人，包括属性数据和行为数据；

——组织：指政府部门、企事业单位、其他法人和非法人组织、团体，包括属性数据和业务数据；

——客体：指非个人或组织的客观实体，如道路、建筑、视频捕捉设备等，包括属性数据和感应数据。

4.3 分类方法

公共数据分类相关方法可参照GB/T 38667-2020第8章的相关要求。

5 数据分级

5.1 一般要求

5.1.1 应客观且可被校验，即通过数据自身的属性和分级规则即可判定其分级。

5.1.2 公共数据的分级应与其共享、开放的类型、范围、审批和管理要求直接相关。

5.1.3 应按照就高从严原则确定数据级别。

5.1.4 应充分考虑数据聚合情况、数据体量、数据时效性、数据脱敏处理等因素。

5.1.5 数据集的级别应根据下属数据项的最高级来定级。

5.1.6 在多类数据中均出现的 “通用数据”，可根据实际内容独立分级。

5.1.7 应结合具体应用场景定级。

5.2 分级维度

根据公共数据破坏后对国家安全、社会秩序、公共利益以及对公民、法人和其他组织的合法权益（受侵害客体）的危害程度来确定数据的安全级别，共分为4级，由高至低分别为：敏感数据（L4级）、较敏感数据（L3级）、低敏感数据（L2级）、不敏感数据（L1级），详细数据级别及分级参考判断标准见表1。

表 1 数据级别与判断标准

数据级别	级别标识	判断标准
L4 级	敏感	有下列情形之一： 对全社会、多个行业、行业内多个组织造成严重影响； 对单个组织的正常运作造成极其严重影响； 对人身和财产安全、个人名誉造成严重损害。

表 1 数据级别与判断标准(续)

L3 级	较敏感	有下列情形之一： 对全社会、多个行业、行业内多个组织造成中等程度的影响； 对单个组织的正常运作造成严重影响； 对个人名誉造成中等程度的损害。
L2 级	低敏感	有下列情形之一： 对全社会、多个行业、行业内多个组织造成轻微影响； 对单个组织的正常运作造成中等程度或轻微影响； 对个人的合法权益造成轻微损害。
L1 级	不敏感	对社会秩序、公共利益、行业发展、信息主体均无影响。

5.3 分级方法

应根据公共数据遭篡改、破坏、泄露或非法利用后，可能带来的潜在影响的范围和程度进行安全分级，其中：

——影响范围包括：国家安全，全社会、多个行业、行业内多个组织，单个组织或个人；

——影响程度包括：极其严重、严重、中等、轻微、无。

5.4 数据级别变更

5.4.1 主要因素

数据级别变更的主要因素包括：

a) 聚合因素；

b) 体量因素；

c) 时效因素；

d) 加工因素。

5.4.1.1 数据聚合因素

因业务需要将相同或不同级别的公共数据汇聚并进行分析、处理的，数据级别变更应遵循以下原则：

a) 聚合数据的部门应对数据重新定级；

b) 聚合数据安全级别一般不应低于所汇聚的原始数据的最高级别；

c) 原则上不允许原始数据落地，仅允许获取数据分析、处理后的结果。原始数据和临时数据使用应在中间存储环节有效清除。

5.4.1.2 数据加工因素

对公共数据进行汇总、分析、加工后产生的公共数据，若与原始数据之间存在较大差异，宜对新产生的公共数据重新定级，定级的结果可高于、等于、低于原始数据。

5.4.1.3 其他要求

已合法公开披露的公共数据可定为L1级。已脱敏数据可单独定级，经有效脱敏后的公共数据，可视情况降1级。法律法规规章未明确要求公开的个人信息等级不得低于L2级；法律法规明确保护的公共数据，数据安全等级应定为L3级以上；没有任何安全属性标识的公共数据，默认为L2级。

附 录 A
（资料性）
公共数据分类分级示例

数据类型	数据级别			
	L1	L2	L3	L4
组织	数据特征： 已经被企业明示公开或主动披露的数据；一般公开渠道可获取的数据。 示例： 企业信用评价信息，已向社会公示的企业信息、许可信息、处罚信息	数据特征： 涉及法人和其他组织权益的内部数据，用于一般业务使用，针对受限对象共享或开放。 示例： 空气环境监测信息，道路运输许可证信息，科研信用行业评价信息，社会组织严重违法失信名单	数据特征： 涉及法人和其他组织权益的内部数据，仅对受限内部对象共享或开放，一旦泄露会给企业带来直接经济损失或名誉损失的信息。 示例： 出口退税外贸企业申报情况信息，社保欠费企业信息，企业年报	数据特征： 法律法规明确保护的企业数据，泄露会给企业带来严重的经济损失或名誉损失，且对社会及其他组织造成损害的信息。 示例： 银行账户异动信息，法人账号信息，财务报表
个人	数据特征： 已经被政府、个人明示公开或主动披露的数据；一般公开渠道可获取的公民信息数据。 示例： 律师年度评价情况信息，公民法律援助申请信息，个人信用评价信息。	数据特征： 涉及公民的个人数据，用于一般业务使用，针对受限对象共享或开放；个人向特定群体公开的信息。 示例： 老年人优待证信息，无偿献血证	数据特征： 法律法规明确保护的个人隐私数据。泄露会给个人带来直接经济损失的信息。 示例： 社会保障卡，户口本，居住证，不动产权证。	数据特征： 依据国家法律法规和强制性标准或法规规定的特别重要数据，主要用于特定职能部门、特殊岗位的重要业务，只针对特定人员公开，且仅为必须知悉的对象访问或使用的数据。一旦泄露会对国家、社会造成严重损害。 示例： 出院记录，门诊就诊记录，城乡居民财政补助信息

公共数据分类分级示例（续）

数据类型	数据级别			
	L1	L2	L3	L4
客体	数据特征： 按照法律法规，明示公开或主动披露的数据；一般公开渠道可获取的数据。 示例： 废弃排放信息	数据特征： 涉及客体的总体数据或粗颗粒度数据；经规定程序审核后，可以向社会公开的数据。 示例： 近岸海区预报信息	数据特征： 涉及政府的内部信息，用于一般业务使用，针对受限对象共享或开放。 示例： 高速收费站过车信息、市内道路管制信息	数据特征： 国家法律法规和强制性标准定义的重要数据，一般只针对特定人员公开，且仅为必须知悉的对象访问或使用，被破坏或泄露后，会对社会、组织等造成损害。 示例： 空气环境质量小时值、GIS 设备图标信息

附 录 B
（规范性）
公共数据分级保护基本要求

类型	L1	L2	L3	L4
数据采集	1、公共数据采集应遵循合理、正当、必要原则。 2、公共数据采集设备应符合安全认证，采集流程和方式符合相应要求。	1、公共数据采集应遵循合理、正当、必要原则。 2、公共数据采集设备应符合安全认证，采集流程和方式符合相应要求，并对数据的完整性进行校验。	1、公共数据采集应遵循合理、正当、必要原则。 2、公共数据采集设备应符合安全认证，采集流程和方式符合相应要求，并对数据的完整性进行校验。 3、应采用加密方式对数据进行保护。	1、公共数据采集应遵循合理、正当、必要原则。 2、公共数据采集设备应符合安全认证，采集流程和方式符合相应要求，并对数据的完整性进行校验。 3、应采用加密方式对数据进行保护。 4、应使用水印溯源等技术，对数据泄露风险及行为进行追踪，可定位到责任人等。
数据传输	不需要进行传输加密。	1、公共数据在传输过程中应通过VPN等方式建立安全通道。 2、应对敏感数据进行检测。	1、公共数据在传输过程中应通过VPN等方式建立安全通道。 2、应对敏感数据进行检测。 3、应对公共数据进行加密传输，加密算法应符合国家密码相关法律、法规要求。	1、公共数据在传输过程中应通过VPN等方式建立安全通道，并对敏感数据进行检测。 2、应对敏感数据进行检测。 3、应对公共数据进行加密传输，加密算法应符合国家密码相关法律、法规要求。 4、应使用水印溯源等技术，对数据泄露风险及行为进行追踪，如定位到责任人等。
数据存储	1、公共数据应保存在可信或可控的信息系统或物理环境中。 2、应建立数据备份机制，定期进行数据的备份。	1、公共数据应保存在可信或可控的信息系统或物理环境中。 2、应建立数据备份机制，定期进行数据的备份。 3、对存储数据的访问进行日志审计。	1、公共数据应保存在可信或可控的信息系统或物理环境中。 2、应建立数据备份机制，定期进行数据的备份。 3、对存储数据的访问进行日志审计。 4、对公共数据可进行加密存储。	1、公共数据应保存在可信或可控的信息系统或物理环境中。 2、应建立数据异地备份机制，定期进行数据的备份。 3、对存储数据的访问进行日志审计。 4、应对公共数据进行加密存储。

公共数据分级保护基本要求（续）

类型	L1	L2	L3	L4
数据访问	1、设置身份标识与鉴别机制。 2、对数据访问行为进行审计与分析。	1、设置身份标识与鉴别机制。 2、对数据访问行为进行审计与分析。 3、可采用口令、密码、生物识别等鉴别技术对用户进行身份鉴别。	1、设置身份标识与鉴别机制。 2、对数据访问行为、访问内容、访问频率等访问情况进行审计、分析。 3、应采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别。	1、设置身份标识与鉴别机制。 2、对数据访问行为进行审计与分析。 3、应采用口令、密码、生物识别等两种或两种以上组合的鉴别技术对用户进行身份鉴别。 4、应持续对用户账号进行风险监测，并对账号进行动态授权。
数据共享	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批后无条件共享。	审批要求：数据主管部门审批和数据提供单位授权后受限共享。 技术要求： 1、视情况脱敏。 2、对数据共享全链路各环节的权限最小化控制，比如白名单控制并对异常进程监控。 3、对数据共享全链路各环节风险进行监控。	不共享
数据开放	无条件开放	审批要求：数据主管部门审批后受限开放或无条件开放。 技术要求：视情况脱敏。	审批要求：数据主管部门审批和信息主体授权后受限开放。 技术要求： 1、脱敏后受限开放。 2、对数据开放全链路各环节的权限最小化控制，如进行白名单控并对异常进程监控。	禁止开放
数据销毁	1、建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。 2、业务终止时自行决定数据是否需要销毁，宜采用删除、覆写法等方式进行数据销毁。	1、建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。 2、业务终止时宜采用删除、覆写法等方式销毁有关数据。	1、建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。 2、业务终止时应以不可逆的方式销毁有关数据。	1、建立数据销毁和存储媒体销毁审批机制，并对销毁过程进行记录。 2、业务终止时应以不可逆的方式销毁有关数据。