# DB3311

浙 江 省 丽 水 市 地 方 标 准

DB3311/T 127—2020

# 公共数据共享安全管理规范

2020－01－15 发布　　2020－02－15 实施

丽水市市场监督管理局　　发 布

# 目　　次

# 前　言

本标准依据 GB/T 1.1-2009 给出的规则起草。

本标准由丽水市大数据发展管理局提出并归口。

本标准起草单位：丽水市数据管理中心、丽水市公安科技信息化局、亚信科技(成都)有限公司。

本标准起草人：王玲玲、项伟平、刘晓峰、周嘉盈、朱大鹏、周伟华、王啸、廖双晓、李著。

本标准属首次发布。

# 公共数据共享安全管理规范

## 1 范围

本标准规定了公共数据共享安全管理的术语和定义、管理要求、工作机制、数据归集、数据共享、安全运营。

本标准适用于非涉密公共数据共享安全管理。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是已经标注日期的引用文件，仅所注明日期的版本适用于本标准。凡是未标注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 22239 网络安全等级保护基本要求

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**公共数据**

各级行政机关、履行公共管理和服务职能的机构在依法履职过程中采集和产生的各类数据资源。

3.2

**公共数据共享**

各级行政机关、履行公共管理和服务职能的机构因履行职责需要使用其他政务公共数据资源或为其他政务部门提供公共数据资源的行为。

3.3

**敏感数据**

包含内容可能对国家机关、公民、法人和其他组织造成不良影响的数据。

3.4

**资源目录**

对公共数据资源依据规范的描述，按照一定分类方法进行排序和编码的一组信息，用以描述资源特征。

3.5

**数据脱敏**

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.6

**公共数据平台**

支撑数据管理工作的信息系统，包含数据资源目录管理、数据供需管理、数据共享交换支撑等功能。

## 4 管理要求

4.1 应按照“统筹管理、按需共享、最小够用、安全可控”的要求，维护国家和社会公共安全，保守国家秘密，保护商业机密、个人隐私。

4.2 制作、采集或使用行政相对人商业秘密、个人隐私等敏感数据的，应明确数据使用范围和保护责任。

## 5 工作机制

5.1 各政务部门应根据公共数据管理工作机制，成立工作组或工作专班。

5.2 各政务部门应配备数据专员，包含但不限于以下职责：

a) 牵头本部门公共数据资源目录编制；
b) 归集本部门待归集数据；
c) 根据本部门需求在公共数据平台上提起数据共享需求；
d) 在公共数据平台上响应其他部门提起的数据需求。

## 6 数据归集

### 6.1 资源编目

#### 6.1.1 目录编制

各政务部门应在公共数据平台中登记公共数据目录，完整、准确提供数据资源名称、资源格式、共享属性、更新频率、数据项详情内容（包括数据项名称、类型、长度、是否可空等）、安全保护要求等信息。

#### 6.1.2 目录更新

各政务部门应按照有效性与及时性要求进行资源目录更新。

#### 6.1.3 审核发布

数据管理部门应建立资源目录审核发布机制，资源目录通过公共数据平台发布。

#### 6.1.4 目录校核

对公共数据资源目录有疑义或发现错误的，由数源部门校核。

### 6.2 数据治理

#### 6.2.1 完整性

数源部门应按照资源目录约定内容和数据覆盖范围提供数据，目录中必填数据项不得为空值。特别涉及个人、法人的关键指标项（姓名、证件号码、统一社会信用代码等）不得空缺，且能通过公共数据平台的个人、法人信息校验。

#### 6.2.2 及时性

数源部门应按照资源目录约定的数据更新频率按时归集数据。

#### 6.2.3 准确性

数源部门应确保提供各数据项与实际数据保持一致，且无明显错误。

## 7 数据共享

### 7.1 需求管理

7.1.1 数据需求部门应通过公共数据平台提出需求，明确需要的数据项、共享方式和具体应用场景。
7.1.2 数源部门对需求进行确认，数据管理部门对需求进行审核。

### 7.2 共享实施

在需求完成审批后由数据管理部门进行技术对接，依托公共数据平台向数据需求部门提供公共数据。在技术条件允许的情况下，应优先使用需求部门申请时要求的共享模式。

### 7.3 使用限制

7.3.1 数据需求部门未经数源部门授权，不得将共享数据对外提供或发布，不得以任何方式或形式用于社会有偿服务或其他商业用途。
7.3.2 使用个人敏感数据的，应建立个人授权机制。

### 7.4 共享终止

7.4.1 数源部门要求下架共享数据时，应向数据管理部门提交备案并说明数据共享终止原因，数据管理部门审核通过后终止数据共享。
7.4.2 达到数据共享期限时，应及时终止数据共享服务。

## 8 安全运营

### 8.1 技术要求

8.1.1 采用身份鉴别、数据源认证等安全机制保障共享数据来源的真实性。
8.1.2 在不影响共享数据使用情况下，具备条件的数源部门应在本地对敏感数据进行脱敏后再进行数据归集。数源部门不具备条件在本地脱敏而有必要进行脱敏的，应在资源编目安全保护要求明确提出脱敏需求，并由数据管理部门在抽取数据至共享交换平台之前完成数据脱敏。
8.1.3 对未脱敏的敏感数据以内容加密或链路加密的方式进行传输。在共享交换平台中，需根据数源部门的要求对未脱敏的敏感数据进行加密存储。

8.1.4 记录并保存数据交换日志，数据操作行为可管可控并全程留痕，保证审计日志的完整性和真实性，防范数据伪造、篡改或者窃取，确保任何数据泄密泄露事故及风险可追溯到相关责任单位和责任人。
8.1.5 制定访问控制策略，规范不同等级用户在交换节点、公共数据工作平台和共享交换平台的权限，防止未经授权查询、修改或者传输数据。

### 8.2 平台运维

8.2.1 公共数据平台部署于电子政务外网，应符合GB/T 22239中的三级安全要求，各政务部门应建立规范的运维管理制度。
8.2.2 共享交换平台由中心库、交换节点、交换链路、交换前置机组成。中心库、交换节点、交换链路的安全由数据管理部门管理；交换前置机的安全由提供部门管理；业务信息系统和交换前置机之间的安全由各政务部门自行管理。

### 8.3 外包管理

8.3.1 各政务部门采用外包服务提供商参与公共数据共享相关工作时，涉及收集、存储、传输或者应用数据等操作行为的，应当依法与外包服务提供商签订数据处理协议和保密协议，并对所有数据操作行为进行监督，每季度至少一次审计操作日志。
8.3.2 外包服务提供商应当具备相应资质，建立和落实数据安全管理、个人隐私保护、应急管理等管理制度和技术防护措施。

### 8.4 应急管理

各政务部门应落实公共数据安全应急工作机制，制定公共数据安全事件应急预案，每年至少一次组织演练。各政务部门应建立应急协同机制。

### 8.5 风险评估

数据管理部门每年至少一次组织开展公共数据安全风险评估，发现公共数据共享过程中潜在的安全风险，并发布评估报告。

### 8.6 安全培训

各政务部门和数据管理部门应建立公共数据安全培训制度，每年至少一次对系统建设、运维、使用和从业人员进行公共数据安全培训。