重庆市大数据应用发展管理局文件

渝大数据发〔2023〕39号

重庆市大数据应用发展管理局
关于印发《重庆市公共数据分类分级指南2.0（试行）》的通知

各区县（自治县），两江新区、西部科学城重庆高新区、万盛经开区管委会，市级各部门，有关单位：

为深入贯彻落实《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《重庆市数据条例》等数据安全有关要求，加强数据分类分级保护，我局研究编制了《重庆市公共数据分类分级指南2.0（试行）》，现印发给你们，请认真贯彻执行。

附件：重庆市公共数据分类分级指南2.0（试行）

重庆市大数据应用发展管理局

2023年7月31日

附件

重庆市公共数据分类分级指南 2.0

（试行）

目录

1 范围

本指南规定了重庆市公共数据分类分级原则、要求、维度与方法。

本指南适用于本市范围内公共数据的分类分级管理。

2 规范性引用文件

下列文件是本指南的重要参考依据。凡是注日期的引用文件，仅所注日期的版本适用于本指南。凡是不注日期的引用文件，其最新版本适用于本指南。

《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》

《重庆市数据条例》

GB/T 7027-2002 信息分类和编码的基本原则与方法

GB/T 10113-2003 分类与编码通用术语

GB/T 21063.4-2007 政务信息资源目录体系

GB/T 25069-2010 信息安全技术 术语

GB/Z 28828-2012 信息安全技术 公共及商用服务信息系统个人信息保护指南

GB/T 35295-2017 信息技术 大数据 术语

GB/T 37988-2019 信息安全技术 数据安全能力成熟度模型

GB/T 35273-2020 信息安全技术 个人信息安全规范

GB/T 38667-2020 信息技术 大数据 数据分类指南

GB/T 4754-2017 国民经济行业分类

3 术语和定义

下列术语和定义适用于本指南。

3.1 公共数据

公共数据是指国家机关和法律、法规授权的具有管理公共事务职能的组织（以下称政务部门）为履行法定职责收集、制作的数据，及医疗、教育、供水、供电、供气、通信、文旅、体育、环境保护、交通运输等公共企业事业单位（以下称公共服务组织）在提供公共服务过程中收集、制作的涉及公共利益的数据。

3.2 数据分类

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

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、公共利益以及公民、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。

3.4 分类维度

用于实现公共数据分类的某个或某些共同特征。

3.5 分级维度

用于实现公共数据分级的某个或某些共同特征。

4 总体要求

4.1 数据范围

本市区域范围内政务部门和公共服务组织，在依法履行职责过程中获得的各类数据资源。

医疗、教育、供水、供电、供气、通信、文旅、体育、环境保护、交通运输等公共企业事业单位涉及公共属性的数据，参照适用本指南；法律、法规另有规定的，从其规定。

法律、法规、规章对统计数据、地理信息数据、不动产数据、公共信用数据等公共数据已有规定的，从其规定；没有规定的，参照适用本指南，涉及国家秘密的数据适用《中华人民共和国保守国家秘密法》等法律、行政法规的规定。

4.2 组织保障

应建立公共数据分类分级组织保障体系，明确相关部门的组织领导、业务管理、安全管理等职责和人员岗位角色要求。

4.3 制度保障

应建立公共数据分类分级制度保障，明确分类分级的原则、方法和要求，确立日常管理流程和操作规程，制定考核评价等机制。

4.4 技术要求

使用技术手段实现公共数据安全分类分级的人工/自动属性标识，应通过人工/自动方式维护公共数据资源目录，定期对公共数据安全属性进行评审和修订。

5 数据分类

5.1 分类原则

a）科学性原则：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、系统化的分类，分类规则相对稳定。

b）规范性原则：所使用的词语或短语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。用语标准、简洁。

c）实用性原则：类目划分应结合现实需求，符合用户对公共数据分类的普遍认知。每个类目下都有公共数据，不设没有意义的类目。

d）扩展性原则：应充分考虑发展趋势，定期征询相关专家组织意见，完善和调整数据类目设置和层级划分。

e）唯一性原则：同一分类维度内，同一条公共数据只分入一个类别。

5.2 分类维度

公共数据分类维度分为数据管理、业务应用、安全保护、数据对象等。

5.2.1 数据管理维度

公共数据管理维度应从元数据角度对其进行分类。包括但不限于数据产生频率、数据体量、数据产生方式、数据结构化特征、数据存储方式、数据质量要求等分类维度。

5.2.1.1 根据数据产生频率和数据体量

按产生频率分类是指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。

根据数据产生周期可分为每秒、分、时、天、周、月、季度、半年、年，不定期，不更新数据等；根据单位周期中数据的产生量，可以以记录条数表示或者以数据占用空间表示，如百万条记录、千万条记录、GB 级数据、TB 级数据等。

5.2.1.2 根据数据产生方式

按公共数据产生方式可包括人工采集数据、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。

5.2.1.3 根据数据结构化特征

按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。

5.2.1.4 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。

5.2.1.5 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。

5.2.2 业务应用维度

业务应用维度包括但不限于数据产生来源、数据业务主题、数据所属行业、数据应用领域、数据共享属性、数据开放属性等分类维度。其中数据产生来源、数据所属行业应按照 GB/T 38667-2020 中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。

5.2.2.1 根据数据应用领域

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，可分为数字党建、数字政务、数字社会、数字经济、数字文化、数字法治、基层智治等领域。

5.2.2.2 根据数据共享属性

根据数据共享属性可分为：无条件共享类、有条件共享类和不予共享类。

可以提供给所有政务部门和公共服务组织共享使用的,为无条件共享数据。

可以部分提供或者按照特定要求提供给相关政务部门和公共服务组织共享使用的，为有条件共享数据。列入有条件共享数据的，应当有法律、行政法规或者国家有关规定为依据，并明确共享条件。

不宜提供给其他政务部门和公共服务组织等共享使用的，为不予共享数据。列入不予共享数据的，应当有法律、行政法规或者国家有关规定为依据。

列入有条件共享和不予共享的数据，可以经脱敏等处理后向政务部门和公共服务组织提供，法律、法规另有规定的除外。

5.2.2.3 根据数据开放属性

根据数据开放属性可分为：不予开放类、有条件开放类、无条件开放类。

不予开放类包括：依法确定为国家秘密的；开放后危及国家安全、公共安全、经济安全和社会稳定的；涉及商业秘密、个人隐私的；因数据获取协议或者知识产权保护等禁止开放的；法律、法规规定不得开放的。

有条件开放类包括：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；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；开放安全风险难以评估的；依法经脱敏等处理的不予开放类公共数据，符合有条件开放的，应列为有条件开放类公共数据。

无条件开放类包括：除不予开放类与有条件开放类公共数据以外的其他公共数据；已脱敏等处理的不予开放类与有条件开放类公共数据，符合无条件开放的，可列为无条件开放类公共数据。

5.2.3 安全保护维度

安全保护维度包括但不限于重要程度等分类维度。按照重要程度进行划分，公共数据可以划分为核心数据、重要数据和一般数据。

a）核心数据：对政务部门和公共服务组织履行社会管理职能或从事经营活动极其重要的公共数据。

b）重要数据：政务部门和公共服务组织收集、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。

c）一般数据：政务部门和公共服务组织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，不包含核心数据和重要数据。

5.2.4 数据对象维度

数据对象维度主要将公共数据所描述的对象分为个人、组织、客体三类。其中个人指自然人，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，包括组织属性数据和业务数据；客体是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。

5.3 分类方法

5.3.1 线分类法

线分类法旨在将分类对象按选定的若干个属性或特征，逐次分为若干层级，每个层级又分为若干类别。同一分支下，同层级

类别之间构成并列关系，不同层级类别之间构成隶属关系。同层级类别互不重复，互不交叉。线分类法适用于针对一个类别只选取单一分类维度进行分类的场景。

5.3.2 面分类法

面分类法是将所选定的分类对象，依据其本身的固有的各种属性或特征，分成相互之间没有隶属关系即彼此独立的面，每个面中都包含了一组类别。将某个面中的一种类别和另外的一个或多个面的一种类别组合在一起，可以组成一个复合类别。

面分类法是并行化分类方式，同一层级可有多个分类维度。面分类法适用于对一个类别同时选取多个分类维度进行分类的场景。

5.3.3 混合分类法

混合分类法是将线分类法和面分类法组合使用，克服这两种基本方法的不足，得到更为合理的分类。混合分类法的特点是以其中一种分类方法为主，另一种做补充。混合分类法适用于以一个分类维度划分大类、另一个分类维度划分小类的场景。

6 数据分级

6.1 分级原则

a）可执行性原则：公共数据级别划分应满足相关法律、法规及监管要求，避免对数据进行过于复杂的分级规划，保证数据分级使用和执行的可行性。

b）时效性原则：公共数据的定级具有一定的有效期，数据级别可能因时间变化按照预定的安全策略发生改变。

c）合理性原则：公共数据定级不宜过高或过低，级别划定过低可能导致数据不能得到有效保护；级别划定过高可能不利于数据利用或产生不必要的管理成本。

d）客观性原则：公共数据的分级规则是客观并可以被校验的，即通过数据自身的属性和分级规则即可判定其分级。

6.2 分级要求

a）公共数据的分级与其共享、开放的类型、范围、审批和管理要求直接相关。

b）应加强个人信息和重要数据保护，按照就高从严原则确定数据级别。

c）数据定级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，根据实际升高或降低数据级别。

d）数据集的级别根据下属数据项的最高级来定级。

6.3 分级维度

公共数据分级应充分考虑公共数据对国家安全、社会秩序和公共利益的重要程度，以及是否涉及个人隐私和商业秘密等敏感信息。综合考虑公共数据在遭到破坏后对国家安全、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，并根据各级别的公共数据特

征，梳理安全控制点，提出分类分级的安全管控规则。

6.4 分级方法

6.4.1 数据定级的影响因素

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。影响范围主要包括国家安全，全社会、多个行业、行业内多个组织，单个组织或个人。影响程度划分为极其严重、严重、轻微、无。

6.4.2 定级标准

根据上述因素，公共数据分为敏感数据（L4）、较敏感数据（L3）、低敏感数据（L2）、不敏感数据（L1）。

表 1 数据级别与判断标准

数据级别	级别标识	判断标准
L4	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。
L3	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	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	不敏感	对社会秩序、公共利益、行业发展、信息主体均无影响。

6.4.3 数据分级中的关键问题处理

6.4.3.1 数据升降级主要因素

a）从数据聚合考虑，聚合了多家业务部门的公共数据宜从高定级。

b）从数据体量来考虑，大量公共数据聚合宜升级。

c）从数据时效性考虑，历史数据可考虑降 1 级处理，但需明确历史数据的含义，并明确某时间点之前的数据。

d）已公开披露的公共数据可降低数据级别。

e）脱敏数据宜单独定级。经有效脱敏后的公共数据，可降 1－2 级，但视情况处理。

6.4.3.2 数据聚合与数据级别变更

因业务需要，需要将相同或不同级别的公共数据汇聚在一起进行分析、处理时，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。

6.4.3.3 数据汇总、分析、加工产生的数据与数据级别变更

因业务需要，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，定级的结果可能高于、等于、低于原始数据。

6.4.3.4 通用数据独立定级

在公共数据定级过程中，在多类数据中均出现的某些数据（数据表/数据项），可视为“通用数据”，可以将“通用数据”进行独立定级。具体的级别根据实际内容确定。

6.4.3.5 数据定级其他要求

已合法公开披露的公共数据可定为L1。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；法律法规明确保护的公共数据，数据安全等级应定为L3以上；没有任何安全属性标识的公共数据，默认为L2。

6.4.3.6 数据共享与数据级别

数据共享按照共享属性分为无条件共享，有条件共享，不予共享三类。

a）数据共享应遵循履职需要与最小必要原则。

b）L1 数据无条件共享；L2 数据无条件共享或有条件共享；L3 数据有条件共享；L4 数据有条件共享。

c）不共享类数据必须有相应法律、法规和政策依据。

d）行政相对人对数据共享有特殊要求且合法的，应从其约定。

e）因依法履职需要使用非涉密共享数据，且有法律、法规、

政策等依据或主体授权的，可直接获得授权使用共享数据。

6.4.3.7 数据开放、利用与数据级别

公共数据按开放属性分为不予开放类、有条件开放类、无条件开放类。

a）通过有条件开放方式获取的公共数据不得用于申请之外的用途。

b）L1 数据无条件开放；L2 数据无条件开放或有条件开放；L3 数据有条件开放；L4 数据不予开放。

c）获取有条件开放类数据的用户应落实公共数据开放利用协议中约定的安全保障措施。

6.5 分级保护基本要求

根据公共数据定级结果，按照公共数据分级保护基本要求，对数据采集、数据传输、数据存储、数据访问、数据共享、数据开放、数据销毁等全生命周期进行保护，具体如表 2 所示。

表 2 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。

类型	L1	L2	L3	L4
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。
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。

类型	L1	L2	L3	L4
数据共享	审批要求：无条件共享。	审批要求：有条件共享或无条件共享。 技术要求：视情况脱敏。	审批要求：有条件共享。 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。	审批要求：有条件共享。 技术要求： 1.须脱敏后才可共享。 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。 4.应使用水印溯源等技术，对数据泄密风险及行为进行追踪，如定位到责任人等。
数据开放	无条件开放	审批要求：有条件开放或无条件开放。 技术要求：视情况脱敏。	审批要求：有条件开放。 技术要求： 1.脱敏后有条件开放。 2.对数据开放全链路各环节的权限最小化控制，如进行白名单控制并对异常进程监控。	不予开放。
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。

附录 1

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： 企业统一社会信用代码、隶属企业名称。	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： 企业年报及股东认缴出资方式、企业年报资产总额。	数据特征： 涉及法人和其他组织权益的内部数据，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： 企业年报基本信息,企业出资信息，企业未履行生效裁判信息。	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： 法定代表人移动电话,法定代表人身份证件号码,核准股权出质债权人证件号码。
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： 居住证签发机关统一社会信息代码、学生ID。	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： 户口所属派出所名称、婚姻登记机关。	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： 人口出生日期，婚姻登记合影照片，公积金个人贷款信息。	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： 公民身份证号码，公积金月缴存额,监狱服刑人员关押地点。
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： 机动车行驶证发证机关、房地产权登记机构。	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： 不动产权不动产单元号、机动车车辆型号	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： 房产规划用途、机动车车辆识别代号。	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： 不动产建筑面积、不动产坐落地址。

附录 2

法人数据分级示例

数据项	示例	数据级别
统一社会信用代码	91500000MA60G3R48R	L1
组织机构代码	MA60G3R4-8	L1
法人名称	数字重庆大数据应用发展有限公司	L1
法定代表人/负责人	严**	L1
法定代表人/负责人证件类型	**	L4
法定代表人/负责人证件号	**	L4
登记机关	重庆市市场监督管理局	L1
业务主管机关	重庆市大数据应用发展管理局	L1
登记日期	2019-07-26	L1
存续状态	开业	L1
从业人数	30	L2
登记注册证类型	有限责任公司（法人独资）	L1
登记注册号	500000011963485	L1
宗旨和业务范围	一般项目：大数据服务；互联网数据服务；工业互联网数据服务；信息安全设备销售等	L1
兼营	无	L1
注册资本/开办资金	200,000,000	L1
币种代码	人民币/元	L1
经费来源	国有资本	L2
机关事业性质	非事业编	L1
社会组织类型	小型	L1
市场主体类型编码	170	L2
市场主体类型大类	国有企业	L1
行业门类	其他 IT 与互联网服务	L2
行业代码	210	L2
核准日期	2022-10-31	L1
经营（营业）起始日期	2019-07-26	L1
经营（营业）截止日期	无固定期限	L1

数据项	示例	数据级别
属地监管工商所	重庆市市场监督管理局	L2
属地监管税务部门	国家税务总局重庆市税务局	L2
个体工商户组成形式	否	L1
是否城镇	是	L1
宗教教别	否	L1
宗教派别	否	L1
民宗部门内设机构	否	L1
行政机构级别	无	L2
是否具备行政执法主体资格	无	L2
教育机构办学类型	无	L1
文化机构评估定级情况	无	L2
联系电话	138********	L4
电子邮箱	**@163.com	L3
联系传真	023-67725628	L3
单位名称（简称）	Digital Chongqing Big Data Application Development Co., Ltd.	L1
法人名称（英文）	ZhiqiangYan	L1
注册地址	重庆市渝北区渝兴广场 B1 栋 17 楼	L1
法人机构代码	91500000MA60G3R48R	L2

附录 3

人口数据分级示例

数据项	示例	数据级别
姓名	张三	L4
身份证	500101198808******	L4
性别	男	L3
民族	汉	L3
出生日期	1988 年 8 月*日	L4
宗教信仰	*教	L2
家庭住址	*市*区*街道*路*号	L4
固定电话	1991234****	L4
兵役状况	服兵役	L3
居委会	**社区	L3
门楼牌	*路*号	L4
归侨回国时间	20**年*月	L3
产权证编号	渝（2021）xx 区不动产权第 000******号	L3
不动产权证缮证时间	20**年*月*日	L3
房屋面积	***平方米	L4
存款信息	***元	L4
域名信息	***.net	L3
遗传疾病	***	L4
单位名称	重庆****公司	L3
商标	**	L3
学号	2006042601	L2
学校名称	重庆交通大学	L1

重庆市大数据应用发展管理局办公室　　2023 年 8 月 1 日印发