

武汉市公共数据资源开放分级分类指南（试行）

1 引言

本指南规定了公共数据资源开放的分级分类流程、要点、方法、示例等内容，本市各级政务部门、公共服务企事业单位（以下统称公共数据资源开放主体）根据本指南对公共数据资源进行分级分类，并采取相应风险防控和安全保障措施，保障本市公共数据资源开放工作有力有序开展。

2 范围

本指南适用于本市公共数据资源开放主体在依法履职过程中，采集和产生的各类数据资源面向社会开放的分级分类。

本指南提供通用、共性参考原则和方法，各公共数据资源开放主体根据本行业、本区域的法律法规和相关规定，对本指南进行调整、补充，并制定本部门公共数据资源开放分级分类细则。

涉及国家秘密的公共数据资源管理，按照相关保密法律、法规的规定执行，不纳入本指南开放范围。

3 规范性引用文件

GB/T 35295-2017 信息技术 大数据 术语

GB/T 35273-2020 个人信息安全规范

4 术语和定义

4.1 公共数据资源

本市各级政务部门、公共服务企事业单位在履行职责、提供服务过程中采集、产生的各类数据的总称。政务部门包括本市各级行政机关以及法律、法规授权具有社会公益服务职能的事业单位和社会组织。公共服务企事业单位包括本市供水、供电、供气、交通运输和邮政、通信、教育、医疗、康养以及其他承担公共服务职能的企事业单位。

4.2 公共数据资源开放分级

公共数据资源开放分级是指在公共数据资源开放过程中，从公共数据资源安全要求、个人和企业信息保护要求和应用要求等因素，将公共数据资源分为不同级别的管理方式。

4.3 公共数据资源开放分类

公共数据资源开放分类是指在公共数据资源开放过程中，将公共数据资源分为无条件开放、有条件开放、不予开放三种开放类型的管理方式。

4.4 个人敏感信息

一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。例如个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰，以及基因、影像资料（包括照片、视频等）、人脸识别、指纹等生物特征数据。

4.5 开放风险

公共数据资源开放过程中可能对个人、组织、社会利益或国家机关运作造成影响或损害。

5 分级分类原则

5.1 依从性原则

公共数据资源开放分级分类应遵循国家、地方、部门相关法律、法规及监管要求。

5.2 安全性原则

分级分类应以公共数据资源安全可控开放为基础。

5.3 可操作性原则

应避免对公共数据资源开放进行过于复杂的分级分类规划，保证公共数据资源开放分级分类能够快速有效地制定妥善的开放方式。

5.4 时效性原则

公共数据资源开放的分级分类具有一定的有效期。公共数据资源开放的级别和类型可能因时间变化按照一些预定的安全策略发生改变。

5.5 可扩展性原则

分级分类应充分考虑国际国内发展趋势，定期征询相关专家，完善和调整分级分类规则。

6 开放类型

公共数据资源开放类型分为无条件开放、有条件开放和不予开放三种类型，如表1所示。

表 1 公共数据资源开放类型

开放类型	说明
不予开放	涉及商业秘密、个人隐私，或者法律、法规规定不得开放的公共数据资源。
有条件开放	需要按照特定条件提供给自然人、法人和非法人组织的公共数据资源。
无条件开放	除不予开放和有条件开放以外的其它公共数据资源。

6.1 开放条件

对于不予开放类公共数据资源，不得开放；

对于无条件开放类公共数据资源，无需任何条件直接开放；

对于有条件开放类公共数据资源，需通过实名认证开放或审核开放。

6.2 管控要求

不同的公共数据资源开放类型有不同的管控要求，如表2所示。

表 2 不同公共数据资源开放类型管控要求

数据开放类型	数据开放类型管控要求	开放条件
无条件开放类数据	公共数据资源开放主体通过市公共数据资源开放平台无条件开放。	无
有条件开放类数据	公共数据资源开放主体通过市公共数据资源开放平台公布利用数据的技术能力和安全保障措施等条件，向符合条件的自然人、法人和非法人组织开放。	实名认证 开放 审核开放
不予开放类数据	公共数据资源开放主体可以根据社会需求，对非开放类数据进行脱密、脱敏等处理或者相关权利人同意开放的，降级后按对应类别开放。	

7 分级分类

7.1 公共数据资源开放分级分类要点

(1) 对数据泄露或损坏影响应基于数据完全泄露或损坏来考虑，而不应基于已有任何技术的防护措施来考虑。

(2) 《中华人民共和国网络安全法》已明确要对个人信息保护，要高度重视服务对象或业务相关的个人信息保护，在数据开放分级中从高考虑。

(3) 对于数据体量大，涉及的服务对象（包含部门或个人）多、涉及服务对象（包含部门或个人）的服务内容重要，影响程度应考虑从高确定。

(4) 安全属性（完整性、保密性、可用性、可靠性、不可抵赖性）是信息安全风险评估中的重要参考属性，针对数据开放分级，数据开放安全属性遭到破坏后可能造成的影响，是确定数据开放级别的重要判断依据。

7.2 公共数据资源开放分级分类方法

7.2.1 数据开放分级分类要素

数据开放分级主要考虑三个要素，即影响的对象、影响范围、影响程度。

影响对象划分为：部门、企业、个人。

影响范围划分为：多个部门、多个企业、社会群体。

影响程度划分为：严重、中等、轻微和无影响，指数据开放安全属性遭到破坏后带来的影响大小。

7.2.2 数据开放分级分类的流程

数据开放分级分类一般按照如下四个步骤执行：

步骤一：确定影响对象。

步骤二：确定影响范围。确定该类数据开放安全属性遭到破坏后可能影响的范围，包括多个部门、多个企业、社会群体等。

步骤三：确定影响程度。确定该类数据开放安全属性遭到破坏后可能影响程度，包括严重、中等、轻微和无影响。

步骤四：综合上述三要素，对数据开放分级分类。

汇总上述步骤确定的该类数据开放安全属性遭到破坏后的影响对象、影响范围、影响程度，对数据开放进行分级分类，如表3所示：

表 3 公共数据资源开放分级分类对照表

开放级别	影响程度	参考说明	开放类型	开放条件
4	严重	1、可能导致一个或多个部门全部工作无法开展，会给企业造成重大经济损失。 2、可能引发多人诉讼或集体诉讼，甚至引发群体性事件。 3、可能导致个人重大经济损失，甚至人身安全。	不予开放	-
3	中等	1、可能导致政府部门部分业务无法开展，企业经营造成较大经济损失。 2、可能引发一定范围的企业、个人对政府主管部门的投诉。 3、可能导致个人较严重的经济或其他损失。	有条件开放	审核开放
2	轻微	1、可能导致个别业务短时间无法开展，造成轻微的社会影响。 2、可能导致企业经营受到损失、影响社会诚信。 3、可能对个人、政府部门或企业声誉造成一定程度损害。	有条件开放	实名认证
1	无影响	对部门、企业、个人无不良影响。	无条件开放	-

8 分级分类示例

例1：党政部门在网站上发布的文件、组织机构、主要领导职责等；发布的各类指标、气象数据、水质指标、交通数据等，按照影响对象、影响范围和影响程度分析，属于无影响，开放级别属1级。可定为无条件开放类型。

例2：数据集名称：2018年交通处罚信息。

字段：决定书编号，案件案号，处罚当事人，法人代表，违章事实，处罚依据，处罚结果，执法主体，处罚日期。

影响对象：个人（受处罚的当事人、法人代表）；

影响范围：社会群体；

影响程度：轻微；

该数据集为有条件开放；开放级别为2级，开放条件为实名认证。

例3：数据集名称：市长热线数据

字段：投诉人信息、投诉日期、投诉内容、处理意见等。

影响对象：个人（投诉人）、部门或企业（被投诉对象）；

影响范围：社会群体、多个部门或多个企业。

影响程度：中等；

可造成个人或群体（投诉人）、部门或企业（被投诉对象）的信誉受到影响，对被投诉人的经济状况或企业的经营敏感信息的泄露。

确定为有条件开放，开放级别为3级，开放条件为审核开放。

9 数据融合风险

分级分类时，应当预判与已开放的数据集多源融合可能造成的数据安全风险。例如：数据集A采用了删除身份证号码中间8位的匿名处理后开放（如420102XXXXXXXX1234），但同时开放的数据集B中包含了自然人生日信息，在该情况下，等同于开放了自然人全部身份证号码。数据开放主体应当对A、B重新定为更高级别开放，或改变匿名处理方式，处理后重新开放。

对于无法评估的不确定性风险，组织行业专家研讨等方式确定开放类型和开放条件。

10 数据开放条件及要求

10.1 数据开放安全条件

对于开放级别2的数据，公民、法人和其他组织（以下称为“公共数据资源利用主体”）需具备基础的数据安全保护能力，并通过实名认证才能申请使用。

对于开放级别3的数据，公共数据资源利用主体需提供较完善的数据安全保护体系，有等保2级以上或ISO27000等认证，或有满足同等要求的数据安全保护措施，并通过实名认证才能申请使用。

10.2 应用场景要求

公共数据资源利用主体申请使用开放级别2及以上的数据时，不得用于挖掘个人敏感信息，仅可在自身业务范围内进行科学研究、咨询报告、业务支撑以及主管部门授权等场景使用，不得对外提供查询服务，不得针对具体组织对外发布新闻等信息，同时禁止用于营销等目的的个人敏感信息挖掘，禁止用于向他人提供敏感信息的查询，禁止发布相关解读。