

# DB3207

连 云 港 市 地 方 标 准

DB3207/T 2019—2024

## 网络数据安全规范

Network data security management specifications

2024-03-25 发布

2024-04-01 实施

连云港市市场监督管理局 发布

目 次

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 总体框架和要求 ..... 2

4.1 总体框架 ..... 2

4.2 总体要求 ..... 3

5 安全管理要求 ..... 4

5.1 机构管理 ..... 4

5.1.1 基本要求 ..... 4

5.1.2 增强要求 ..... 4

5.2 制度管理 ..... 4

5.2.1 基本要求 ..... 5

5.2.2 增强要求 ..... 5

5.3 人员管理 ..... 5

5.3.1 基本要求 ..... 5

5.3.2 增强要求 ..... 6

5.4 外包管理 ..... 6

5.5 分类分级 ..... 7

5.5.1 基本要求 ..... 7

5.5.2 增强要求 ..... 7

5.6 个人信息保护 ..... 7

5.7 云安全防护 ..... 8

6 数据处理活动 ..... 8

6.1 数据收集 ..... 8

6.1.1 基本要求 ..... 8

6.1.2 增强要求 ..... 9

6.2 数据存储 ..... 9

6.2.1 基本要求 ..... 9

6.2.2 增强要求 ..... 10

6.3 数据使用 ..... 10

6.3.1 基本要求 ..... 10

6.3.2 增强要求 ..... 10

6.4 数据加工 ..... 10

6.4.1 基本要求 ..... 10

6.4.2 增强要求 ..... 11

6.5 数据传输 ..... 11

6.5.1 基本要求 ..... 11

6.5.2 增强要求 ..... 12

6.6 数据提供 ..... 12

6.6.1 基本要求 ..... 12

6.6.2 增强要求 ..... 12

6.7 数据公开 ..... 12

6.7.1 基本要求 ..... 12

6.7.2 增强要求 ..... 13

6.8 数据销毁 ..... 13

6.8.1 基本要求 ..... 13

6.8.2 增强要求 ..... 13

6.9 数据委托 ..... 14

6.10 数据交易 ..... 14

6.11 数据出境 ..... 14

7 安全运营要求 ..... 15

7.1 风险评估 ..... 15

7.1.1 基本要求 ..... 15

7.1.2 增强要求 ..... 15

7.2 监测预警 ..... 16

7.2.1 基本要求 ..... 16

7.2.2 增强要求 ..... 16

7.3 应急管理 ..... 16

7.3.1 基本要求 ..... 16

7.3.2 增强要求 ..... 17

8 监督、评价、投诉处理与改进 ..... 17

8.1 监督 ..... 17

8.2 评价 ..... 17

8.3 投诉处理 ..... 17

8.4 改进 ..... 17

参考文献 ..... 18

## 前 言

本文件按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》规定编写。

本文件由中共连云港市委网络安全和信息化委员会办公室提出并归口。

本文件起草单位：中共连云港市委网络安全和信息化委员会办公室、连云港市政务服务管理办公室、连云港市大数据管理中心、连云港市人力资源和社会保障局、连云港市城建控股集团有限公司、快页信息技术有限公司、连云港大数据产业发展有限公司、联通数字科技有限公司、凭阑江苏实验室科技有限公司。

本文件主要起草人：陈勇、李伟、王光杰、王传尚、董亮、徐毅、窦全成、李鑫、孙益龙、张周华、吴青松、杨焕烽、王钢、陈雨萱、邱会。

# 网络数据安全管理规范

## 1 范围

本文件规定了网络数据安全、网络数据处理活动、网络数据安全运营的合规管理要求。

本文件适用于网络数据处理者的网络数据安全合规管理，网络数据安全监管者的监督管理、检查评估工作。

## 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 19038 顾客满意测评模型和方法指南
- GB/T 19039 顾客满意测评通则
- GB/T 25069 信息安全技术 术语
- GB/T 31167 信息安全技术 云计算服务安全指南
- GB/T 35273 信息安全技术 个人信息安全规范
- GB/T 37988 信息安全技术 数据安全能力成熟度模型
- GB/T 39477 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

GB/T 25069、GB/T 35273和GB/T 37988界定的以及下列术语和定义适用于本文件。

### 3.1

**数据 data**

任何以电子或者其他方式对信息的记录，描述的方式包括如数字、文字、音频、图像等形式。

### 3.2

**网络数据 network data**

通过网络收集、存储、使用、加工、传输、提供、公开的各种数据。

### 3.3

**核心数据 core data**

对领域、群体、区域具有较高覆盖度或达到较高精度、较大规模、一定深度的重要数据，一旦被非法使用或共享，可能直接影响政治安全。

注：核心数据主要包括关系国家安全重点领域的数据，关系国民经济命脉、重要民生、重大公共利益的数据，经国家有关部门评估确定的其他数据。

3.4

**重要数据 important data**

我国机构和个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的

注：重要数据通常指公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的各类机构在开展业务活动中收集和产生的，不涉及国家秘密，但一旦泄漏、篡改或滥用将会对国家安全、经济发展和社会公共利益造成不利影响的数据（包括原始数据和衍生数据）。

3.5

**一般数据 general data**

核心数据、重要数据之外的其他数据。

3.6

**数据活动 data activity**

组织、机构针对数据开展的一组特定任务的集合，数据活动主要包括收集、存储、使用、加工、传输、提供、公开等。

3.7

**网络数据处理者 network data processor**

在网络数据处理活动中自主决定处理目的和处理方式的个人和机构。

4 总体框架和要求

4.1 总体框架

围绕“构建全方位数据安全体系、筑牢网络数据安全防护线”的总体目标，坚持“实战化、体系化、常态化”理念，以国家法律法规为依据，基于“统筹规划、统一策略、分级建设”的原则，构建一体化网络数据安全保障体系，将数据安全能力贯穿于数据管理的各领域和全过程，实现数据可知、风险可视、安全可控、问题可溯。总体框架见图 1。

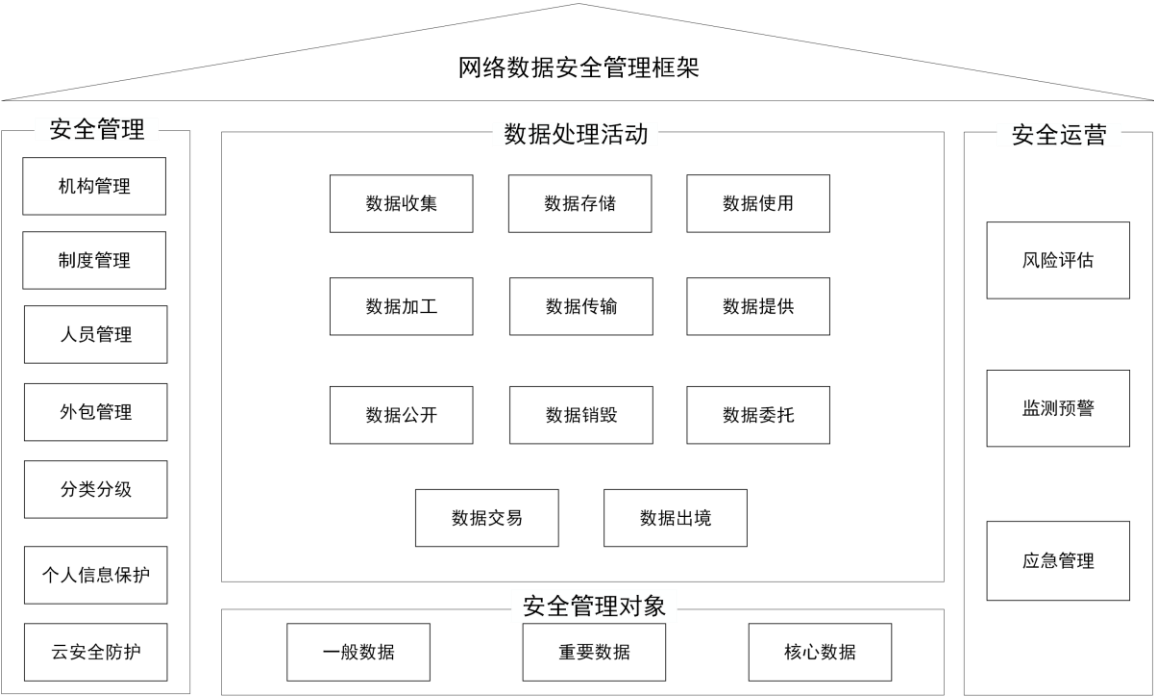


图 1 网络数据安全管理框架

注：（1）网络数据安全管理

网络数据安全管理主要是通过构建符合数据安全相关政策法规、规章制度和业务发展所需要的管理组织、管理制度、人员能力和技术规范，做好机构管理、制度管理、人员管理、外包管理、分类分级、个人信息保护、云安全防护等日常工作，安全管理贯穿整个数据处理活动。

（2）网络数据处理活动

网络数据处理活动是数据安全体系建设的核心支撑，通过技术措施保证数据的收集、存储、使用、加工、传输、提供、公开、销毁、委托、交易、出境等全生命周期安全。具体建设可根据实际数据、业务场景、安全需求以及现状选择相应的安全能力。

（3）网络数据安全运营

网络数据安全运营是数据安全管控工作常态化构建，运用适当的安全技术和管理手段整合人、技术、流程，实现数据安全策略持续动态调整和安全积极防御，做好数据风险评估、监测预警、应急管理等日常运维及运营工作，安全运营贯穿整个数据处理活动。

4.2 总体要求

网络数据安全管理主要包含安全管理要求、数据处理活动要求、安全运营要求三个部分。关键信息基础设施、重要网络数据处理活动，以及网络数据监管者、网络数据处理者认为有必要的网络数据安全管理，原则上应在符合基本要求的基础上，满足增强要求。

## 5 安全管理要求

### 5.1 机构管理

#### 5.1.1 基本要求

5.1.1.1 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。

5.1.1.2 应按照相关法律、法规、规章的要求编制数据资源目录，加强数据安全保护。

5.1.1.3 数据安全责任人履行职责应包括但不限于：

- a) 组织制定数据保护计划并落实；
- b) 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；
- c) 按要求组织向有关部门报告数据安全保护和事件处置情况；
- d) 组织受理并处理数据安全投诉和举报事项等。

5.1.1.4 数据安全管理机构应明确数据安全管理人员岗位职责，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：

- a) 负责数据存储、数据权限分配、数据资产梳理等；
- b) 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；
- c) 负责数据安全审计等。

5.1.1.5 处理个人信息达到规定数量的，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。

5.1.1.6 应针对数据类别级别变更、数据权限变更、重要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。

5.1.1.7 涉及数据合作方的，应与其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，每年不低于一次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。

#### 5.1.2 增强要求

5.1.2.1 应针对重要数据处理活动建立逐级审批机制。

5.1.2.2 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。

### 5.2 制度管理



### 5.2.1 基本要求

5.2.1.1 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制定。

5.2.1.2 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规章制度、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、数据安全教育培训、数据合作方管理、个人信息安全保护等。

5.2.1.3 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。

5.2.1.4 应定期对数据安全管理制度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。

5.2.1.5 应设立网络数据安全管理的专项经费，并确保该专项经费专款专用。

### 5.2.2 增强要求

5.2.2.1 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。

根据国家法律、法规、规章等有关要求，结合实际制定个人信息保护管理规章制度，应包括：

- a) 对文件、记录等文档进行备案管理；
- b) 在个人信息保护管理过程中记录与个人信息相关的活动和行为（如：制度建立、宣传、教育培训、安全管理、过程改进等）的目的、时间、范围、对象、方式方法、效果、反馈等信息；
- c) 对信息系统个人信息保护的设计与开发建立相关的规范和流程；
- d) 定期检查个人信息安全策略、制度的适宜性，并对其进行持续的改进和完善；
- e) 为个人信息主体提供投诉或申诉渠道。

5.2.2.2 制定合理、有效的个人信息侵害补救措施（包括纠正错误、消除影响、恢复名誉、适当赔偿等）。

5.2.2.3 应建立个人信息主体保护权益的渠道和机制，及时响应个人信息主体访问、复制、更正、删除、撤回、注销账户、获取副本等请求满足 GB/T 35273 的要求，不对请求设置不合理条件。

## 5.3 人员管理

### 5.3.1 基本要求

5.3.1.1 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要求并严格落实。

5.3.1.2 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

员调离岗位保密要求、保密期限、违约责任等，有效约束操作行为。

**5.3.1.3** 应根据“业务需要”和“最少够用”原则，对信息系统访问权限进行分配，控制对数据的访问和使用，确保任何人都只能在其履行职责时间范围内访问其开展业务所必需的数据，防止未经授权擅自对数据进行查看、披露、篡改或破坏。

### **5.3.2 增强要求**

**5.3.2.1** 应配备专职安全管理员承担数据安全管理员工作。

**5.3.2.2** 应定期对不同数据岗位人员进行技能考核。应组织数据岗位人员考取相关资质证书，持证上岗，证书包括但不限于中国网络安全审查技术与认证中心或中国信息安全测评中心颁发的数据安全相关证书。

**5.3.2.3** 应建立个人信息保护管理责任制，明确个人信息保护管理机构和人员的责任。

## **5.4 外包管理**

**5.4.1** 针对合作方管理机制建设情况，应包括如下要求：

- a) 应建立数据合作方安全管理机制，如对合作方或外包服务机构的选择、评价、管理、监督机制；
- b) 应对数据合作方或外包服务机构的安全能力进行评估；
- c) 应对外包服务机构、人员履行安全责任义务的监督情况进行检查。

**5.4.2** 针对合作协议约束情况，应包括如下要求：

- a) 应在协议中对接收、使用本单位数据的合作方的数据使用行为进行约束；
- b) 应在协议中明确了数据处理目的、方式、范围，安全保护责任、保密约定及违约责任和处罚条款等；
- c) 应在协议中，界定单位与合作方、外包服务机构间的数据安全责任。

**5.4.3** 针对外包访问权限管理情况，应包括如下要求：

- a) 外包人员对数据与系统的访问、修改权限应限于最小必要范围；
- b) 能够在测试环境下或使用测试数据完成的，不得向外包人员开放生产环境权限或真实数据；
- c) 应对外包人员数据导出操作或数据外发操作的情况进行监督管理；
- d) 外包人员对敏感数据的访问及操作应被实时监督或监测；
- e) 对数据外包服务账号及访问权限管理情况进行审计；
- f) 对外包人员远程访问操作系统或数据的情况进行审计。

**5.4.4** 针对第三方接入与数据回收情况，应包括如下要求：

- a) 应对合作方接入的系统、使用的技术工具进行技术检测，避免引入木马、后门等；
- b) 为完成技术或服务目的向合作方提供的数据，在合作结束后应进行回收，并要求合作方对数据进行删除；
- c) 外包服务到期后，应进行账号注销、数据回收、数据删除、数据销毁等。

## 5.5 分类分级

### 5.5.1 基本要求

- 5.5.1.1 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。
- 5.5.1.2 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，数据先按行业领域分类、再按业务属性分类，形成数据资源分类目录。
- 5.5.1.3 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。将数据从高到低分为核心、重要、一般三个基本级别。各行业各领域应在遵循数据分级框架的基础上，明确本行业本领域数据分级规则。
- 5.5.1.4 应在数据分类分级基础上，形成数据资产清单，落实不同数据安全等级差异化防护措施要求。
- 5.5.1.5 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。

### 5.5.2 增强要求

- 5.5.2.1 应采取数据安全防护措施，对核心数据、重要数据和敏感个人信息进行重点保护。
- 5.5.2.2 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，构建数据关系。

## 5.6 个人信息保护

- 5.6.1 应将个人信息保护管理纳入机构的工作和管理，在统一、规范的安全风险管理框架中实施个人信息保护管理。
- 5.6.2 应建立个人信息保护日常管理监督机制，定期检查个人信息保护策略、制度的落实情况，及时进行相关整改，确保个人信息保护的各项工作落实到位。
- 5.6.3 应建立个人信息保护检查评估机制和工作流程，及时发现和评估个人信息保护工作中存在的漏洞及风险。
- 5.6.4 应建立信息系统投入运行前的功能审核机制，保证信息系统无个人信息数据主动外泄的隐藏功

能。

5.6.5 应建立第三方评估机构定期对信息系统进行安全测评的机制，发现问题及时整改，以提高系统的安全性和个人信息防护水平。

5.6.6 应建立个人信息保护应急响应机制，形成应急预案，并定期演练，以有效应对个人信息安全事件。

5.6.7 应定期开展个人信息保护管理相关的内部或外部审计，并根据审计结果持续改进相关策略、制度和流程。

5.6.8 应建立个人信息安全事件报告和通报机制，提高个人信息保护的安全防范和告警能力。

5.6.9 数据处理者应遵守以下规定：

- a) 按照服务类型分别向个人申请处理个人信息的同意，不得使用概括性条款取得同意；
- b) 处理个人生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等敏感个人信息应当取得个人同意；
- c) 处理不满十四周岁未成年人的个人信息，应当取得其监护人同意；
- d) 不应通过误导、欺诈、胁迫等方式获得个人的同意；
- e) 不应超出个人授权同意的范围处理个人信息；
- f) 不应在个人明确表示不同意后，频繁征求同意、干扰正常使用服务。

## 5.7 云安全防护

5.7.1 采用云平台部署信息系统，应依据 GB/T 31167-2023 和 GB/T31168-2023，部署前考核云计算服务商的能力水平。

5.7.2 应使用密码技术用于核心数据、重要数据的传输和存储。按密码应用要求，定期开展商用密码应用安全性评估，并根据测评情况完成整改。

5.7.3 应与云平台服务商签订协议，使其保证不对信息系统的个人信息进行转存、读取、分析和外泄，并定期对信息系统进行安全检查，服务商还应确定有强大的用户访问控制机制、事件应急反应机制、数据备份与恢复机制。

5.7.4 应对云上个人信息处理系统的安全性进行风险评估。

## 6 数据处理活动

### 6.1 数据收集

#### 6.1.1 基本要求

6.1.1.1 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。

6.1.1.2 收集外部机构数据前，应确保收集的数据不含有恶意代码或恶意软件。

6.1.1.3 仅收集与所需目的相关的数据，非必要不收集敏感数据。对于敏感数据的收集，需要额外的审慎和安全措施。

6.1.1.4 应建立数据质量管理和监控的手段，对异常数据及时告警、及时更正采取的手段措施。

6.1.1.5 通过人工方式采集数据时，应对数据采集人员进行严格管理，保证将采集数据直接报送到相关人员或系统，采集任务完成后及时删除采集人员留存的数据。

## 6.1.2 增强要求

6.1.2.1 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。

6.1.2.2 提供服务的网络应用程序或第三方应用，应遵循最小化必要原则，不得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网络应用程序或第三方应用。

6.1.2.3 定期审核数据收集事件，确保合规性和风险评估的更新。

6.1.2.4 对收集的数据进行必要的匿名化或去标识化处理，保护个人隐私。

6.1.2.5 在收集数据时使用安全通道，例如 HTTPS 或 SSL 等加密协议。

6.1.2.6 App、Web 等客户端完成相关业务后，应对留存敏感个人信息或重要数据情况进行检测。

## 6.2 数据存储

### 6.2.1 基本要求

6.2.1.1 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，防止未经授权的访问。

6.2.1.2 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。

6.2.1.3 应建立存储介质安全管理规范，明确对存储介质存储数据的安全要求。

6.2.1.4 应建设并落实数据存储安全策略和操作规程。

6.2.1.5 对数据进行分类和标记，实施不同等级的安全策略，确保敏感数据得到更严格的保护。

6.2.1.6 建立访问审计日志，记录数据处理、权限管理、人员操作等日志，日志留存时间不少于六个月。

## 6.2.2 增强要求

6.2.2.1 个人生物识别信息应与个人信息分开存储，非必要不存储原始个人生物识别信息，仅存储个人生物识别信息的摘要信息。

6.2.2.2 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。

## 6.3 数据使用

### 6.3.1 基本要求

6.3.1.1 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，在保证安全的条件下开展数据利用。

6.3.1.2 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。

6.3.1.3 应根据不同数据使用场景采用安全处理措施，降低数据敏感度及暴露风险。

6.3.1.4 在使用数据时，必须遵守适用的法律法规和合规性要求。确保数据使用的目的和方式符合法律规定，并获得必要的授权和许可。

6.3.1.5 仅在获得合法的数据许可和使用权的情况下使用数据。遵守数据提供方的规定和约束，不得超越许可范围进行数据的使用。

6.3.1.6 对数据的访问和使用进行监控和审计，及时发现和处理异常行为。

6.3.1.7 应建立数据使用策略，明确访问控制和权限分配。

### 6.3.2 增强要求

6.3.2.1 应采取技术措施保证汇聚大量数据时不暴露敏感信息。

6.3.2.2 应对接入或嵌入的第三方应用加强数据安全管控，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应立即叫停。

6.3.2.3 应采用技术手段记录和管理数据使用操作行为。

## 6.4 数据加工

### 6.4.1 基本要求

6.4.1.1 数据加工过程中应确保数据的完整性和准确性，加工后的数据应符合数据隐私保护的法规要求。

6.4.1.2 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。

6.4.1.3 应在数据加工前，书面明确数据加工的目的、范围、期限、规则及数据加工主体的责任与义务。

6.4.1.4 开展数据加工活动过程中，对可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止加工活动。

6.4.1.5 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，不得超出已征得个人信息主体授权同意的范围。

6.4.1.6 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。

6.4.1.7 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。

#### 6.4.2 增强要求

6.4.2.1 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并处置。

6.4.2.2 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。

### 6.5 数据传输

#### 6.5.1 基本要求

6.5.1.1 应制定数据跨机构传输管理规则，并建立相关技术措施对跨机构数据传输进行安全保障。

6.5.1.2 应明确数据传输相关安全管控措施，包括不限于传输通道加密、数据内容加密、数据接口传输安全等。

6.5.1.3 定期更新加密协议。

6.5.1.4 对敏感数据的传输进行额外的身份验证和授权。

6.5.1.5 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。

6.5.1.6 应采用校验技术保证数据在传输过程中的完整性。

6.5.1.7 实施多层次的网络安全措施。

6.5.1.8 建立加密密钥管理策略，定期轮换密钥。

6.5.1.9 应建立数据传输日志。以便于监控数据传输活动的安全和合规。

## 6.5.2 增强要求

6.5.2.1 对传输的数据进行完整性验证和防止重放攻击的措施。

6.5.2.2 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。

## 6.6 数据提供

### 6.6.1 基本要求

6.6.1.1 提供的数据应符合法律法规和政策要求。

6.6.1.2 在提供数据给第三方之前，确保已获得数据主体的同意或授权。

6.6.1.3 对数据提供方进行尽职调查，确保其具备数据安全能力。

6.6.1.4 制定并发布统一、权威的公共数据、开放目录。明确可开放数据的范围，完善各敏感程度数据的开放管理规定。

6.6.1.5 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。

6.6.1.6 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。

6.6.1.7 政务信息资源交换平台的政务信息共享应履行 GB/T39477—2020 第 6 章确定的共享数据安全技术要求。

6.6.1.8 提供数据的人员应经过身份验证和授权，确保只有合法用户才能够访问数据。

### 6.6.2 增强要求

6.6.2.1 对数据提供进行定期审核，确保合规性和风险管理。

6.6.2.2 公共数据提供部门应对共享的数据采取数字水印等技术，确保共享数据可溯源。

## 6.7 数据公开

### 6.7.1 基本要求

6.7.1.1 在数据公开前应先进行风险评估工作，对敏感数据进行匿名化或脱敏，以防止数据主体的身份泄露。

6.7.1.2 开放的公共数据实行统一目录管理，实现“应开尽开”。

6.7.1.3 对非涉密但涉及敏感信息的公共数据，由公共管理和服务机构按照国家有关规定，进行脱敏、



清洗后向社会开放。

6.7.1.4 在数据公开活动中应遵守以下要求：

- a) 涉及国家秘密、政务敏感、工作秘密等重要数据，不得公开；
- b) 涉及个人隐私等敏感数据，任何单位和个人未经被收集者同意不得公开；
- c) 已公开数据不得含有《网络信息内容生态治理规定》中定义的违禁内容。

6.7.1.5 在进行数据公开时，需要注意保护个人隐私和敏感信息。对于包含个人身份信息的数据，进行脱敏处理或采取其他隐私保护措施，以防止个人信息的泄露和滥用。

6.7.1.6 建立数据公开审核流程，确保公开数据的安全性和合规性。

## 6.7.2 增强要求

6.7.2.1 向数据主体提供更多的数据控制选项，例如选择性公开或数据访问撤销。

6.7.2.2 在展示重要数据和敏感个人信息时，应采用防截屏或屏幕水印等技术。

## 6.8 数据销毁

### 6.8.1 基本要求

6.8.1.1 定期审查不再需要的数据，并建立销毁计划。

6.8.1.2 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。

6.8.1.3 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。

6.8.1.4 如因业务终止或机构解散，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。

6.8.1.5 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。

6.8.1.6 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。

6.8.1.7 应建立存储介质销毁策略和操作规程，明确各类介质的销毁流程、方式和要求，妥善处置销毁的存储介质。

6.8.1.8 应按照 GB/T35273—2020 中 8.3 规定的要求执行个人信息删除操作。

### 6.8.2 增强要求

6.8.2.1 应在中国境内对介质存储的数据进行销毁或删除。

6.8.2.2 进行定期的数据销毁审计，销毁数据的过程中应实施加密和粉碎等措施，确保数据无法被恢复和读取。另外可以考虑使用第三方认证机构对数据的销毁过程进行审计和记录，以确保数据的彻底销毁。

## 6.9 数据委托

6.9.1 委托他人处理网络数据，应履行审批手续，以合同等手段监督受托方履行相应的数据安全保护义务。

6.9.2 数据处理受托方应依照法律、法规的规定和合同约定履行数据安全保护义务的，不得擅自留存、使用、泄露或者向他人提供数据。

6.9.3 委托方应定期审查受托方的数据保护措施，确保它们符合约定和法律要求。

## 6.10 数据交易

6.10.1 确保在数据交易过程中，数据以加密的方式进行传输。使用安全协议和加密算法，保护数据在传输过程中的机密性和完整性。

6.10.2 实施严格的访问控制措施，限制对数据的访问权限。采用身份验证机制，确保只有授权的用户才能访问和处理数据。

6.10.3 建立安全审计和监控机制，对数据交易过程进行实时监测和记录。通过日志记录、异常检测和报警机制等手段，及时发现和应对安全事件和威胁。

6.10.4 在数据交易过程中，确保与交易方签订明确的合同和协议。明确数据使用和保护的范围、责任和义务，包括数据安全、隐私保护、数据用途限制等方面的规定。遵守适用的法律法规，确保数据交易的合法性和合规性。

6.10.5 如果涉及第三方服务提供商或合作伙伴，需进行严格的风险评估和管理。确保第三方具备适当的安全措施和合规性，保护数据不受未经授权的访问和滥用。

6.10.6 如采用第三方数据交易平台进行交易，平台应具有相应的资质，平台应要求数据提供方说明数据来源，审核交易双方的身份，并留存审核和交易记录。

6.10.7 数据交易前，应该先进行数据脱敏，避免从数据中提取隐私信息的情况。

## 6.11 数据出境

6.11.1 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，严禁未经授权数据出境行为。

6.11.2 境内用户在境内访问境内网络的，其流量不应路由至境外。

6.11.3 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。

6.11.4 向境外提供个人信息和重要数据的数据处理者，应当编制数据出境安全报告，定期向设区的市级网信部门报告上一年度数据出境情况。

6.11.5 数据处理者向境外提供数据应履行以下义务：

a) 不得超出报送网信部门的个人信息保护影响评估报告中明确的目的、范围、方式和数据类型、规模等向境外提供个人信息；

b) 不得超出网信部门安全评估时明确的出境目的、范围、方式和数据类型、规模等向境外提供个人信息和重要数据；

c) 国家网信部门会同国务院有关部门核验向境外提供个人信息和重要数据的类型、范围时，数据处理者应当以明文、可读方式予以展示；

d) 个人信息出境后确需再转移的，应当事先与个人约定再转移的条件，并明确数据接收方履行的安全保护义务。

## 7 安全运营要求

### 7.1 风险评估

#### 7.1.1 基本要求

7.1.1.1 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。

7.1.1.2 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。

7.1.1.3 处理重要数据或者赴境外上市的数据处理者，应当自行或者委托数据安全服务机构每年开展一次数据安全评估，并定期将上一年度数据安全评估报告报设区的市级网信部门及有关主管部门。

#### 7.1.2 增强要求

7.1.2.1 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。

7.1.2.2 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及应对措施等。

7.1.2.3 当有新的攻击技术出现后，应立即触发网络安全风险评估工作。

## 7.2 监测预警

### 7.2.1 基本要求

7.2.1.1 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。

7.2.1.2 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。

7.2.1.3 应完善网络安全事件应急预案和网络安全信息共享平台，加强数据安全信息共享、数据安全风险和威胁监测预警以及数据安全事件应急处置工作。

7.2.1.4 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。

### 7.2.2 增强要求

7.2.2.1 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。

7.2.2.2 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。

7.2.2.3 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。

## 7.3 应急管理

### 7.3.1 基本要求

7.3.1.1 制定实施数据安全保护计划和数据安全事件应急预案，对预案进行评审，并定期完善。

7.3.1.2 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。

7.3.1.3 应建立数据安全应急处置机制，依据本地区、本行业网络安全事件应急相关文件开展应急处置工作。

7.3.1.4 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，及时告知相关权益人，并按照有关规定向网信、公安部门和有关行业主管部门报告。

7.3.1.5 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。

7.3.1.6 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，发生重要数据或者十万人以上个人信息泄露、毁损、丢失等数据安全事件时应向网信部门报告。

7.3.1.7 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。

### 7.3.2 增强要求

7.3.2.1 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。

7.3.2.2 关键信息基础设施系统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。

7.3.2.3 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 监督、评价、投诉处理与改进

### 8.1 监督

8.1.1 应主动向社会公示服务内容、服务依据、服务流程、服务时限、服务要求、投诉渠道，保障服务对象的知情权和监督权。

8.1.2 应实施内部服务质量考核与评估，并接受行政监督和社会监督。

### 8.2 评价

8.2.1 应采取内部评价和外部评价相结合，开展以服务对象满意度测评为核心要素的服务质量。

8.2.2 对服务对象的满意度测评应符合 GB/T 19038 和 GB/T 19039 要求。

### 8.3 投诉处理

应提供现场、信函、电话、网络等投诉渠道，明确专门部门负责调查、处理服务对象的投诉处理结果告知投诉人。

### 8.4 改进

8.4.1 应注重服务对象的满意度和公共服务效能的提升，持续提高服务质量。

8.4.2 应根据服务评价对服务内容、服务形式、服务流程进行优化和改进。

8.4.3 应根据监督和审核结果，及时纠正或采取预防措施，提高社会满意度。

## 参考文献

- [1] 中华人民共和国网络安全法
  - [2] 中华人民共和国数据安全法
  - [3] 中华人民共和国个人信息保护法
  - [4] 中华人民共和国密码法
  - [5] 关键信息基础设施安全保护条例
  - [6] GB/T22239 信息安全技术 网络安全等级保护基本要求
  - [7] GB/T31168 信息安全技术 云计算服务安全能力要求
  - [8] GB/T37932 信息安全技术 数据交易服务安全要求
  - [9] GB/T39335 信息安全技术 个人信息安全影响评估指南
  - [10] GB/T41479 信息安全技术 网络数据处理安全要求
-