ICS 35.020
CCS L80

DB3704

枣 庄 市 地 方 标 准

DB3704/T 0040-2024

公共数据安全管理规范

2024－ 03－27 发布　　2024－04 －27 实施

枣庄市市场监督管理局　　发布

目　次

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。

本文件由枣庄市大数据局提出、归口并组织实施。

本文件起草单位：枣庄市大数据中心、北京安华金和科技有限公司。

本文件主要起草人：王辉、陈夫真、赵瑞欣、陈亚楠、郗金鑫、郭腾、王俐、徐娟、雷嘉宾、赵善文。

本文件为首次发布。

公共数据安全管理规范

1 范围

本文件规定了公共数据在数据处理活动中的安全管理要求。

本文件适用于指导涉及公共数据采集、存储和使用的各单位进行数据安全管理能力建设，规范公共数据的使用。

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，仅该日期对应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 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 37964-2019 信息安全技术 个人信息去标识化指南

GB/T 39477-2020 信息安全技术 政务信息共享数据安全技术要求

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

国家机关，法律法规授权的具有管理公共事务职能的组织，具有公共服务职能的企业事业单位，人民团体等（以下统称公共数据提供单位）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。

3.2

数据安全

通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

3.3

网络安全

通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

3.4

数据处理活动

包括数据的采集、传输、存储、汇聚、使用、共享、开放等。

4 总体原则

为规范公共数据安全的基本要求，防范和抵御数据可能面临的各类安全风险，公共管理和服务机构在处理数据过程中，应遵循下列原则，具体包括：

a）合法正当原则：公共数据收集采取合法、正当的方式，不应窃取或者以其他非法方式获取数据，数据处理活动过程不应危害国家安全、公共利益，不应损害个人、组织的合法权益。

b）权责明确原则：采取技术和其他必要的措施保障数据的安全，对数据处理活动中涉及的组织和个人的合法权益负责。

c）目的明确原则：数据处理活动具有明确、清晰、具体的目的。

d）最小必要原则：数据处理活动仅处理可满足特定公共服务为目的所需的最少数据类型和数量。

e）公开透明原则：以明确、易懂和合理的方式公开个人信息处理的范围、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。

f）动态调整原则：数据安全等级随着数据对客体侵害程度的变化进行动态调整，数据重要程度、数据处理活动过程、数据安全管控措施等的变更可能引起数据对客体侵害程度的变化。

g）全程可控原则：采取必要管控措施确保数据处理活动各环节的可控性，防止未授权访问及处理公共数据，记录数据处理活动各环节过程，记录内容清晰可追溯。

5　通用安全能力

5.1　人员管理

图1　数据安全管理人员架构图

a）应设立数据安全管理机构，明确数据安全责任人，落实数据安全保护责任,负责公共数据的安全管理工作，应当加强人员管理，明确在人员培训、人员考核、保密协议、离岗离职、外部人员管理等方面的管理规定并严格落实。

b）数据安全管理机构应明确数据管理员、数据安全管理员、数据安全审计员等岗位职责，落实岗位人员，保障数据安全管理与审计工作开展。

5.2 人员职责

数据安全责任人：

负责组织制定数据保护计划并落实。

负责组织开展数据安全影响分析和风险评估，督促整改安全隐患。

负责组织按要求向有关部门报告数据安全保护和事件处置情况。

负责组织受理并处理数据安全投诉和举报事项等。

数据管理员：

负责管理数据的生命周期，包括数据的收集、存储、处理和分发；

负责确保数据的可靠性、完整性和安全性；

负责管理数据质量，确保数据的准确性和一致性；

数据安全管理员：

负责制定和执行数据安全策略和程序，确保数据的机密性、完整性和可用性；

负责管理访问控制、身份验证、加密、备份和恢复等数据安全措施；

数据安全审计员：

负责审核和评估组织的数据安全策略、程序和实践，确保其符合行业标准和法规要求；

负责评估数据安全风险和威胁，提出改进建议和解决方案；

负责监测和分析数据安全事件，及时采取措施防止和应对安全威胁；

a）大数据管理部门处理个人信息时，应指定个人信息保护负责人，负责对个人信息处理活动以及采取的保护措施等进行监督，并公开个人信息保护负责人联系方式，将个人信息保护负责人的姓名、联系方式等报送履行个人信息保护职责部门。

b）应针对数据类别级别变更、数据权限变更、重大数据操作及外部系统接入等事项建立审批程序，按照审批程序执行审批过程。

c)涉及数据合作方的机构，应与数据合作方签订合作协议及数据安全保密协议，明确双方数据安全保密责任与义务，宜定期审核数据合作方资质背景、数据安全保障能力等，并组织动态合规评估。

5.3 委托处理

a）大数据管理部门组织企业和其他机构等受托方建设、维护信息系统或者存储、加工数据等场景时，应当对受托方的数据安全保护能力、资质进行核实，并与受托方签订保密协议，并要求其签订安全承诺书，明确相关安全责任不随委托关系转移，监督并定期检查受托方履行数据安全保护义务情况。

b)要组织受托方与相关服务单位和人员签订保密协议。

c)要严格管控数据的权限管理，禁止受托方接触、处理批量原始数据，做好其操作行为的日志记录与风险预警，确保受委托方不擅自留存、使用、泄露、销毁或者向他人提供数据。

d)受委托方承建、运维信息系统的用户超过100万人时，社会管理和公共服务机构应提供数据安全保护措施和评估措施方案，并将评估情况报同级网信部门。

5.4 安全评估

a）应结合自身数据安全要求，制定数据安全风险评估方法，明确风险评估目的、范围、依据、评估流程、评估频率、实施评估、综合评估分析等内容。

b）在出现法律、资产、业务等方面重大情况变化时应进行局部或全面数据安全风险评估，形成数据安全风险评估报告。

c）涉及国家、行业存在数据安全合规监管要求的机构，应定期开展数据安全合规性评估，并向有关主管部门报送合规性评估报告。

d）涉及敏感个人信息处理活动时，应事先开展个人信息保护影响评估，评估记录至少保存五年。

5.5 应急响应

a）预案制定。各级应当制定数据安全事件应急预案，发生安全事件时，应当按照应急预案及时开展应急处置；事件处置完成后，应当在规定期限内形成总结报告，报送同级部门。

b）应急演练。各级应当根据应急预案定期开展应急演练，保存演练记录，针对演练中发现的问题，应当立即进行整改，发现安全隐患时，应当立即停止使用数据。

c)应根据应急预案明确的数据安全事件场景定期开展应急演练，检验和完善应急处置机制，每年至少一次，事件场景包括但不限于数据泄露、丢失、滥用、篡改、毁损、违规使用等。

5.6 网络安全

支撑公共数据处理活动的基础网络、云平台系统、资源共享网站等基础设施的通用安全要应符合GB/T 22239—2019中的第三级安全要求。

6 数据生命周期管理

6.1 数据采集

a）大数据管理部门应按照“最小必要”原则采集数据，保障被收集人的合法权益。采集过程中应采取相关安全防护措施和技术手段，确保环境、设施、人员等安全可控。

b）大数据管理部门应明确数据分类分级原则、方法和操作指南，对公共数据进行分类分级管理。

c）大数据管理部门进行数据采集活动，应明确数据采集的渠道和外部的数据源，并对外部数据源的合法性进行确认。

d)数据采集中若涉及个人信息，应明确数据采集过程中个人信息和重要数据的知悉范围和需要采集的控制措施，确保采集过程中的个人信息和重要数据不被泄露。

e）大数据管理部门进行数据采集活动，应明确数据质量管理相关的要求；明确数据采集过程中质量监控规则、明确数据质量监控范围及监控方式。

6.2 数据传输

a）数据传输活动应当根据传输的数据类型、级别和应用场景，制定安全策略并采取保护措施。数据传输过程中应当采取必要的安全技术措施保障数据传输安全、可控、及时、高效。

b）应对关键的网络传输链路、网络设备节点实行冗余建设。

c）应制定组织的网络可用性管理指标，包括可用性的概率数值、故障时间/频率/统计业务单元等。基于可用性管理指标，建立网络服务配置方案和宕机替代方案等。

6.3 数据存储

a)数据存储不应因存储形式或存储时效的改变而降低安全保护强度。

b)应根据安全级别、重要性、量级、使用频率等因素，将数据分域分级存储。

c）数据应存储至统一平台，原则上不得在产生、使用数据的相关业务系统之外存储。数据存储应

采取脱敏、加密、访问控制等安全措施。数据应依托政务云平台或信息系统开展容灾备份，建立数据恢复机制，及时开展数据恢复演练。

d）应明确数据逻辑存储隔离授权与操作要求，确保具备多用户数据存储安全隔离能力。

6.4 数据汇聚

a）社会管理和公共服务机构应根据数据资源目录，将本单位所有可汇聚的相关数据汇聚至市级一体化大数据平台，并负责数据及时更新；对不予汇聚的数据，应提出法律法规依据，并作出书面说明。

b）数据要在完成采集后，采用系统对接等方式及时进行汇聚。

6.5 数据使用

6.5.1 数据分析

a）应设立负责数据分析安全的岗位和人员，负责整体的数据分析安全原则制定、提供相应技术支持。

b）应明确数据处理与分析过程的安全规范，覆盖构建数据仓库、建模、分析、挖掘、展现等方面的安全要求，明确个人信息保护、数据获取方式、访问接口、授权机制、分析逻辑安全、分析结果安全等内容。

c）应明确数据分析安全审核流程，对数据分析的数据源、数据分析需求、分析逻辑进行审核，以确保数据分析目的、分析操作等当面的正当性。

d）在针对个人信息的数据分析中，数据分析者应采用多种技术手段以降低数据分析过程中的隐私泄露风险。

6.5.2 数据使用

应明确数据使用的评估制度，所有个人信息和重要数据的使用应先进行安全影响评估，满足国家合规要求后，允许使用。数据的使用应避免精确定位到特定个人，避免评价信用、资产和健康等敏感数据，不得超出与收集数据时所声明的目的和范围。

6.5.3 数据处理环境

a）公共数据处理环境的系统设计、开发和运维阶段应制定相应的安全控制措施，实现对安全风险的管理。

b）应基于数据处理环境建立分布式处理安全要求，对外部服务组件注册与使用审核、分布式处理节点间可信连接认证、节点和用户安全属性周期性确认、数据文件标识和用户身份鉴权、数据副本节点更新检测及防止数据泄露等方面进行安全要求和控制。

6.5.4 数据展示

a）数据展示前，应事前评估展示需求，包括展示的条件、环境、权限、内容等，确定展示的必要性和安全性。

b）涉及到个人信息的对外展示，应遵循GB/T 37964-2019 要求执行。

6.5.5 数据应用

社会管理和公共服务机构应对采集汇聚的数据提供数据应用，挂载到统一平台相关数据资源目录下，并做好运维服务。统一平台提供接口共享和批量共享两种应用方式。接口共享方式，用于数据单

条查询或校核对比；批量共享方式，用于依托统一平台，在保证数据安全基础上进行批量数据导出或脱敏数据导出。鼓励各级依托统一平台建立数据综合分析支撑能力，探索采用“多租户”等模式，由使用数据的社会管理和公共服务机构在统一平台上构建算法模型，开展批量数据应用，获取结果数据。

6.6 数据共享

a）在进行数据共享前，应明确数据共享内容范围和数据共享的管控措施，及数据共享涉及单位或部门相关用户职责和权限。

b）在个人信息委托处理、共享、转让等对外提供的场景下，应采用如数据脱敏、数据加密、安全通道、共享交换区域等手段保证数据共享的安全性能。

c）应对共享数据及数据共享过程进行监控审计，共享的数据应属于共享业务需求且没有超出数据共享使用授权范围。

d）公共数据共享过程中的安全技术保障措施可参考GB/T 39477-2020要求进行建设。

6.7 数据开放

a）在开放数据时需要确保数据的安全性和隐私保护。敏感个人信息和商业机密等不应公开，需要进行脱敏处理或采取其他措施保护隐私。

b）公共数据开放主体在日常监督管理过程中发现开放的公共数据存在安全风险的，应当立即采取中止、撤回开放等措施。