ICS 35.240.01
CCS L 67

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 271—2022

公共数据安全要求

Requirements for common data security

2022-11-14 发布　　2022-12-01 实施

深圳市市场监督管理局　　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。

本文件由深圳市政务服务数据管理局提出并归口。

本文件起草单位：深圳市信息安全管理中心、全知科技（杭州）有限责任公司、金砖国家未来网络研究院中国分院、深圳市智慧城市科技发展集团有限公司、华为技术有限公司、蚂蚁科技集团股份有限公司。

本文件主要起草人：李苏、董安波、林宇群、穆端端、轩豪男、赵剑、方兴、周顿科、魏凤玲、姚冬炎、董亮、宫昊、林桢、刘慧洋、王志、常新苗、白晓媛。

公共数据安全要求

1 范围

本文件规定了公共数据安全要求，主要包括总体安全原则和要求、总体框架、数据分级方法、通用管理安全要求、通用技术安全要求及数据处理活动安全要求。

本文件适用于公共管理和服务机构数据安全能力的建设、评估与监管，也适用于处理大量个人信息的服务平台数据安全能力的建设与评估。

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 20984—2022 信息安全技术 信息安全风险评估方法

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求

GB/T 39786—2021 信息安全技术 信息系统密码应用基本要求

3 术语和定义

GB/T 35273—2020、GB/T 37988—2019界定的以及下列术语和定义适用于本文件。

3.1

公共数据 common data

公共管理和服务机构及处理大量个人信息的服务平台在依法履行公共管理职责或者提供公共服务过程中产生、处理的数据。

注：本文件提及的数据均指公共数据。

3.2

数据安全 data security

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

公共管理和服务机构 public administration and service institutions

本市国家机关、事业单位和其他依法管理公共事务的组织，以及提供教育、卫生健康、社会福利、供水、供电、供气、环境保护、公共交通和其他公共服务的组织。

3.4

敏感个人信息 personal sensitive information

一旦泄露、非法提供或滥用有可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。

注1：敏感个人信息包括公民身份号码、个人生物特征信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

注2：个人信息处理者通过个人信息或其他信息加工处理后形成的信息，如一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息，也属于敏感个人信息。

[来源：GB/T 25069—2022，3.195，有修改]

3.5

重要数据 key data

一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据。

注：包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

[来源：GB/T 41479—2022，3.9，有修改]

3.6

匿名化 anonymization

公共数据中涉及的个人信息经过处理无法识别特定自然人且不能复原的过程。

3.7

数据合作方 data cooperator

与公共管理和服务机构进行业务合作、提供技术支撑和数据服务等，并可能接触到公共数据的外部单位。

3.8

安全多方计算 secure multi-party computation

在无可信第三方的情况下，各方约定一个安全计算函数，确保计算过程中各方数据安全的同时，得到预期计算的结果。

3.9

第三方应用 third party application

第三方提供的产品或服务，以及被接入或嵌入公共管理和服务机构产品或服务中的自动化工具。

注：包括但不限于软件开发工具包、第三方代码、组件、脚本、接口、算法模型、小程序等。

[来源：GB/T 41479—2022，3.12，有修改]

4 总体安全原则和要求

4.1 总体安全原则

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) 明示同意原则：数据相关主体拥有对其个人信息的处理目的、方式、范围等规则的知情权，在进行数据处理活动前应向数据相关主体明示，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：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；
f) 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；
g) 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；
h) 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。

4.2 总体安全要求

承载公共数据的信息系统应按GB/T 22239—2019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；数据处理过程涉及的密码技术应按GB/T 39786—2021描述的密码应用基本要求执行。

5 总体框架

5.1 总体框架图

总体框架如图1所示。

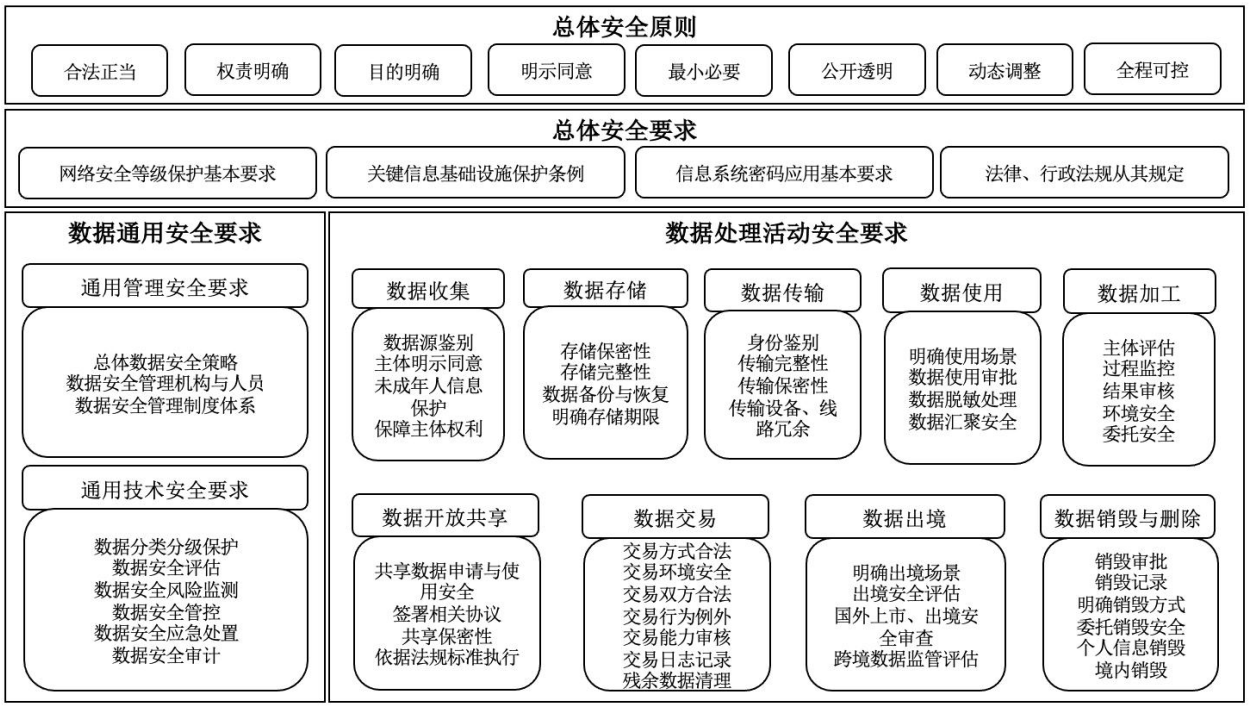


图1 总体框架

5.2 安全要求类别

在总体安全要求基础上，公共数据安全要求由如下两大类构成：

a) 数据通用安全要求：明确通用管理安全要求及通用技术安全要求，从管理及技术角度分级阐述公共数据安全要求；

b) 数据处理活动安全要求：数据处理活动围绕数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据交易、数据出境、数据销毁与删除9个过程，分级阐述公共数据安全要求。

6 数据分级方法

6.1 分级概述

公共管理和服务机构应对数据进行分类管理，在数据分类基础上，根据数据在经济社会发展中的重要程度，以及一旦遭到篡改、破坏、泄露或者被非法获取、非法利用，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的损害程度，对数据分级。

6.2 确定定级对象

数据定级对象应包括数据库和数据子类，也可为数据子类下的具体数据字段。数据定级对象分级方法不适用于半结构化及非结构化数据。

6.3 定级要素

数据定级对象的定级要素包括：

a) 受侵害的客体；

b) 对客体的侵害程度。

6.3.1 受侵害的客体

数据定级对象受到破坏所侵害的客体包括以下三个方面：

a) 个人信息主体及公共管理和服务机构的合法权益；

b) 社会秩序和公共利益；

c) 国家安全。

6.3.2 对客体的侵害程度

对客体的侵害程度应根据数据定级对象遭受篡改、破坏、泄露或者被非法获取、非法利用时，涉及的数据类型、数据量、数据影响面综合判定。对客体造成的侵害程度归结为以下四种：

a) 无损害；

b) 一般损害；

c) 严重损害；

d) 特别严重损害。

6.4 定级要素与等级关系

应对业务系统的数据库、数据子类或数据字段分别定级；针对业务系统的数据库，按照GB/T 22240—2020中4.3规定的定级要素及安全保护等级的关系，以及6.1规定的业务信息安全定级方法，参照表1定级，形成业务系统数据库清单，相关示例见表A.1；数据子类或数据字段定级要素与等级关系应符合附录B的规定。

表1　数据库定级要素与安全等级关系

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
个人信息主体及公共管理和服务机构的合法权益	第一级	第二级	第二级
社会秩序和公共利益	第二级	第三级	第四级
国家安全	第三级	第四级	第五级

6.5　定级步骤

数据对象定级步骤依据图2。

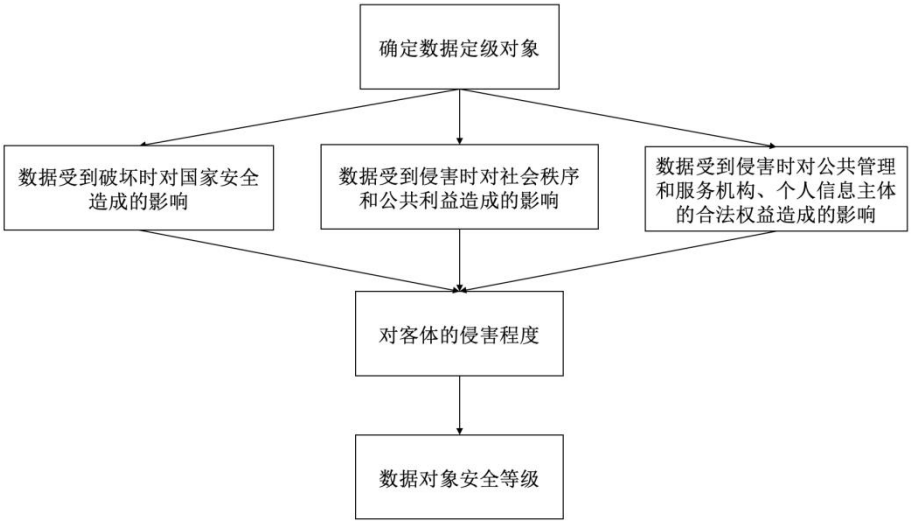


图2　数据对象定级步骤

6.6　级别变更

数据处理活动过程中，数据级别发生变更的，应及时对变更后数据重新级别判定，数据级别可能发生变更的场景包括但不限于数据汇聚融合、加工、脱敏、超过时效等。

6.7　级别要求

当不同级别的数据同时被处理且无法精细化管控时，应“就高不就低”，按照数据对象安全等级最高的要求实施保护。数据库安全等级与其安全要求的对应关系见表2，数据子类或数据字段安全等级与其安全要求的对应关系应符合附录B的规定。

表 2　数据库安全等级与安全要求关系

数据库安全等级	安全要求
第一级	基本安全要求
第二级	基本安全要求
第三级	基本安全要求、三级增强安全要求
第四级	基本安全要求、三级增强安全要求、四级增强安全要求
第五级	第五级为非常重要的监督管理对象，其安全要求不在本文件描述

7　通用管理安全要求

7.1　总体数据安全策略

7.1.1　基本安全要求

应明确数据安全管理的策略，包括管理目标、原则、要求等内容，制定或修订完善总体安全管理框架，公共数据安全管理应作为重点内容，纳入总体安全管理范畴。

7.1.2　三级增强安全要求

应定期对数据安全策略的合理性及适用性进行论证和审定，动态调整。

7.1.3　四级增强安全要求

四级无增强安全要求。

7.2　数据安全管理机构与人员

7.2.1　基本安全要求

7.2.1.1　机构管理

机构管理包括如下要求：

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；
b)　应按照相关法律、法规、规章的要求编制公共数据资源目录，加强数据安全保护；
c)　数据安全责任人履行职责包括但不限于：
　　1)　组织制定数据保护计划并落实；
　　2)　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；
　　3)　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；
　　4)　组织受理并处理数据安全投诉和举报事项等。

d) 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。相关岗位职责应包括：
   1) 数据管理员负责数据存储、数据权限分配、数据资产梳理等；
   2) 数据安全管理员负责数据权限审批、数据分类分级、数据安全风险检测与评估、数据安全事件应急响应处置、教育培训等，可由安全管理员兼任；
   3) 数据安全审计员负责数据安全审计等。
e) 处理个人信息达到国家网信部门规定数量的，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；
f) 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；
g) 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。

7.2.1.2 人员管理

人员管理包括如下要求：

a) 应加强人员管理，明确规定人员录用、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管理要求并严格落实；
b) 应与内部数据岗位人员、数据合作方人员签订保密协议，明确数据访问范围、操作权限、人员调离岗保密要求、保密期限、违约责任等，有效约束操作行为；
c) 应制定数据安全培训计划，定期组织数据安全培训工作，每年至少一次；针对机构全员，培训内容包括但不限于数据安全意识、法律法规等；针对数据岗位人员，培训内容包括但不限于标准规范、技能培训、应急响应、应急演练等，留存培训记录；
d) 宜组织数据岗位人员考取相关资质证书，持证上岗。

7.2.2 三级增强安全要求

7.2.2.1 机构管理

机构管理包括如下要求：

a) 应针对重大数据处理活动建立逐级审批机制；
b) 应定期审查审批事项，及时更新需授权和审批的项目、审批部门和审批人等信息。

7.2.2.2 人员管理

人员管理包括如下要求：

a) 应配备专职安全管理员承担数据安全管理员工作；
b) 应针对不同数据岗位制定不同的培训计划，对数据安全基础知识、岗位操作规程等进行培训；
c) 应定期对不同数据岗位人员进行技能考核。

7.2.3 四级增强安全要求

7.2.3.1 机构管理

四级无增强安全要求。

7.2.3.2 人员管理

人员管理包括如下要求：

a) 关键事务岗位应配备多人共同管理；
b) 应从内部人员中选拔从事关键数据岗位的人员。

7.3 数据安全管理制度体系

7.3.1 基本安全要求

数据安全管理制度体系包括如下要求：

a) 应指定专门的部门或授权数据安全管理机构负责数据安全管理制度的制定；
b) 应建立健全数据安全保护制度体系，制度体系内容包括但不限于数据安全政策、组织机构与人员管理、数据分类分级、数据安全评估、数据安全风险监测、数据访问权限管控、数据安全应急与处置、数据安全审计、数据活动安全管理要求（包括数据收集、存储、传输、使用、加工、开放共享、交易、出境、销毁等）、数据安全教育培训、数据合作方管理、个人信息安全保护等；
c) 提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督；
d) 应建立投诉、举报受理处置制度，收到通过其平台编造、传播虚假信息，发布侵害他人名誉、隐私、知识产权和其他合法权益信息，以及假冒、仿冒、盗用他人名义发布信息的投诉、举报，自接受投诉举报起，受理时间不超过3天，受理后进行调查取证，一经查实，应依法采取停止传输、消除等处置措施；
e) 应建立个人信息主体保护权利的渠道和机制，及时响应个人信息主体查阅、复制、更正、删除其个人信息及注销账号的请求，按照GB/T 35273—2020中8.7规定的要求响应个人信息主体的请求，不应对请求设置不合理条件；
f) 应通过正式、有效的方式发布数据安全管理制度，并进行版本控制；
g) 应定期对数据安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。

7.3.2 三级增强安全要求

应形成由安全策略、管理制度、操作规程、记录表单等构成的全面的数据安全管理制度体系。

7.3.3 四级增强安全要求

四级无增强安全要求。

8 通用技术安全要求

8.1 数据分类分级保护

8.1.1 基本安全要求

数据分类分级保护包括如下要求：

a) 应结合数据资产识别技术手段，梳理数据资产，并明确数据资产类型、数据量、存储位置、数据关联系统、数据共享情况、数据出境情况等；

b) 应明确数据分类标准，依据数据资源属性特征，将数据合理划分类别，形成数据资源分类目录，相关示例见附录C；
c) 应明确数据对象安全等级，依据数据一旦遭到篡改、破坏、泄露或者非法获取、非法利用时，对国家安全、社会秩序和公共利益或者个人信息主体、公共管理和服务机构合法权益造成的侵害程度确定安全等级，常见个人信息分类分级相关示例见附录D；
d) 应在数据分类分级基础上，形成数据资产清单，相关示例见附录A，落实不同数据安全等级差异化防护措施要求；数据库安全等级差异化防护要求依据本文件第7至9章落实执行，数据子类或数据字段安全等级差异化防护措施应符合附录B的规定；
e) 应定期评审数据对象的类别和级别，如需变更数据所属类型或级别，应依据变更审批流程执行变更。

8.1.2 三级增强安全要求

应采取数据安全防护措施，对重要数据和敏感个人信息进行重点保护。

8.1.3 四级增强安全要求

应建立数据资产识别技术能力，对数据对象进行标记与跟踪，构建数据血缘关系。

8.2 数据安全评估

8.2.1 基本安全要求

数据安全评估包括如下要求：
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) 在出现法律法规重大更改或增删、业务活动发生重大变化、数据资产发生重大变化、发生重大数据安全事件、数据安全管理方针发生变化等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、个人信息自动化决策、委托处理、他人提供（含境外）、公开、其他对个人权益有重大影响的个人信息处理活动等，应事先开展个人信息保护影响评估，评估记录至少保存三年。

8.2.2 三级增强安全要求

应定期开展数据安全自评估工作，涉及处理敏感个人信息及国家规定的重要数据的机构，应按照有关规定定期开展风险评估，并向有关主管部门报送风险评估报告，风险评估报告应包括处理的重要数据种类、数量，开展数据处理活动的情况，面临的数据安全风险以其应对措施等。

8.2.3 四级增强安全要求

四级无增强安全要求。

8.3 数据安全风险监测

8.3.1 基本安全要求

数据安全风险监测包括如下要求：

a) 应具备常态化数据安全风险监测能力，持续监测数据安全风险，风险类型包括但不限于账号风险、权限风险、异常操作行为、数据出境风险、数据暴露面风险等；
b) 应加强数据安全风险闭环管理，持续提升数据安全风险处置能力。

8.3.2 三级增强安全要求

数据安全风险监测包括如下要求：
a) 应建立数据安全风险监测预警机制，制定合理有效的风险监测指标；
b) 应对数据安全事件和可能引发数据安全事件的风险隐患进行收集、分析判断和持续监控预警，建立数据安全监测预警流程，有效保障业务系统所承载数据资产的机密性、完整性、可用性；
c) 应配备专人负责数据安全风险监测工作，定期出具风险监测报告；
d) 应定期对数据安全风险监测工作的有效性、全面性进行审核验证。

8.3.3 四级增强安全要求

四级无增强安全要求。

8.4 数据安全管控

8.4.1 基本安全要求

8.4.1.1 数据访问权限管控

数据访问权限管控包括如下要求：
a) 应根据不同数据级别，明确数据管理、审计类账号权限开通、分配、使用、变更、注销等安全管理要求，账号关联对象包括机构内部及数据合作方人员；
b) 应对账号及对应权限进行记录，并在账号或权限发生变更时及时更新，重点关注离职人员账号回收、管理权限变更、沉默账号、复活账号；
c) 应严格控制账号访问、操作权限，明确账号权限审批流程；
d) 应对账号进行统一身份认证、操作行为记录；
e) 应对业务系统之间的数据访问采取身份鉴别、访问控制、安全审计、资源控制等技术措施；
f) 应对数据批量下载、上传、删除、共享和销毁等重大操作行为设置内部审批流程，并记录操作行为。

8.4.1.2 数据防泄露管控

应在网络层面对数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警。

8.4.1.3 数据接口管控

数据接口管控包括如下要求：
a) 应在数据接口调用前进行身份鉴别，通过技术手段限制非白名单接口接入；
b) 应对数据接口定期开展安全检测，及时发现并处置数据安全风险隐患；
c) 应对数据接口实施调用审批流程，对接口调用行为进行日志记录；
d) 应定期梳理数据接口，形成接口清单。

8.4.2 三级增强安全要求

8.4.2.1 数据访问权限管控

应对数据跨网络区域传输采取安全管控措施，包括但不限于网络及应用层的访问控制策略，控制粒度为端口级。

8.4.2.2 数据防泄露管控

应在终端层面对数据流转、泄露和滥用情况进行监控，及时对异常数据操作行为进行预警，并在网络层面实现对异常数据操作行为及时定位和阻断。

8.4.2.3 数据接口管控

数据接口管控包括如下要求：

a) 应对异常数据接口调用行为实现自动预警、拦截功能；
b) 应对开放数据接口的平台相关接口数据交互行为进行监测，对接口数据交互行为进行日志记录；
c) 应建立数据接口全生命周期管理机制，形成接口清单，动态更新接口活动状态，如新增、活跃、失活、复活、下线等接口状态，并采取安全管控措施。

注：开放数据接口的平台包括但不限于数据开放平台、数据共享交换平台、数据交易平台、大数据平台、能力开放平台。

8.4.3 四级增强安全要求

8.4.3.1 数据访问权限管控

应基于数据分级分类结果配置主体对客体的访问控制策略，访问控制粒度应达到主体为用户级或进程级，客体为接口、应用功能、文件、数据库表级等。

8.4.3.2 数据防泄露管控

应在终端层面对异常数据操作行为及时定位和阻断。

8.4.3.3 数据接口管控

四级无增强安全要求。

8.5 数据安全应急处置

8.5.1 基本安全要求

数据安全应急处置包括如下要求：

a) 应建立数据安全应急处置机制，依据本市、本区、本行业网络安全事件应急相关文件开展应急处置工作；
b) 发生数据泄露、毁损、丢失、篡改等数据安全事件时应立即启动应急预案，采取相应的应急处置措施，及时告知相关权利人，并按照有关规定向市网信、公安部门和有关行业主管部门报告；
c) 数据安全应急处置后应分析事件发生原因，总结应急处置经验，调整数据安全策略，形成事件调查记录和总结报告，避免再次发生类似情况；
d) 发生个人信息泄露、毁损、丢失等数据安全事件，或发生数据安全事件风险明显加大时，应立即采取补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体，并主动报告有关主管部门，必要时应向市网信部门报告；
e) 应采取技术手段对数据安全事件的日志或流量关联分析进行溯源，造成严重事件的应依法追究事件主体责任；

f） 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。

8.5.2 三级增强安全要求

数据安全应急处置包括如下要求：

a） 应跟踪和记录数据收集、分析、加工、挖掘等过程，保证在发生事件时溯源数据能重现相应过程；

b） 关键信息基础设施系统数据在发生重要数据泄露、较大规模个人信息泄露时，应及时上报关键信息基础设施安全保护工作部门。

8.5.3 四级增强安全要求

应采取技术手段保证数据处理活动的溯源数据真实性和保密性。

8.6 数据安全审计

8.6.1 基本安全要求

数据安全审计包括如下要求：

a） 应制定数据安全审计制度，审计覆盖面包括数据收集、数据存储、数据传输、数据使用、数据加工、数据开放共享、数据销毁与删除等数据处理活动各环节，明确审计策略、审计对象、审计内容、审计周期、审计结果、审计问题跟踪等要求；

b） 应对数据处理活动环节实施日志留存管理，日志记录至少包括时间、IP地址、操作账号、操作内容、操作结果等，在发生安全事件时可提供溯源取证能力，日志保存时间不少于180天；

c） 应定期对数据处理活动各环节日志进行数据安全审计，每年至少一次，形成数据安全审计报告。

8.6.2 三级增强安全要求

应定期对数据账号操作及接口调用情况进行安全审计。

8.6.3 四级增强安全要求

四级无增强安全要求。

9 数据处理活动安全要求

9.1 数据收集

9.1.1 基本安全要求

数据收集包括如下要求：

a） 应对数据收集来源进行鉴别和记录，确保数据收集来源的合法性、正当性，明确数据类型及收集渠道、目的、用途、范围、频度、方式等；

b） 收集外部机构数据前，应对外部机构数据源的合法性、合规性进行鉴别；

c） 个人信息收集应遵循合法、正当、必要和诚信原则，并获得个人信息主体的明示同意，不应通过误导、欺诈、胁迫或者其他违背个人信息主体真实意愿的方式获取其同意；

d） 应按照GB/T 35273—2020中5.1至5.6规定的要求开展个人信息收集工作；

e） 提供公共服务的移动互联网应用程序或第三方应用，应遵循最小化收集原则，不应因个人信息主体不同意收集非必要个人信息，而拒绝个人信息主体使用移动互联网应用程序或第三方应用。

9.1.2 三级增强安全要求

收集外部机构数据前，应对数据收集过程中的网络环境、系统进行安全评估，确保收集数据的机密性、完整性和可用性。

9.1.3 四级增强安全要求

四级无增强安全要求。

9.2 数据存储

9.2.1 基本安全要求

数据存储包括如下要求：

a） 应明确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；
b） 应明确数据备份与恢复安全策略，建立数据备份恢复操作规程，说明数据备份周期、备份方式、备份地点；建立数据恢复性验证机制，保障数据的可用性与完整性；
c） 应提供异地数据备份功能，利用通信网络将数据定时批量传送至备用场地；
d） 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；
e） 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。

9.2.2 三级增强安全要求

数据存储包括如下要求：

a） 应提供异地实时备份功能，利用通信网络将数据实时备份至备份场地；
b） 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；
c） 应提供数据处理环节关联信息系统的热冗余，保证数据的高可用性。

9.2.3 四级增强安全要求

应建立异地灾难备份中心，提供数据的实时切换。

9.3 数据传输

9.3.1 基本安全要求

数据传输包括如下要求：

a） 应明确数据传输相关安全管控措施，如传输通道加密、数据内容加密、数据接口传输安全等；
b） 应对数据传输两端进行身份鉴别，确保数据传输双方可信任；
c） 应采用校验技术保证数据在传输过程中的完整性。

9.3.2 三级增强安全要求

数据传输包括如下要求：

a) 应对关键网络传输线路及核心设备实施冗余建设，确保数据传输的网络可用性；
b) 重要数据不应通过离线或即时通信方式传输。

9.3.3 四级增强安全要求

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。

9.4 数据使用

9.4.1 基本安全要求

数据使用包括如下要求：

a) 应明确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，开展数据利用；
b) 应明确数据统计分析、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) 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；
e) 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；
f) 利用所掌握的数据资源，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。

9.4.2 三级增强安全要求

数据使用包括如下要求：

a) 应采取技术措施保证汇聚大量数据时不暴露敏感信息；
b) 宜对不同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；
c) 宜对接入或嵌入的第三方应用加强数据安全管理，宜对接入或嵌入的第三方应用开展技术检测，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。

9.4.3 四级增强安全要求

四级无增强安全要求。

9.5 数据加工

9.5.1 基本安全要求

数据加工包括如下要求：

a) 应对参与数据加工活动的主体进行合法性、正当性的评估，确保参与数据加工活动的主体为合法合规的组织机构或个人；
b) 应在数据加工前，书面明确数据加工目的、范围、期限、规则及数据加工主体的责任与义务；
c) 开展数据加工活动过程中，知道或应知道可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止加工活动；

d) 委托他人加工处理数据的，应与其订立数据安全保护合同，明确双方安全保护责任；委托加工处理个人信息的，应约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等，并对受托人的个人信息处理活动进行监督，不应超出已征得个人信息主体授权同意的范围。

9.5.2 三级增强安全要求

数据加工包括如下要求：

a) 应对数据加工的过程进行评估与监控，对数据加工过程的数据操作行为进行记录、审计，对异常数据操作行为及时预警、处置；
b) 应对数据加工结果进行评估，如产生新数据，应对新数据进行安全审核，确保新数据不存在数据泄露风险；
c) 应提供安全的数据加工环境，包括网络环境、终端环境等，避免加工过程导致数据泄露、数据破坏等安全风险；
d) 加工重要数据的，应加强访问控制，建立登记、审批机制并留存记录。

9.5.3 四级增强安全要求

四级无增强安全要求。

9.6 数据开放共享

9.6.1 基本安全要求

数据开放共享包括如下要求：

a) 公共数据提供部门应与公共数据使用部门签署相关协议，明确数据使用目的、供应方式、保密约定、数据共享范围、数据安全保护要求等内容；
b) 公共数据提供部门应采用国家相关标准规定的密码技术，保障数据共享过程的保密性和完整性；
c) 政务信息资源交换平台的政务信息共享应履行GB/T 39477—2020第6章确定的共享数据安全要求。

9.6.2 三级增强安全要求

数据开放共享包括如下要求：

a) 公共数据提供部门应建立内部审批机制，明确数据对外共享目的、范围、期限、频次等内容；
b) 公共数据提供部门宜对共享的数据采取数字水印等技术，确保共享数据可溯源；
c) 宜采用多方安全计算、同态加密等数据隐私计算技术实现数据共享的安全性。

9.6.3 四级增强安全要求

四级无增强安全要求。

9.7 数据交易

9.7.1 基本安全要求

应按照相关法律、法规、规章的要求开展数据交易，加强交易过程的数据安全保护。

9.7.2 三级增强安全要求

三级无增强安全要求。

9.7.3 四级增强安全要求

四级无增强安全要求。

9.8 数据出境

9.8.1 基本安全要求

数据出境包括如下要求：

a) 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；
b) 境内用户在境内访问境内网络的，其流量不应路由至境外；
c) 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。

9.8.2 三级增强安全要求

三级无增强安全要求。

9.8.3 四级增强安全要求

四级无增强安全要求。

9.9 数据销毁与删除

9.9.1 基本安全要求

数据销毁与删除包括如下要求：

a) 应建立数据销毁与删除规程，明确数据销毁与删除场景、方式及审批机制，设置相关监督角色，记录数据销毁与删除操作过程；
b) 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；
c) 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；
d) 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；
e) 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。

9.9.2 三级增强安全要求

数据销毁与删除包括如下要求：

a) 应在中国境内对介质存储的数据进行销毁或删除；
b) 应对存储数据的介质或物理设备采取无法恢复的方式进行数据销毁与删除，如物理粉碎、消磁、多次擦写等。

9.9.3 四级增强安全要求

四级无增强安全要求。

附 录 A
（资料性）
公共数据分类分级清单示例

业务系统（数据库）清单示例见表 A.1，数据资产分类分级（数据子类或数据字段）清单示例见表 A.2。

表 A.1 业务系统（数据库）清单示例

序号	平台系统名称	责任部门	数据库名称	IP 地址	端口号	数据库版本信息	大小	库表数量	表序号	表名称	安全等级
1	*示例：某政务系统*	*xx 部门*	*user_center*	*192.168.x.x*	*1521*	*Oracle 10*	*10GB*	*10*	1	*user*	*第二级*
	示例：某政务系统	*xx 部门*	*user_center*	*192.168.x.x*	*1521*	*Oracle 10*	*10GB*	*10*	2	*person_identity*	*第二级*

表 A.2 数据资产分类分级（数据子类或数据字段）清单示例

序号	数据子类类型	数据字段名称	数据总量	分类分级（数据类别）	分类分级（数据级别）	存储位置（平台系统名称-数据库名称-表名）	是否涉及访问及导出	是否涉及数据共享	是否涉及出境	是否国家定义的重要数据
1	*示例：个人身份信息*	*person_id*	*50000*	*身份证*	*3 级*	*某政务系统-user_center-person_identity*	*是*	*是*	*否*	*否*
	示例：个人身份信息	*person_name*	*50000*	*姓名*	*3 级*	*某政务系统-user_center-person_identity*	*是*	*是*	*否*	*否*

附 录 B
（规范性）
公共数据子类或数据字段定级及级别要求

B.1 定级要素与等级关系

数据子类或数据字段作为定级对象，应依据表B.1定级，形成数据资产分类分级（数据子类或数据字段）清单。

表B.1 数据子类或数据字段定级要素与安全等级关系

数据定级要素		数据一般特征	对应级别
受侵害的客体	对客体的侵害程度		
国家安全	特别严重损害/严重损害/一般损害	• 数据子类或单一数据字段安全性遭到破坏，关联同一库表其它数据字段后可能对国家安全造成影响，对社会秩序和公共利益造成严重影响，对个人信息主体及公共管理和服务机构的合法权益造成特别严重影响。 • 个人信息主体涉及GB/T 35273—2020附录A、附录B中的“个人健康生理信息”、“个人生物识别信息”等。	4
社会秩序和公共利益	特别严重损害/严重损害		4
个人信息主体及公共管理和服务机构的合法权益	特别严重损害		4
社会秩序和公共利益	一般损害	• 数据子类或单一数据字段安全性遭到破坏，关联同一库表其它数据字段后可能对社会秩序和公共利益造成一般影响，或对个人信息主体及公共管理和服务机构的合法权益造成严重影响，但不影响国家安全。 • 个人信息主体涉及的GB/T 35273—2020附录A、附录B中的“个人基本资料”“、“个人身份信息”、“个人通信信息”、“个人位置信息”、“联系人信息”、“个人财产信息”、“其它信息”等。	3
个人信息主体及公共管理和服务机构的合法权益	严重损害		3
个人信息主体及公共管理和服务机构的合法权益	一般损害	• 数据子类或单一数据字段安全性遭到破坏，关联同一库表其它数据字段后可能对个人信息主体及公共管理和服务机构的合法权益造成一般影响，但不影响国家安全、社会秩序和公共利益。 个人信息主体涉及的GB/T 35273—2020附录A、附录B中的“个人教育工作信息”、“网络身份标识信息”“个人上网记录”、“个人常用设备信息”等。	2

表 B.1　数据子类/数据字段定级要素与安全等级关系（续）

数据定级要素		数据一般特征	对应级别
受侵害的客体	对客体的侵害程度		
国家安全	无损害	• 数据子类或单一数据字段一般是可公开的或可被公众获知、使用。 • 个人信息主体涉及的可公开或主动公开的信息。	1
社会秩序和公共利益	无损害		1
个人信息主体及公共管理和服务机构的合法权益	无损害		1

B.2 级别要求

应根据公共数据子类或数据字段不同安全等级要求，依据表 B.2 采取差异化防护措施，如无法对具体数据字段采取精细化管控，可对关联数据子类中的所有数据字段采取统一管控措施。

表 B.2 公共数据子类或数据字段安全等级与安全要求关系

处理活动	级别要求			
	4 级	3 级	2 级	1 级
数据收集	• 通过 API 或 SDK 方式收集数据字段前，应进行身份鉴别，并存储数据收集日志记录。 • 新建系统宜具备数据字段级别的分类分级功能模块，实现对收集的数据字段自动进行分类分级标识。	• 通过 API 或 SDK 方式收集数据字段前，应进行身份鉴别，并存储数据收集日志记录。 • 新建系统宜具备数据字段级别的分类分级功能模块，实现对收集的数据字段自动进行分类分级标识。	• 通过 API 或 SDK 方式收集数据字段前，应进行身份鉴别，并存储数据收集日志记录。 • 新建系统宜具备数据字段级别的分类分级功能模块，实现对收集的数据字段自动进行分类分级标识。	• 新建系统宜具备数据字段级别的分类分级功能模块，实现对收集的数据字段自动进行分类分级标识。
数据存储	• 应采用密码算法或哈希算法对数据字段进行加密或哈希存储，其中口令应采用加盐哈希存储。 • 应仅存储个人生物识别信息的摘要信息。 • 宜采用 DBMS 工具字段权限管理模块，合理化配置数据字段访问和使用权限，确保数据字段在合理范围内被查询和使用。	• 应采用密码算法或哈希算法对数据字段进行加密或哈希存储，其中口令应采用加盐哈希存储。 • 宜采用 DBMS 工具字段权限管理模块，合理化配置数据字段访问和使用权限，确保数据字段在合理范围内被查询和使用。	• 宜采用 DBMS 工具字段权限管理模块，合理化配置数据字段访问和使用权限，确保数据字段在合理范围内被查询和使用。	-

表 B.2　公共数据子类或数据字段安全等级与安全要求关系（续）

处理活动	级别			
	4 级	3 级	2 级	1 级
数据传输	• 应采用通道加密方式对数据字段进行传输。 • 宜在通道加密基础上，采用内容加密方式，对数据字段进行传输。 • 应对离线或即时通信方式传输的数据字段采取加密、脱敏等安全措施，确保传输安全性。	• 应采用通道加密方式对数据字段进行传输。 • 应对离线或即时通信方式传输的数据字段采取加密、脱敏等安全措施，确保传输安全性。	• 宜对离线或即时通信方式传输的数据字段采取加密、脱敏等安全措施，确保传输安全性。	-
数据使用	• 应在各类数据使用场景（如生产数据应用为测试数据、数据统计分析、数据对外展示、提供作为参赛数据等）中，采用动态或静态脱敏技术，对非必要使用的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 数据使用场景（如提供作为参赛数据）中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 应在各类数据使用场景（如生产数据应用为测试数据、数据统计分析、数据对外展示、提供作为参赛数据等）中，采用动态或静态脱敏技术，对非必要使用的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 数据使用场景（如提供作为参赛数据）中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 宜在各类数据使用场景（如生产数据应用为测试数据、数据统计分析、数据对外展示、提供作为参赛数据等）中，采用动态或静态脱敏技术，对非必要使用的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。	-
数据加工	• 应在数据加工场景中，采用动态或静态脱敏技术，对非必要加工的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 数据加工场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 应在数据加工场景中，采用动态或静态脱敏技术，对非必要加工的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 数据加工场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 宜在数据加工场景中，采用动态或静态脱敏技术，对非必要加工的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。	-

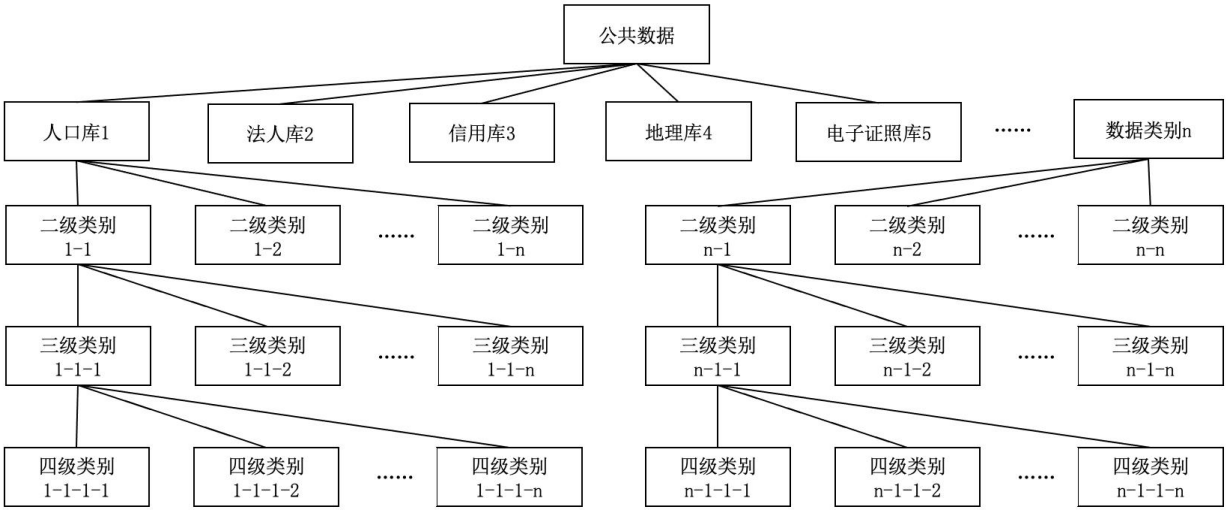
表 B.2　公共数据子类或数据字段安全等级与安全要求关系（续）

处理活动	级别			
	4 级	3 级	2 级	1 级
数据开放共享	• 应在数据开放共享场景中，采用动态或静态脱敏技术，对非必要共享的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 在数据开放共享场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 应在数据开放共享场景中，采用动态或静态脱敏技术，对非必要共享的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。 • 在数据开放共享场景中，如需实现数据可用不可见，宜采用隐私计算技术，例如多方计算、联邦学习等。	• 宜在数据开放共享场景中，采用动态或静态脱敏技术，对非必要共享的数据字段进行脱敏处理，脱敏方式包括变形、屏蔽、替换、随机化等，涉及静态脱敏工具或动态脱敏工具。	-
数据交易	• 应采用日志或流量采集技术全面采集、存储数据交易记录（syslog、kafka 等），确保数据交易的具体字段上下游链路清晰，各类数据字段交易过程可视可追溯。	• 应采用日志或流量采集技术全面采集、存储数据交易记录（syslog、kafka 等），确保数据交易的具体字段上下游链路清晰，各类数据字段交易过程可视可追溯。	• 宜采用日志或流量采集技术全面采集、存储数据交易记录（syslog、kafka 等），确保数据交易的具体字段上下游链路清晰，各类数据字段交易过程可视可追溯。	• 宜采用日志或流量采集技术全面采集、存储数据交易记录（syslog、kafka 等），确保数据交易的具体字段上下游链路清晰，各类数据字段交易过程可视可追溯。
数据出境	-	-	-	-
数据销毁与删除	• 应采用物理破坏的方式，对存储的数据字段进行数据销毁处理，确保数据不可恢复。	• 应采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不可恢复。	• 宜采用多次重写、覆盖、删除等方式对销毁数据字段进行擦除，确保数据不可恢复。	-

附 录 C
（资料性）
公共数据分类方法

C.1 分类方法及示例

公共数据分类可按照线分类法进行分类,公共管理和服务机构应收集内部所有业务系统的数据资源，梳理数据资源类别，依据线分类法，按照业务数据属性或特征，将公共数据按照基础库或其它库题分为若干大类，并根据类别及数据隶属关系，将每个大类的数据分为若干层级，同时每个层次也可分为若干子类，同一分支的同层级子类构成并列关系，不同层级子类之间构成隶属关系，最终形成数据资源目录树，如图C.1所示。



图C.1 公共数据分类示例

C.2 不同行业分类方法

公共数据各行业可依据其行业制定的分类分级标准开展数据分类分级工作，金融行业数据分类分级方法见JR/T 0171—2020、JR/T 0197—2020，基础电信企业分类分级方法见YD/T 3813—2020，其它行业暂无已发布的行业标准参考的，则可依据本文件的公共数据分类方法执行。

附 录 D
（资料性）
常见个人信息分类分级参考表

表D.1列举常见个人信息的分类分级情况，公共管理和服务机构可参考表D.1落实公共数据中涉及个人信息的分类分级工作。

表D.1 常见个人信息分类分级参考表

一级类别	二级类别	典型示例和说明	参考级别
个人信息	个人健康生理信息	指个人因生病医治等产生的相关记录，如：病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况相关的其他信息，如吸烟史等。	4
	个人生物识别信息	指辅助识别个人身份的生物信息，如： • 弱隐私生物特征信息，包括人脸、声纹、步态、耳廓、眼纹、笔迹等； • 强隐私生物特征信息，包括个人基因、指纹、掌纹、虹膜等。	4
	个人鉴别信息	指个人的金融用户鉴别信息，如： • 个人银行卡磁道（或芯片等效信息）、卡片验证码（CVN和CVN2）、卡片有效期、银行卡密码、网络支付交易密码； • 账户（包括但不限于支付账号、证券账户、保险账户）登录密码、交易密码、查询密码、USBKEY、U盾（网银、手机银行密保工具信息）等。	4
		指个人的其它用户鉴别信息，且泄露后不造成个人经济损失，但会对个人工作或生活造成影响，如： • 公共管理和服务机构对社会公众提供服务的网站涉及的用户鉴别信息，如社保、教育、交通、水电等相关系统； • 公共管理和服务机构内部系统涉及的用户鉴别信息，包括OA系统、邮件系统等用户鉴别信息。	3
	个人基本资料	指个人基本情况，如：个人姓名、生日、性别、民族、国籍、家庭关系、住址、电子邮件地址、婚姻状况等。	3
	个人身份信息	指个人的身份信息，如：身份证、军官证、护照、驾驶证、工作证、社保卡、居住证、港澳通行证、驾照编号等。	3
	个人通信信息	指个人的通信记录数据，如：通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据(通常称为元数据)等。	3
	个人位置信息	指能具体定位到个人的地理位置信息，如：行踪轨迹、精准定位信息、住宿信息、经纬度等常在位置和当前位置等信息。	3
	联系人信息	指个人各类通信联系方式数据，如：手机号码、固定电话、电子邮箱地址、微信号、QQ号等。	3

表 D.1　常见个人信息分类分级参考表（续）

一级类别	二级类别	典型示例和说明	参考级别
个人信息	联系人信息	指好友通信联系方式数据，如：通讯录、好友列表、群列表、电子邮件地址列表、微信群号等。	3
	未成年个人信息	指未满14周岁（含）的未成年人个人信息。	3
	个人关系信息	指个人与个人关联方关系的记录数据，如：子女、父母、兄弟姐妹、配偶、社交关系等。	3
		指个人与单位关联方关系的记录数据，如：法定代表人、财务负责人、业务经办人、一般雇员、高管人员等。	2
	个人财产信息	指个人的财产数据，如： • 个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额、个人社保、医保缴存金额等； • 银行账户、存款信息(包括资金数量、支付收款记录等)、信贷记录（如个人借款信息、还款信息、欠款信息等）、征信信息、交易和消费记录、流水记录等，以及虚拟货币、虚拟交易、游戏类兑换码等虚拟财产信息； • 用户鉴别辅助信息（如动态口令、短信验证码、密码提示问题答案、动态声纹密码）； • 金融产品与服务的关键信息，如交易信息（如交易指令、交易流水、证券委托、保险理赔）等。	3
		指金融业机构内部使用的个人金融信息，如：账户开立时间、开户机构、基于账户信息产生的支付标记信息。	2
	个人司法信息	指与未公开的个人违法犯罪记录。	3
		指公开的个人相关司法信息记录数，如：失信被执行人信息、被执行人信息、开庭公告信息、立案公告信息、犯罪记录、违法违规记录等。	2
	其他信息	指其他个人隐私信息，如；宗教信仰、性取向、私人生活信息等。	3
	个人教育工作信息	指个人受教育或职业情况的记录信息，如： • 入学日期、毕业日期、学号、就读学校名称、就读学校院系、学历、学位及学科信息、挂科情况、成绩单等； • 个人职业、职位、工作单位、职称、工作时间、工作地点、工作经历、培训记录等。	2
		指个人获得资质证书的记录信息，如：资质证书名称、证书等级、颁发机构、生效时间、到期时间等。	2
		指个人政治面貌相关数据，如：党派所属、加入时间、退出时间、党费缴纳记录等。	2
	网络身份标识信息	指个人的网络身份标识信息，如：个人信息主体账号、IP地址、个人数字证书等。	2

表 D.1　常见个人信息分类分级参考表（续）

一级类别	二级类别	典型示例和说明	参考级别
个人信息	个人上网记录	指通过日志储存的个人信息主体操作记录，如：网站浏览记录、软件使用记录、点击记录、收藏列表等。	2
	个人常用设备信息	指包括硬件序列号、设备MAC地址、软件列表、唯一设备识别码(如IMEI/AndroidID/IDFA/OpenUDID/GUID/SIM卡IMSI信息等)等在内的描述个人常用设备基本情况的信息。	2
	个人行为信息	指发生业务关系时的行为数据，如：描述用户通过社保局系统等咨询、办理社保业务时产生的数据，包括办理时间、地点、网页浏览记录、APP浏览记录等。	2
	个人用户画像	指基于个人的基本或关联属性构建的用户画像的标签数据，如：兴趣爱好标签、人物性格标签、购物喜好标签等。	2
	个人公开信息	指个人可对外公开或个人主动公开的信息，如：法定代表人公开基本信息（如姓名、股份占比、变更情况等）、社会公众用户发布的微博内容、微信朋友圈内容、网站注册用户昵称、互联网公开发布文章的数据等。	1

参 考 文 献

[1] GB/T 25069—2022 信息安全技术 术语

[2] GB/T 37932—2019 信息安全技术 数据交易服务安全要求

[3] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南

[4] GB/T 41479—2022 信息安全技术 网络数据处理安全要求

[5] JR/T 0171—2020 个人金融信息保护技术规范

[6] JR/T 0197—2020 金融数据安全 数据安全分级指南

[7] JR/T 0223—2021 金融数据安全 数据全生命周期安全规范

[8] YD/T 3813—2020 基础电信企业数据分类分级方法

[9] T/ISEAA 002—2021 信息安全技术 网络安全等级保护大数据基本要求

[10] ISO/IEC 27001:2013 information technology—security techniques—information security management systems—requirements

[11] 中华人民共和国国务院.第133次常务会议通过《关键信息基础设施安全保护条例》:中华人民共和国国务院令[2021]745号.2021年

[12] 国家互联网信息办公室秘书局、工业和信息化部办公厅、公安部办公厅、国家市场监督管理总局办公厅.关于印发常见类型移动互联网应用程序必要个人信息范围规定的通知:国信办秘字[2021]14号.2021年

[13] 深圳市第七届人民代表大会常务委员会.第二次会议通过《深圳经济特区数据条例》:深圳市第七届人民代表大会常务委员会[2021].2021年