

SZSD

数 字 山 东 工 程 标 准

SZSD13 0005—2024

公共数据 数据生命周期安全规范

Public data-Security specification of data lifecycle

2024 - 04 - 15 发布

2024 - 06 - 01 实施

临沂市大数据局 发 布

目 次

前 言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 概述 2

5 总体原则 3

6 基本要求 3

7 各阶段安全要求 3

 7.1 公共数据采集 4

 7.2 公共数据传输 4

 7.3 公共数据存储 4

 7.4 公共数据使用 5

 7.5 公共数据交换 5

 7.6 公共数据退役 6

前 言

本文件按照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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由临沂市大数据局提出、归口并组织实施。

本文件起草单位：运筹数据技术（临沂）有限公司、临沂市大数据中心、临沂市罗庄区大数据局。

本文件主要起草人：于运程、解桂林、李小清、邓兰华、邓征启、上官相伟、卢彦辉、高蕾红、路敏敏。

公共数据 数据生命周期安全规范

1 范围

本文件规定了公共数据的总体原则和基本要求，同时规定了公共数据生命周期包含的公共数据采集、传输、存储、使用、交换和退役六个阶段的数据安全要求。

本文件适用于指导临沂市公共数据管理者、公共数据提供单位和公共数据利用主体等在公共数据生命周期各阶段的数据安全管理工作。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅注日期的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- GB/T 22239 信息安全技术 网络安全等级保护基本要求
- GB/T 25069 信息安全技术 术语
- GB/T 35273—2020 信息安全技术 个人信息安全规范
- GB/T 35274 信息安全技术 大数据服务安全能力要求
- GB/T 35295 信息技术 大数据 术语
- GB/T 37973 信息安全技术 大数据安全管理指南
- GB/T 37988 信息安全技术 数据安全能力成熟度模型
- GB/T 39786 信息安全技术 信息系统密码应用基本要求
- JR/T 0223 金融数据安全 数据生命周期安全规范
- DB37/T 3523.1 公共数据开放 第1部分：基本要求
- DB37/T 3523.2 公共数据开放 第2部分：数据脱敏指南
- DB37/T 3523.3 公共数据开放 第3部分：开放评价指标体系
- DB3713/T 261 公共数据 开放数据质量管理规范

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 public data

公共数据提供单位在依法履行公共管理职责、提供公共服务过程中，收集和产生的各类数据。

[来源：DB3713/T 261—2022，3.1]

3.2

数据生命周期 data lifecycle

将原始数据转化为可用于行动的知识的一组过程。

[来源：GB/T 35295-2017，2.1.2]

3.3

数据安全 data security

通过管理和技术措施，确保数据有效保护和合规使用的状态。

[来源：GB/T 37988—2019，3.1]

3.4

公共数据管理者 public data administrator

贯彻国家、省市关于大数据发展的方针政策和决策部署，统筹管理辖区公共数据资源的政务部门，一般指市级和县区级大数据局（大数据中心）。

[来源：DB3713/T 261—2022，3.5]

3.5

公共数据开放主体 public data open main organization

国家机关、法律法规授权的，具有管理公共事务职能的各级组织，具有公共服务职能的企业事业单位，人民团体等公共数据提供单位。

[来源：DB3713/T 261—2022，3.4]

3.6

公共数据利用主体 public data user

依法依规获取各类公共数据的自然人、法人和其他组织。

[来源：DB3713/T 261—2022，3.6，有修改]

4 概述

公共数据的生命周期主要包括公共数据采集、公共数据传输、公共数据存储、公共数据使用、公共数据交换和公共数据退役六个阶段，结构图见图1。

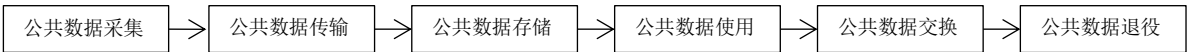


图1 公共数据生命周期结构图

各阶段具体定义如下：

- 公共数据采集：公共数据提供单位业务系统新产生数据，以及从外部系统收集数据的阶段。在本阶段，公共数据提供单位因履职需要，采用直接采集、委托第三方机构采集、协商等方式向公民、法人和其他组织获取有关数据，以及通过业务系统、监测、测量、录音、录像等方式产生有关数据。
- 公共数据传输：公共数据从一个实体通过网络或物理存储介质流动到另一个实体的阶段，涉及公共数据提供单位将公共数据传输归集到云平台、数据共享交换平台、大数据中心等，以及下级部门将公共数据传输汇聚到上级部门等。
- 公共数据存储：公共数据以任何数字格式进行物理存储或云存储的阶段。公共数据存储涉及采集数据存储、归集汇聚后的数据存储、数据共享交换后的数据存储等。
- 公共数据使用：公共数据管理者针对公共数据进行处理、计算、分析、可视化等操作的阶段。通常是对公共数据进行整合，形成基础数据库和主题数据库，并进行大数据分析利用转化成公共数据产品或服务。

——公共数据交换：公共数据提供单位之间或公共数据提供单位与公共数据利用主体进行数据共享、交换、开放的阶段。公共数据共享通常是公共数据提供单位因履行职责需要使用其他公共数据提供单位的公共数据，并为其他公共数据利用主体提供公共数据。公共数据交换通常是公共数据提供单位间或公共数据提供单位与公共数据利用主体进行数据交互；公共数据开放通常是公共数据开放主体通过数据开放平台向公共数据利用主体开放公共数据。

——公共数据退役：不再进行使用和交换的公共数据进入数据退役阶段，涉及公共数据管理者对公共数据的归档、转移、丢弃、销毁以及对存储介质的销毁处理等。

特定的公共数据所经历的生命周期由实际的业务场景所决定，所有的公共数据都会完整地经历前四个阶段。

5 总体原则

为规范公共数据安全的基本要求，防范和抵御公共数据可能面临的各类安全风险，各方在处理公共数据过程中，应遵循下列原则，具体包括：

- a) 合法正当原则：公共数据的管理和使用应符合法律法规和伦理规范，不应侵犯他人的合法权益，应确保公共数据生命周期各阶段数据活动的合法性和正当性；
- b) 权责明确原则：应明确各方公共数据安全管理职责，各方应积极履行相应职责，对公共数据的保密性、完整性、可用性和可追溯性负责；
- c) 目的明确原则：各方的公共数据处理活动应具有明确、清晰、具体的目的；
- d) 明示同意原则：公共数据提供单位应拥有对其所提供数据的处理目的、方式、范围等的知情权，公共数据利用主体在进行公共数据处理活动前应向公共数据提供单位明示，并获得授权同意，法律、行政法规另有规定的例外情况，从其规定；
- e) 最小必要原则：公共数据处理活动应仅处理可满足特定公共服务为目的所需的最少数量的公共数据；
- f) 公开透明原则：应以明确、易懂和合理的方式公开公共数据处理的范围、目的、规则等，并接受外部监督，法律、行政法规另有规定的例外情况，从其规定；
- g) 动态调整原则：公共数据的安全管理原则和安全防护要求应基于业务需求、安全风险态势、利用主体行为等因素实施动态调整；
- h) 全程可控原则：应采取与公共数据安全级别相匹配的安全管控机制和安全防护措施，确保公共数据在生命周期各阶段的保密性、完整性和可用性，避免公共数据在生命周期内被未经授权访问、破坏、篡改、泄露或丢失等。

6 基本要求

公共数据基本要求如下：

- a) 应建立完善的安全管理体系，包括安全策略、安全管理机构、安全责任、安全审计、安全培训和演练等方面；
- b) 应严格遵守相关法律法规和伦理规范，不应侵犯第三方的合法权益；
- c) 承载公共数据的信息系统应按GB/T 22239描述的基本要求，同步规划、建设、运营信息系统并对信息系统组织开展定级备案、等级测评、安全整改工作；
- d) 公共数据处理过程涉及的密码技术应按GB/T 39786描述的密码应用基本要求执行。

7 各阶段安全要求

7.1 公共数据采集

公共数据采集阶段要求如下：

- a) 应设立公共数据采集安全管理的岗位，由任职于该岗位的人员负责制定相关的公共数据采集安全管理的制度，推动相关要求、流程的落地，并对具体业务或项目的风险评估提供咨询和支持；
- b) 应按照规定的采集方式采集公共数据，如直接采集、委托第三方机构采集或者协商的方式采集，也可通过业务系统、监测、测量、录音、录像等方式产生有关数据，应遵守保护国家秘密、商业秘密和个人隐私的相关规定；
- c) 应对公共数据采集来源进行鉴别和记录，确保数据采集来源的合法性、正当性，明确数据类型及采集渠道、目的、用途、范围、频度、方式等；
- d) 采集外部系统数据前，应对数据采集过程中的网络环境、系统进行安全评估，确保采集数据的机密性、完整性和可用性；
- e) 应明确数据安全元数据管理要求，如口令策略、权限列表、授权策略等；
- f) 应按照科学的原则和方法对公共数据进行数据分类和安全定级；
- g) 涉及个人信息的，应按照GB/T 35273—2020中5.1至5.6规定的要求开展数据采集工作。

7.2 公共数据传输

公共数据传输阶段要求如下：

- a) 应设立公共数据传输安全管理的岗位，由任职于该岗位的人员负责制定相关的公共数据传输安全管理的制度，推动相关要求、流程的落地，并对具体业务或项目的风险评估提供咨询和支持；
- b) 应设立专门的网络可用性管理部门，由该部门人员来处理 and 解决公共数据传输过程中网络故障和维护网络的正常运行，降低网络故障或瘫痪可能性，同时网络和业务恢复时间应处在可控范围之内，保障数据在网络中传输的稳定性；
- c) 应在不同网络环境之间设置防火墙、入侵检测等安全防御措施来维护网络边界安全，以确保不同安全级别的网络相连接的安全性；防止未经授权的网络流量、恶意程序和攻击者进入网络破坏公共数据；
- d) 应明确公共数据传输安全管理规范、传输安全要求（如传输通道加密、数据内容加密、签名验签、身份鉴别、数据传输接口安全等），确定需要对数据传输加密的场景；
- e) 应对公共数据传输两端进行身份鉴别，确保数据传输双方可信任；
- f) 应采用校验技术保证公共数据在传输过程中的完整性；
- g) 应通过网络基础设施以及按照网络层数据防泄漏设备的备份建设，实现网络的高可用性，以保证公共数据传输过程中的稳定性；
- h) 重要数据不应通过离线或即时通信方式传输；
- i) 在可能涉及法律责任认定的应用中，应采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的抗抵赖和数据接收行为的抗抵赖。

7.3 公共数据存储

公共数据存储阶段要求如下：

- a) 应设立公共数据存储安全管理的岗位，由任职于该岗位的人员确定加密原则和技术工作，指导技术团队负责实现具体场景下的数据存储加密；
- b) 应确保公共数据存储设备或公共数据存储媒介（如硬盘驱动器、固态硬盘、USB闪存驱动器等）安全，并根据具体的应用场景和使用需求进行选择；

- c) 应明确公共数据存储相关安全管控措施，如加密、访问控制、数字水印、完整性校验等；
- d) 应明确公共数据备份与恢复安全策略，应建立公共数据备份与恢复操作规程，说明数据备份周期、备份方式、备份地点；应建立数据恢复性验证机制，保障数据的可用性与完整性；
- e) 应对公共数据进行异地备份，确保必要时可进行实时切换；
- f) 个人生物识别信息应与个人身份信息分开存储，原则上不应存储原始个人生物识别信息（如样本、图像等），仅存储个人生物识别信息的摘要信息；
- g) 个人信息存储期限应为实现个人信息主体授权使用目的所必需的最短时间，法律法规另有规定或者个人信息主体另行授权同意的除外，超出个人信息存储期限后，应对个人信息进行删除或匿名化处理；
- h) 应具备勒索病毒事前预警、事中阻断及事后恢复的保障能力；
- i) 应提供公共数据处理环节关联信息系统的冗余，保证数据的高可用性；
- j) 公共数据存储阶段应确保公共数据存储容器、方式、流程等的合法性、合规性。

7.4 公共数据使用

公共数据使用阶段要求如下：

- a) 应明确公共数据使用业务场景的目的、范围、审批流程（含权限授予、变更、撤销等）、人员岗位职责等，鼓励在保障安全的情况下，开展数据使用；
- b) 应明确公共数据统计分析、展示、发布、公开披露等不同数据使用场景的安全管理要求；
- c) 应根据不同公共数据使用场景采用安全处理措施（如去标识化、匿名化等），降低数据敏感度及暴露风险；
- d) 应建立严格的访问控制策略，以限制对公共数据使用相关系统的访问权限。仅经过授权的人员才能访问和使用数据，避免数据泄露和未经授权的访问；
- e) 应在公共数据使用过程中采用加密技术来保护数据的机密性和完整性。加密技术可以防止数据在使用过程中被窃取或攻击；
- f) 应建立安全审计和监控机制。通过审计和监控记录，及时发现和纠正安全问题，确保公共数据的使用过程符合规范和规定；
- g) 存在利用算法推荐技术进行自动化决策分析的情形，应保证决策的透明度和结果公平合理；
- h) 数据公开前应开展数据安全风险评估，明确公开数据的内容与种类、公开方式、公开范围、安全保障措施、可能的风险与影响范围等。涉及敏感个人信息、商业秘密信息的，以及可能对公共利益或者国家安全产生重大影响的，不应公开，法律法规、规章另有规定的除外；
- i) 利用所掌握的公共数据资源，公开市场预测、统计等信息时，不应危害国家安全、公共安全、经济安全和社会稳定；
- j) 应采取技术措施保证汇聚大量公共数据时不暴露敏感信息；
- k) 应对不同公共数据使用场景采取数字水印等技术，实现数据防泄密及溯源能力；
- l) 应对接入或嵌入的第三方应用加强数据安全管理和开展技术检测，确保其数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入；
- m) 应设置管理、防病毒、防入侵、防火墙、主动防御、法规遵从等功能，保护公共数据使用的网络免受病毒的危害；
- n) 应设置身份认证和准入控制，通过对PC、手机、平板等办公设备使用者的身份认证和准入控制，保证终端使用人身份的合法性。

7.5 公共数据交换

公共数据交换阶段要求如下：

- a) 应设立公共数据交换安全管理的岗位，由任职于该岗位的人员负责制定相关的公共数据交换安全管理的制度和方案，推动相关要求、流程的落地，并对具体业务或项目的风险评估提供咨询和支持；
- b) 应明确公共数据交换的原则、安全规范以及审核制度，应明确公共数据交换的内容、范围、管控措施、涉及机构或部门相关用户的职责和权限；
- c) 应通过对发布公共数据的格式、适用范围、发布者与使用者权利和义务执行必要控制，实现公共数据发布过程中数据的安全可控与合规；
- d) 应采用国家相关标准规定的密码技术，保障公共数据交换过程的保密性和完整性；
- e) 在公共数据交换过程中，应对数据密级进行划分，应对数据库的访问情况、用户查询数据权限的划分，敏感数据信息按要求进行脱敏或屏蔽；
- f) 应建立公共服务数据接口的安全管理机制，防范公共数据使用主体在数据接口调用过程中的安全风险；
- g) 应定期对数据交换平台的核心数据库进行安全状况检查，包括相关数据库安全漏洞、安全配置、弱口令、缺省口令、补丁更新、脆弱代码、程序后门等检测项，有效评估后建立数据库安全基线，并提供加固建议以此保证核心数据库的可靠性和可用性；
- h) 应明确数据出境业务场景，严格遵守国家法律、行政法规数据出境安全监管要求，符合国家法律、行政法规规定情形的，应提前开展数据出境安全评估及网络安全审查工作，严禁未授权数据出境行为；
- i) 应建立跨境数据的评估、审批及监管控制流程，并依据流程实施相关控制并记录过程。

7.6 公共数据退役

公共数据退役阶段要求如下：

- a) 应设立负责公共数据退役管理的岗位，由任职于该岗位的人员制定公共数据退役处置规范，明确公共数据转移、归档、销毁和删除要求，推动相关要求在业务部门落地实施；
- b) 应建立数据退役规程，明确数据退役场景、方式及审批机制，设置相关监督角色，记录数据退役操作过程；
- c) 应记录转移过程和转移的数据情况，保证数据转移过程的安全性、可靠性和可用性，确保转移数据的一致性、完整性；
- d) 可单独采用电子归档形式，应按国家和自治区有关规定对公共数据资源进行归档和登记备份；
- e) 应建立归档数据的压缩或加密策略，确保归档数据存储空间的有效利用和安全访问；
- f) 应建立归档数据的安全策略和管控措施，确保非授权用户不能访问归档数据；
- g) 应依照公共数据分类分级建立数据退役策略和管理制度，明确数据的退役对象、退役场景、退役方式和退役要求；
- h) 如因业务终止或组织解散，无数据承接方的，应及时有效销毁其控制的数据，法律、法规另有规定的除外；
- i) 委托数据合作方完成数据处理后，应要求数据合作方及时销毁委托的相关数据，法律、法规另有规定或者双方另有约定的除外；
- j) 根据要求、约定删除数据或完成数据处理后无需保留源数据的，应及时删除相关数据；
- k) 应按照GB/T 35273—2020中8.3规定的要求执行个人信息删除操作；
- l) 应按照相关的销毁介质标准和规定，确保不会对环境对人体造成潜在危害，对公共数据存储介质进行物理或化学销毁，以确保数据无法恢复。物理销毁常用的方法有消磁、捣碎和焚毁；化学销毁方法主要是滴盐酸法。
