ICS 35.040
CCS L 80

DB4401

广　州　市　地　方　标　准

DB4401/T 276—2024

网络数据安全管理规范

Network data security management specification

2024-08-28 发布　　2024-09-28 实施

广州市市场监督管理局　　发布

目　　次

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》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这些专利的责任。

本文件由广州市互联网信息办公室提出并归口。

本文件起草单位：广州市信息安全测评中心、广州市标准化研究院、北京安华金和科技有限公司、中电科网络安全科技股份有限公司、广州赛西标准检测研究院有限公司、杭州安恒信息技术股份有限公司、奇安信网神信息技术（北京）股份有限公司、广东华进律师事务所、中国联合网络通信有限公司广州市分公司、广州绿盟网络安全技术有限公司。

本文件主要起草人：陆志强、贺忠、鲁胜兵、施冰、王冰、曾剑锋、徐湛、魏力、吴杨松、刘柳妹、王龙、颜爱军、宋常林、楚赟、程珂昵、晁静洋、陈朝华、彭冕莉、余清霞。

网络数据安全管理规范

1 范围

本文件给出了网络数据安全管理的基本要求，包括网络数据安全管理要求、网络数据通用安全要求、网络数据处理活动安全要求和个人信息保护扩展要求。

本文件适用于指导各行业、各领域、各地区、各部门数据处理者开展网络数据安全管理工作，也可为数据安全监管部门、数据安全认证、评估、审计机构或其他有关组织对网络数据处理活动实施安全监管、评估提供参考。

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 25069—2022 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

3 术语和定义

GB/T 25069—2022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。

3.2

网络 network

由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

3.3

网络数据 network data

通过网络收集、存储、传输、处理和产生的各种电子数据。

3.4

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。

3.5

数据处理活动 data processing activities

数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等活动。

数据处理者 data processor

在数据处理活动中自主决定处理目的、处理方式的组织、个人。

［来源：GB/T 43697—2024，3.11］

3.6

重要数据 key data

特定领域、特定群体、特定区域或达到一定精度和规模，一旦被泄露或篡改、损毁，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

注：仅影响组织自身或公民个体的数据一般不作为重要数据。

［来源：GB/T 43697—2024，3.2］

3.7

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，一旦被非法使用或共享，可能直接影响政治安全的重要数据。

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。

［来源：GB/T 43697—2024，3.3］

3.8

一般数据 general data

核心数据、重要数据之外的其他数据。

［来源：GB/T 43697—2024，3.4］

3.9

个人信息 personal information

以电子或者其他方式记录的与已识别或者可以识别自然人有关的各种信息。

注1：个人信息不包括匿名化处理后的信息。

注2：个人信息包括姓名、出生日期、公民身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息等。

［来源：GB/T 41479—2022，3.6］

3.10

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注：敏感个人信息包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

［来源：GB/T 41479—2022，3.7］

3.11

个人信息主体 personal information subject

个人信息已识别或可识别（所标识或关联到）的自然人。

［来源：GB/T 41479—2022，3.8］

3.12

个人信息处理者 personal information processor

个人信息处理者，是指在个人信息处理活动中自主决定处理目的、处理方式的组织、个人。

3.13

数据合作方 data partner

通过业务合作、提供技术支撑和数据服务等，并可能接触到组织机构数据的外部机构。

3.14

第三方应用 third party application

由第三方提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务中的自动化工具。

注：本文件中的第三方应用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］

3.15

匿名化 anonymization

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。

［来源：GB/T 41479—2022，3.13］

3.16

去标识化 de-identification

通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体的过程。

注：去标识化建立在个体基础之上，保留了个体颗粒度，采用假名、加密、哈希函数等技术手段替代对个人信息的标识。

［来源：GB/T 35273—2020，3.15］

3.17

数据脱敏 data desensitization

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。

［来源：GB/T 37988—2019，3.12］

3.18

数据安全风险评估 data security risk assessment

对数据和数据处理活动安全进行风险识别、风险分析和风险评价的整个过程。

注：根据发起者不同，分为自评估和检查评估。自评估由数据处理者自身发起，组成机构内部评估小组或委托第三方评估机构，依据有关政策法规与标准，对评估对象的数据安全风险进行评估的活动。检查评估由数据处理者的上级主管部门、业务主管部门或国家有关主管（监管）部门发起的，依据有关政策法规与标准，对评估对象

的数据安全风险进行的评估活动。

3.19

大型互联网平台 large internet platform

通过网络技术将个人与个人、商品、信息、服务、线下资源、数据、资金、软件等进行连接，并以此为基础提供业务的较大规模的网络平台。

注1：较大规模是指在过去的一年期间，在我国累计活跃用户总数不低于5000万。

注2：提供业务包括但不限于即时通信、社交网络、电子商务、直播、短视频、信息资讯、应用商店、网络预约汽车、网络支付等。

4 网络数据安全管理总体框架

4.1 网络数据安全管理应包括网络数据安全管理要求、网络数据通用安全要求、网络数据处理活动安全要求和个人信息保护扩展要求四部分内容，网络数据安全管理要求指导落实网络数据处理活动安全要求和个人信息保护扩展要求，网络数据通用安全要求作为整体数据安全管理的基础技术支撑。其中，一般数据保护应满足数据安全的基本保护要求；重要数据保护应同时满足基本保护要求和重要数据扩展要求；核心数据应在重要数据保护的基础上依照有关规定从严保护；个人信息保护应在上述基础上，满足个人信息保护扩展要求。总体框架图见图1。

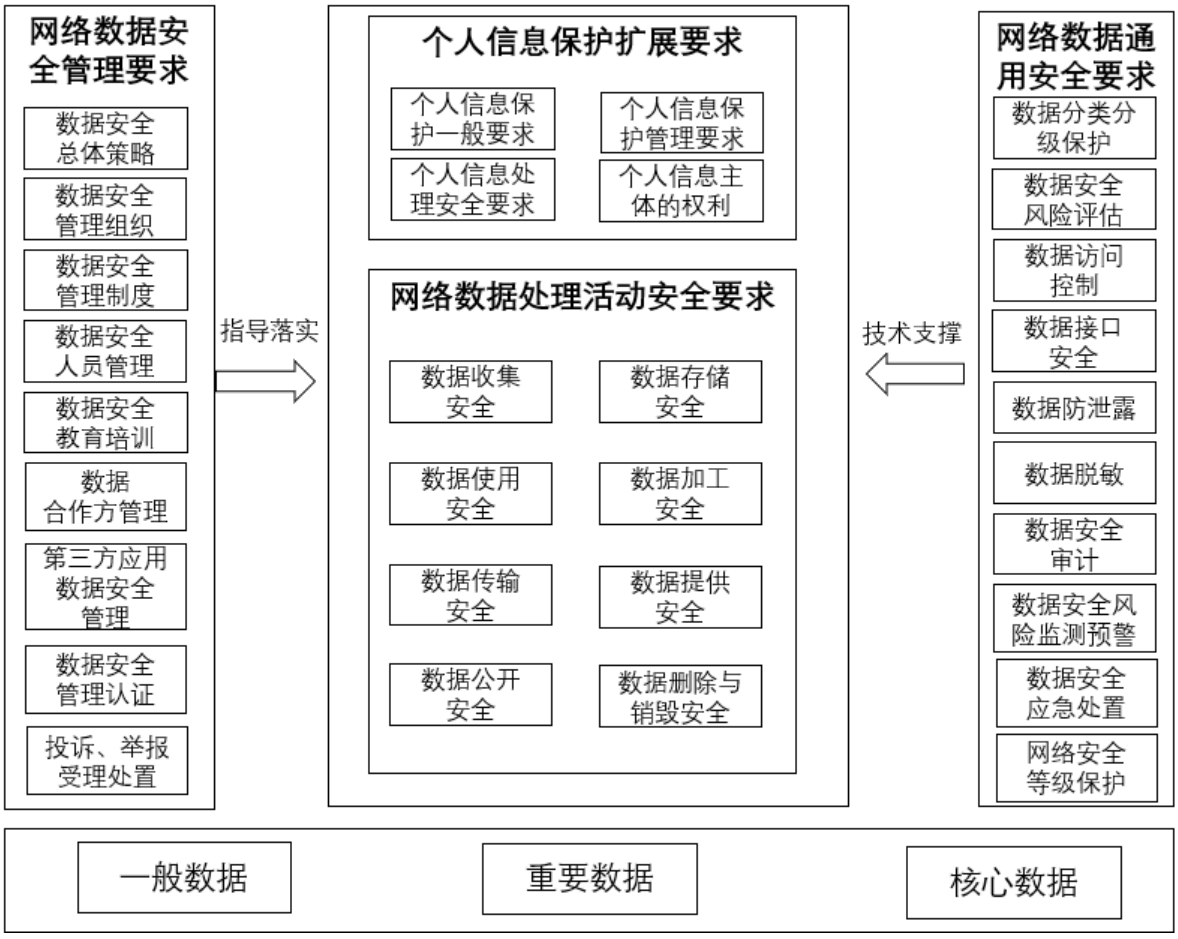

图1 总体框架图

4.2 网络数据安全管理要求

围绕数据安全总体策略、数据安全管理组织、数据安全管理制度、数据安全人员管理、数据安全教育培训、数据合作方管理、第三方应用数据安全管理、数据安全管理认证和投诉、举报受理处置等方面，建立完善符合法律法规、相关标准规范的数据安全管理组织。

4.3 网络数据通用安全要求

围绕数据分类分级保护、数据安全风险评估、数据访问控制、数据接口安全、数据防泄露、数据脱敏、数据安全审计、数据安全风险监测预警、数据安全应急处置、网络安全等级保护等方面落实基础安全管理措施。

4.4 网络数据处理活动安全要求

围绕数据的收集、存储、使用、加工、传输、提供、公开、删除与销毁等数据处理活动，开展数据安全管理，落实技术保护措施。

4.5 个人信息保护扩展要求

围绕个人信息保护一般要求、个人信息保护管理要求、个人信息处理安全要求以及个人信息主体的权利等方面规范保护要求，落实个人信息保护措施。

5 网络数据安全管理要求

5.1 数据安全总体策略

5.1.1 基本保护要求

5.1.1.1 应制定总体安全管理框架，明确数据安全管理总体策略，包括管理目标、原则、要求等内容。

5.1.1.2 制定数据安全管理总体策略应以重要数据、个人信息为重点。

5.1.2 重要数据保护扩展要求

无重要数据保护扩展要求。

5.2 数据安全管理组织

5.2.1 基本保护要求

5.2.1.1 应通过正式文件或制度明确数据安全管理各级组织及相应职责。

5.2.1.2 应明确数据安全负责人。职责包括但不限于负责牵头制定数据安全管理制度、指导数据安全管理工作、协调各相关部门开展数据保护工作、组织内部数据安全教育培训工作、提出数据安全保护的对策建议、监督管理制度和措施的执行落实情况等。

5.2.1.3 应明确数据安全管理机构。数据安全管理机构在数据安全负责人的领导下，履行以下职责：

a) 研究提出数据安全相关重大决策建议；
b) 制定实施数据安全保护计划和数据安全事件应急预案；
c) 开展数据安全风险监测，及时处置数据安全风险和事件；
d) 定期组织开展数据安全宣传教育培训、风险评估、应急演练等活动；
e) 受理、处置数据安全投诉、举报；
f) 按照要求及时向网信部门和主管、监管部门报告数据安全情况。

5.2.1.4　应明确数据安全管理部门，牵头承担单位整体数据安全管理工作，落实数据安全保护责任。包括但不限于组织制定数据安全管理制度并执行，落实数据安全技术防护措施，开展数据安全教育培训、数据安全评估、数据安全监测、数据安全事件应急处置等工作。

5.2.1.5　应明确岗位职责和能力要求，足额配备具备相应岗位能力的数据安全人员，负责具体落实数据安全管理工作。包括但不限于数据梳理、分类分级、安全评估、合规性检查、权限管理、安全审计、监测预警、应急处置和信息报送、教育培训等工作。数据管理员、数据安全管理员、数据安全审计员应专人专岗。

5.2.1.6　宜建立独立的数据安全审计机构，负责开展数据安全和个人信息保护监督审计工作，并向管理层直接汇报。

5.2.2　重要数据保护扩展要求

5.2.2.1　重要数据处理者的数据安全负责人应由数据处理者决策层成员承担，并具备数据安全专业知识和相关管理工作经历。

5.2.2.2　掌握国家网信部门或者有关主管部门规定的特定种类、规模的重要数据的，数据安全管理机构应独立设立。

5.3　数据安全管理制度

5.3.1　基本保护要求

5.3.1.1　应建立健全数据安全管理制度，并通过正式、有效的方式发布数据安全管理制度和实施版本控制，并严格执行。

5.3.1.2　应形成由总体策略、管理规范、操作规程、记录表单等构成的数据安全管理制度体系。

5.3.1.3　制度体系内容应包括但不限于数据安全总体策略、组织机构与人员管理、数据分类分级、数据处理活动安全管理要求、数据访问控制、数据安全评估、数据安全审计、数据安全风险监测预警、数数据安全应急与处置、数据安全教育培训、合作方管理、数据出境、投诉举报受理处置等制度。

5.3.1.4　应建立数据安全制度文件管理控制流程，规范制度文件的建立、审批、发布、修订和废止，实施文件版本控制，确保制度文件的及时更新和有效访问。

5.3.1.5　应定期对数据安全管理制度的合理性、充分性和适用性进行论证和评价，对存在不足或需要改进的数据安全管理制度进行修订。

5.3.2　重要数据保护扩展要求

重要数据处理者应确保重要数据安全管理制度覆盖全部重要数据处理活动，并在安全环境、法规政策、组织架构或业务发生重大变化时及时评估和修订数据安全管理制度和安全策略。

5.4　数据安全人员管理

5.4.1　基本保护要求

5.4.1.1　应明确规定人员录用、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的数据安全管理要求并予以落实。

5.4.1.2　应明确人员岗位职责、数据访问和操作权限管理要求、人员调离保密要求、保密期限、违约责任等，定期审查其行为，对其数据操作行为进行有效约束。

5.4.1.3　在开展与关键信息基础设施网络安全和信息化有关的决策时，应有专门数据安全管理机构人员参与。

5.4.1.4　数据安全人员履职情况应留存相关工作记录，如数据安全管理监督检查记录、数据安全事件信息报送记录等。

5.4.2　重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据等人员落实资格审查、签署保密协议、审批和登记，明确岗位职责、数据访问范围、操作权限、人员调离保密要求、保密期限、违约责任等措施，定期审查其行为，对其数据操作行为进行有效约束。

5.5　数据安全教育培训

5.5.1　基本保护要求

5.5.1.1　应建立数据安全教育培训制度，明确培训周期、培训对象、培训内容、次数、课时和考核评价等。

5.5.1.2　应制定数据安全培训计划，定期（至少每年一次）或者政策发生变化时组织数据安全专业化培训工作，并对培训结果进行考核评价，留存相关记录（如培训计划、培训通知、培训课件、签到表、培训考核情况等相关记录文件）。

5.5.1.3　数据安全教育培训应覆盖单位全员，培训内容覆盖数据安全法律法规、单位制度要求和实操规范等内容。针对单位全员的培训内容包括但不限于普及数据安全意识、法律法规等，针对数据安全人员的培训内容包括但不限于标准规范、技能培训、安全评估、应急响应、应急演练等。

5.5.1.4　数据安全人员宜考取资质证书，持证上岗。

5.5.2　重要数据保护扩展要求

应对数据安全负责人、关键岗位人员、接触重要数据的相关人员每年开展数据安全培训考核，依据考核结果确定任职资格。

5.6　数据合作方管理

5.6.1　基本保护要求

5.6.1.1　应明确管理相关数据合作方的数据安全管理部门和执行配合部门，并设置专岗负责相关工作，明确工作职责。

5.6.1.2　应梳理形成数据合作方清单并定期更新，合作方清单包含合作方名称、合作业务或系统、合作形式、合作期限、合作方联系人、合作涉及数据类型、数量以及数据重要程度等信息。

5.6.1.3　应建立数据合作方安全管理机制，如对合作方的选择、评价、管理、监督机制等。明确合作方的数据安全保护方式和责任落实要求，包括但不限于服务合同、合作方资质审核、接入管理、权限管理、主体授权、多个合作方管理、安全技术要求、数据脱敏、行为监测、数据销毁、数据安全应急响应及处置等管理要求。

5.6.1.4　应审核数据合作方的资质、网络和数据安全保障能力、业务连续性保障能力、数据安全事件发生、数据安全事件应急响应和处置能力等情况，并开展安全评估。

5.6.1.5　应通过服务合同或安全保密协议等形式明确数据合作方的数据安全保护责任和义务。明确具体条款，包含但不限于下述内容：合作方及参与人员可接触到的数据处理相关平台系统范围，及数据使用权限、内容、范围、期限及用途（应符合最小化原则），合作方及参与人员的数据安全责任，合作方的保障措施配备情况（保障措施不低于本方的安全要求），合作结束后数据删除要求，合作方违约责任和处罚等。

5.6.1.6　应在合作结束后停用或下线向数据合作方提供的系统权限和接口，并回收数据及要求合作方对数据进行删除。

5.6.2　重要数据保护扩展要求

5.6.2.1　对处理重要数据的数据合作方，应重点排查数据传输安全、数据存储安全、数据访问安全、数据提供安全、数据删除与销毁等方面的风险并加强管控。
5.6.2.2　对处理重要数据的数据合作方，应每年组织开展合作方安全检查或评估工作，对发现的问题及时督促整改，必要时停止合作，并留存相关检查和安全评估记录不少于三年。

5.7　第三方应用数据安全管理

5.7.1　基本保护要求

5.7.1.1　应对接入或嵌入其他产品或服务的第三方应用加强数据安全管理，通过签订合同等方式明确数据安全责任和义务。
5.7.1.2　应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，对技术检测时发现超出双方约定的行为应及时停止接入。
5.7.1.3　应定期开展安全检查，发现第三方应用没有落实安全管理责任的，应及时督促整改，必要时停止接入。
5.7.1.4　服务结束后，应停用或下线相关系统权限和接口。

5.7.2　重要数据保护扩展要求

5.7.2.1　重要数据处理者对第三方应用应至少每年开展一次安全检查或评估工作，对发现的问题及时督促整改，必要时停止合作，并留存相关检查和安全评估记录不少于三年。
5.7.2.2　第三方应用发生重大变更或更新时，应在变更和更新前进行安全评估。

5.8　数据安全管理认证

5.8.1　基本保护要求

宜开展数据安全管理认证工作，通过认证方式规范网络数据处理活动，加强网络数据安全保护。

5.8.2　重要数据保护扩展要求

无重要数据保护扩展要求。

5.9　投诉、举报受理处置

5.9.1　基本保护要求

应建立投诉、举报受理处置制度，包括建立数据安全事件投诉、举报渠道及受理处置流程以及公布接受投诉、举报的联系方式、责任人等受理处置信息。收到通过其服务或业务平台编造、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、举报的，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，对于查实的编造、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，依法采取停止传输、消除等处置措施。

5.9.2　重要数据保护扩展要求

无重要数据保护扩展要求。

6 网络数据通用安全要求

6.1 数据分类分级保护

6.1.1 基本保护要求

6.1.1.1 应结合数据识别技术手段，梳理数据，形成数据清单。清单内容包括所属部门、数据类型、数据项名称、数据数量、数据来源、存储位置（如系统名称、数据库、表名等）、数据处理情况（访问、导出、共享、出境等）、数据关联系统等，并定期对已形成的数据清单进行更新。

6.1.1.2 应明确数据分类分级标准，确定数据类别和对应的安全等级。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、组织合法权益造成危害程度确定安全等级。

6.1.1.3 应依据数据分类分级制度和方法，在数据清单的基础上标记类别和级别，形成数据分类分级清单。清单内容包括所属部门、数据类别、数据项名称、数据数量、数据级别、数据来源、存储位置（如系统名称、数据库、表名等）、数据处理情况（如访问、导出、共享、出境等）、数据关联系统、是否为重要数据、是否为个人信息数据、是否为敏感个人信息数据等。

6.1.1.4 应根据政策要求和业务变化等对数据分类分级情况进行动态调整和评审，留存调整和评审记录。

6.1.1.5 应在数据分类分级的基础上，落实不同数据安全等级差异化防护措施要求。明确在数据处理活动中针对不同类别、级别的数据采取相应的安全保障措施，包括但不限于数据分类分级标识、数据加密、数据脱敏、去标识化、匿名化、数据访问权限控制、数据流动记录、操作行为记录、数据备份与恢复、数据销毁删除等管理和技术措施。

6.1.1.6 宜建立数据分类分级标识技术措施，管理数据分类分级清单并实现对各类数据的分类分级标识。

6.1.1.7 宜使用数据管理技术工具定期对相关平台系统数据进行定期扫描，能够发现识别重要数据和个人信息、敏感个人信息，定期对数据加密、脱敏、去标识化等技术措施效果进行验证，确保各类数据处理场景中数据保护的持续有效性和合规性。

6.1.2 重要数据保护扩展要求

6.1.2.1 应对重要数据采取加密等安全防护措施重点保护，核心数据应在重要数据保护的基础上依照有关规定从严保护。

6.1.2.2 宜对重要数据的流转进行跟踪溯源。

6.1.2.3 处理重要数据的数据处理者，应在识别重要数据后的十五个工作日内向市级网信部门备案。备案内容包括：

a) 数据处理者基本信息，数据安全管理机构信息、数据安全负责人姓名和联系方式等；
b) 处理数据的目的、规模、方式、范围、类型、数据来源、存储期限、存储地点、数据处理情况、数据安全措施等，不包括数据内容本身；
c) 国家网信部门和主管、监管部门规定的其他备案内容；
d) 处理数据的目的、范围、类型及数据安全措施有着重大变化的，应当重新备案。

6.2 数据安全风险评估

6.2.1 基本保护要求

6.2.1.1　应制定数据安全风险评估制度，明确评估目的、范围、依据、流程、方法、内容、频率等内容。

6.2.1.2　应定期开展数据安全合规性检查或风险评估，包括但不限于数据安全管理、数据处理活动合规、数据安全防护措施落实、个人信息保护等情况，并根据评估结果进行处置。

6.2.1.3　开展数据共享、交易、委托处理等活动前，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。

6.2.2　重要数据保护扩展要求

涉及处理重要数据的机构，应按照有关规定每年开展一次数据安全风险评估，评估报告留存不少于三年，并向市级网信部门和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，存储期限、存储地点、开展数据处理活动的情况、安全措施的有效性，以及面临的数据安全风险和应对措施等。

6.3　数据访问控制

6.3.1　基本保护要求

6.3.1.1　根据不同数据安全级别，应明确数据访问、操作管理、审计账号权限和处理活动业务系统账号权限的分配、开通、使用、变更、注销等安全管理要求以及审批流程要求。

6.3.1.2　数据处理活动使用的账号权限分配应遵循“职责明确、权限分离、最小特权”原则，并分配最小化数据访问权限。

6.3.1.3　应对数据处理全流程使用的各类账号及对应权限进行记录。账号关联对象包括内部、外部和数据合作方人员，重点关注离职人员账号回收、管理权限变更、沉默账号、复活账号等，并在账号或权限发生变更时及时更新记录。

6.3.1.4　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、传输加密等技术措施。

6.3.1.5　应对数据跨安全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。

6.3.1.6　基于数据分类分级结果和业务场景配置主体对客体的访问控制策略，访问控制粒度应达到：主体为用户级或服务、接口级别，客体为接口、应用功能、文件、数据库表级或数据项级别等。

6.3.1.7　应集中管控账号权限，对账号进行统一身份认证和授权，可采用口令管理、生物识别、数字证书、多因子认证等技术措施。

6.3.2　重要数据保护扩展要求

对重要数据的数据访问接口、数据服务调用以及查询、修改、删除、导出、共享、交换、备份、恢复等应设置严格审批流程和访问控制。

6.4　数据接口安全

6.4.1　基本保护要求

6.4.1.1　应明确数据接口的安全要求、管控措施和控制策略，对数据接口实施调用审批流程。

6.4.1.2　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，对接口不安全输入参数进行限制或过滤。身份标识应具有唯一性，身份鉴别信息具有复杂度要求并定期更换，并采取必要措施防止鉴别信息在网络传输过程中被窃听。

6.4.1.3　应与接口调用方明确数据的使用目的、供应方式、保密约定及数据安全责任等情况。

6.4.1.4　应对相关接口调用行为和数据交互行为进行监测，并进行日志记录。

6.4.1.5　应建立数据接口全生命周期管理机制。定期梳理数据接口，形成接口清单，明确不同接口的类型、数据内容、频次、上下游信息系统等信息，并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）。
6.4.1.6　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，不符合要求的接口应落实整改或关停。
6.4.1.7　宜实现对异常数据接口调用行为自动预警、拦截功能。

6.4.2　重要数据保护扩展要求

对重要数据传输接口的调用应采取严格的层级审批程序，由数据安全负责人进行接口调用审批。

6.5　数据防泄露

6.5.1　基本保护要求

6.5.1.1　应对网络、终端等数据泄露、流转途径进行监控，及时对异常数据操作行为进行预警，实现对异常数据操作行为及时定位和阻断。
6.5.1.2　应定期验证数据防泄露技术措施的有效性。

6.5.2　重要数据保护扩展要求

无重要数据保护扩展要求。

6.6　数据脱敏

6.6.1　基本保护要求

6.6.1.1　应制定数据脱敏制度，明确数据脱敏处理的应用场景、处理流程、脱敏规则、脱敏方法、操作记录和脱敏数据的使用限制等要求。
6.6.1.2　应建立静态数据脱敏和动态数据脱敏的技术能力。
6.6.1.3　应定期对开发测试、人员信息公示等应用场景的数据脱敏开展有效性验证。

6.6.2　重要数据保护扩展要求

无重要数据保护扩展要求。

6.7　数据安全审计

6.7.1　基本保护要求

6.7.1.1　应制定数据安全审计制度，审计覆盖数据处理活动各环节，明确审计策略、审计对象、审计内容、审计流程、审计周期、审计结果、审计问题跟踪、审计材料留存时间以及日志记录访问权限控制等要求。
6.7.1.2　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、MAC 地址、操作账号、操作内容、操作结果等，并对日志进行备份，防止数据安全事件导致的日志被删除。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。
6.7.1.3　应定期对数据处理活动各环节的数据访问和操作进行安全审计，每年至少一次，形成数据安全审计报告。针对异常情况进行复核并处置，留存处置记录。

6.7.2　重要数据保护扩展要求

处理重要数据应对数据访问接口、数据服务调用以及查询、修改、更新、删除、导出、共享、交换、备份、恢复等关键操作进行安全审计，并采取技术措施保护审计记录的完整、准确、真实和有效应用。

6.8 数据安全风险监测预警

6.8.1 基本保护要求

6.8.1.1 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，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。风险类型包括但不限于账号风险、权限风险、异常操作行为、数据库漏洞、应用程序漏洞、数据出境风险、数据暴露面风险等。

6.8.1.2 应建立数据安全风险监测预警机制，设置合理有效的风险监测指标。

6.8.1.3 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。

6.8.1.4 宜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的机密性、完整性、可用性。

6.8.1.5 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。

6.8.1.6 宜采取技术工具对数据安全风险进行收集、分析判断和持续监控预警。

6.8.2 重要数据保护扩展要求

应建立覆盖重要数据处理活动的监测规则，能根据监测指标阈值对异常数据处理活动进行告警，并获取发生的位置、操作以及风险和威胁等信息。

6.9 数据安全应急处置

6.9.1 基本保护要求

6.9.1.1 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。

6.9.1.2 应制定数据安全应急预案。预案包括但不限于数据泄露（丢失）、数据滥用、数据被篡改、数据被损毁、数据违规使用等特定场景，明确责任分工、事件监测、事件定位、事件分级、触发、处置措施、报告、应急总结等流程。

6.9.1.3 根据应急预案明确的数据安全事件场景，应每年至少开展一次应急演练，检验和完善应急处置机制，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。

6.9.1.4 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，及时告知相关权利人，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。

6.9.1.5 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。

6.9.1.6 关键信息基础设施发生数据泄露时，应及时上报关键信息基础设施安全保护工作部门。

6.9.1.7 应跟踪和记录数据收集、分析、加工、挖掘等处理过程，实现数据安全事件可溯源。

6.9.1.8 宜采取技术手段对数据安全事件的日志或流量进行关联分析，并保证溯源数据的真实性和保密性。

6.9.2 重要数据保护扩展要求

发生重要数据的数据泄露、毁损、丢失等数据安全事件时，应按规定及时向市级网信部门和有关主管部门报告事件情况，包括涉及的重要数据数量、类型、可能的影响、已经或拟采取的处置措施等，并在事件处置完毕后5个工作日内报告事件原因、危害后果、责任处置、改进措施等情况。

6.10 网络安全等级保护

6.10.1 基本保护要求

应落实网络安全等级保护制度，按要求开展网络定级备案、安全建设整改、等级测评和自查等工作。

6.10.2 重要数据保护扩展要求

处理重要数据和100万人及以上个人信息的信息系统应满足三级及以上网络安全等级保护要求。

7 网络数据处理活动安全要求

7.1 数据收集安全

7.1.1 基本保护要求

7.1.1.1 应明确数据收集的目的、规模、用途、范围、类型、渠道、频度、存储期限、存储地点以及相关的流程和方式，并规范数据格式、数据质量、有效性等原则要求，保证数据收集的合法性、正当性、必要性、一致性。

7.1.1.2 应对数据收集的数据源进行鉴别和记录。对收集的数据需要进行数据来源标识，以便在必要时对数据源进行追踪和溯源，防止数据仿冒和数据伪造。

7.1.1.3 应根据数据分类分级制度和方法，对生成或收集的数据进行分类分级标识，并采取相应级别的安全管控措施。

7.1.1.4 针对外部机构数据源，应要求外部数据提供方说明数据来源，并对信息来源的合法性、合规性进行鉴别，确保数据收集渠道的合法性和正当性。

7.1.1.5 收集外部机构数据前，宜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。

7.1.2 重要数据保护扩展要求

7.1.2.1 应采取加密、访问控制等安全措施保证数据收集过程中重要数据不被泄露。

7.1.2.2 在收集重要数据前应进行安全评估，评估内容包括收集数据的目的、范围、频度、方式、存储期限等是否符合法律法规的规定。

7.2 数据存储安全

7.2.1 基本保护要求

7.2.1.1 应制定数据存储管理制度，对安全管控措施、数据访问流程、访问控制、介质管理、存储时限等作出规定。

7.2.1.2 应针对不同类别级别的数据采取差异化安全存储保护措施，如加密、脱敏、备份、访问控制、数字水印、完整性校验、安全配置、日志管理等。

7.2.1.3 应针对数据存储介质提供有效的技术和管理手段，防止对介质的不当使用而引发的数据泄露风险。存储介质应进行安全性检测，在确保安全的情况下方可使用。

7.2.1.4 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、数据恢复性验证机制等。

7.2.1.5 应建立数据备份与恢复功能，定期开展数据备份及恢复测试，保障数据的可用性与完整性。

7.2.1.6 宜具备勒索病毒事前预警、事中阻断及事后恢复的保障能力。

7.2.1.7 宜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。

7.2.1.8　宜建立异地灾难备份中心，提供数据的实时切换。

7.2.2　重要数据保护扩展要求

7.2.2.1　应采用加密技术对重要数据进行保密性和完整性保护。
7.2.2.2　应在中国境内存储境内收集和产生的重要数据。
7.2.2.3　对重要数据的存储区域应采取严格的访问控制，对不同区域之间的数据流动开展安全管控。
7.2.2.4　存储重要数据应不得超过与重要数据主体约定的存储期限，超存储期限或已达到目的的重要数据应及时销毁。
7.2.2.5　应提供异地数据备份功能，利用通信网络将重要数据实时备份至备份场地。

7.3　数据使用安全

7.3.1　基本保护要求

7.3.1.1　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，在保障安全、数据合法正、当使用的情况下开展数据利用。
7.3.1.2　应根据不同数据使用场景和数据安全等级明确安全管理要求，采用相应级别的安全措施（如去标识化、匿名化、脱敏、数据访问控制、加密、数据防泄露等），并采取技术措施保证汇聚大量数据时不暴露敏感信息，降低数据敏感度及暴露风险。
7.3.1.3　如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。
7.3.1.4　利用所掌握的数据资源公开市场预测、统计等信息时，应不存在危害国家安全、公共安全、经济安全和社会稳定的情况。
7.3.1.5　应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。
7.3.1.6　应完整记录数据使用过程的操作日志，以备对潜在违约使用者责任的识别和追责。
7.3.1.7　生产环境应与测试环境隔离。测试数据应脱敏，并定期清理。

7.3.2　重要数据保护扩展要求

7.3.2.1　应制定重要数据使用的审批制度，明确审批流程、审批内容、安全评估等，并执行及保存审批和评估记录 3 年以上。
7.3.2.2　在使用重要数据前应进行安全评估，评估内容包括目的、范围、方式、安全措施等，确保合法、正当、必要、安全使用重要数据。
7.3.2.3　应对重要数据使用实施严格的访问控制策略和制度，实施安全保护措施。
7.3.2.4　重要数据批量查询、批量修改、批量导出时，应建立多层级的审批程序，并进行记录。

7.4　数据加工安全

7.4.1　基本保护要求

7.4.1.1　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。
7.4.1.2　在数据加工前，应明确数据加工目的、范围、期限、规则及数据加工主体的责任与义务。
7.4.1.3　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。
7.4.1.4　开展数据加工活动，应采取访问控制、数据防泄露、日志留存、安全审计等安全措施确保过程安全、合规可控、可溯源。

7.4.1.5　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，约定委托加工处理的目的、期限、处理方式、数据种类、保护措施，以及第三方接收、返还或删除数据的方式等，并对处理活动进行监督。
7.4.1.6　对数据加工的过程应进行评估与监控，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。
7.4.1.7　对数据加工结果应进行风险评估，确保新数据合法、正当。
7.4.1.8　应提供安全的数据加工环境，包括网络环境、物理环境等，避免因加工活动产生数据泄露、数据破坏等安全风险。

7.4.2　重要数据保护扩展要求

7.4.2.1　应制定重要数据加工的审批制度，明确审批流程、审批内容、安全评估等，并执行及保存审批和评估记录 3 年以上。
7.4.2.2　在加工重要数据前应进行安全评估，评估内容包括目的、范围、方式、安全措施等，确保合法、正当、必要、安全加工重要数据。

7.5　数据传输安全

7.5.1　基本保护要求

7.5.1.1　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、数据传输终端身份鉴别等。
7.5.1.2　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。
7.5.1.3　应采用加密技术保证数据在传输过程中的保密性。
7.5.1.4　应采用校验技术保证数据在传输过程中的完整性。
7.5.1.5　宜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。
7.5.1.6　在可能涉及法律责任认定的应用中，宜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。

7.5.2　重要数据保护扩展要求

传输重要数据时，应采用加密、签名、防重放等安全措施。

7.6　数据提供安全

7.6.1　基本保护要求

7.6.1.1　向他人提供数据前，应进行风险评估，并采取有效的相应安全级别的保护措施。
7.6.1.2　共享、转让、委托处理数据的，应与数据接收方通过合同等方式，明确数据使用目的、供应方式、保密约定、范围、数据安全保护要求等内容，规定数据接收方的责任、义务并进行监督，留存共享、转让情况及安全管理记录。
7.6.1.3　发生收购、兼并、重组、破产时，应通过合同等方式明确数据接收方应继续履行相关数据安全保护义务；没有数据接收方的，应以收集数据时与相关方约定的形式返还、删除原始数据及其加工结果。
7.6.1.4　数据交易应按照相关法律、法规、规章的要求开展，加强交易过程的数据安全保护。
7.6.1.5　应具备数据提供场景的数据溯源能力（如对数据进行签名、添加数字水印等），确保共享、转让数据可溯源。
7.6.1.6　宜采用数据空间、隐私计算、数据沙箱、数字身份等技术实现数据流通的安全性。

7.6.1.7　数据出境应遵守以下要求：

a)　明确数据出境业务场景，并严格遵守国家法律、行政法规数据出境安全监管要求，根据符合的情形，提前开展数据出境的安全评估、安全认证和标准合同及网络安全审查工作，严禁未授权数据出境行为；

b)　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；

c)　境内用户在境内访问境内网络的，其流量不应路由至境外。

7.6.2　重要数据保护扩展要求

7.6.2.1　应制定重要数据提供的审批制度，明确审批流程、审批内容、安全评估等，并执行及保存审批和评估记录 3 年以上。

7.6.2.2　在对外共享、转让、交易、委托处理等重要数据提供活动前，应进行安全评估，评估内容包括目的、范围、方式、数量、安全措施、接收方情况等，确保合法、正当、必要、安全。

7.6.2.3　提供重要数据，应采取加密等安全措施。

7.7　数据公开安全

7.7.1　基本保护要求

7.7.1.1　应制定数据公开的安全制度和审核流程，明确公开数据的内容与种类、公开方式、公开范围、公开时效、安全保障措施、可能的风险与影响范围等。

7.7.1.2　数据公开前应开展数据安全风险评估，涉及商业秘密信息的，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）。

7.7.1.3　应定期审查公开发布的数据及其衍生数据中是否含有非公开信息。

7.7.2　重要数据保护扩展要求

应定期更新和评估已公开的重要数据，对不适宜继续公开或者超出公开期限的数据进行召回或者销毁处理。

7.8　数据删除与销毁安全

7.8.1　基本保护要求

7.8.1.1　应建立数据销毁规程，明确数据删除与销毁场景、方式及审批机制，设置相关监督角色，记录数据删除与销毁操作过程（包括操作人、操作时间、操作内容、操作方式等）。

7.8.1.2　应建立数据存储介质的销毁管理制度，明确存储介质销毁处理策略、流程、技术措施、销毁方法等，并记录存储介质销毁操作过程。

7.8.1.3　有下列情形之一的，应当主动删除数据：

a)　数据处理目的已实现、无法实现或者不再必要；

b)　停止履行相关职能或者提供服务；

c)　数据保存期限已到期；

d)　违反法律、法规、规章及相关规定处理数据；

e)　因安全等原因需要进行回收处理的数据；

f)　法律、法规、规章规定的其他情形。

从技术上难以实现删除的，应停止除存储和采取必要的安全保护措施之外的处理活动。

7.8.1.4　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删除与销毁，如物理粉碎、消磁、多次擦写等。

7.8.1.5　应在中国境内对数据进行删除和对存储介质进行销毁。
7.8.1.6　应明确数据删除与销毁效果评估机制，对数据删除与销毁效果进行认定，通过数据恢复工具或数据发现工具进行数据的尝试恢复及检查，验证数据删除与销毁结果的有效性。

7.8.2　重要数据保护扩展要求

7.8.2.1　应建立重要数据删除与销毁评估与审批机制，对需删除的重要数据范围、理由、数量、采取安全措施、再利用的可能性等方面开展评估，并经数据安全负责人批准。
7.8.2.2　应对重要数据删除与销毁过程留存审计日志，记录数据删除的审批、实施过程，以及被删除数据的具体情况。
7.8.2.3　在删除重要数据后，应及时更新重要数据清单和目录。
7.8.2.4　存储重要数据的介质进行报废处理时，应采用物理损毁等方式销毁介质，以确保重要数据不能被恢复。

8　个人信息保护扩展要求

8.1　个人信息保护一般要求

8.1.1.1　处理个人信息，应同时满足本章和本文件第 5 章至第 7 章的基本保护要求。
8.1.1.2　处理 100 万人及以上个人信息，应同时满足本章和本文件第 5 章至第 7 章的所有要求。

8.2　个人信息保护管理要求

8.2.1　个人信息保护管理组织

8.2.1.1　应通过正式文件或制度明确法定代表人或主要负责人对个人信息保护负全面领导责任。
8.2.1.2　应明确个人信息保护工作机构及负责人，全面统筹实施组织内部的个人信息安全工作，对个人信息安全负直接责任。
8.2.1.3　处理个人信息满足以下条件之一的，应通过正式文件或制度明确专职个人信息保护工作机构和个人信息保护负责人，并公开个人信息保护负责人的联系方式，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：

a)　主要业务涉及个人信息，且从业人员规模大于 200 人；
b)　处理超过 100 万人个人信息，或预计在 12 个月内处理超过 100 万人及以上的个人信息；
c)　处理超过 10 万人及以上敏感个人信息。

8.2.1.4　运营大型互联网平台时，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。
8.2.1.5　境外个人信息处理者应明确境内专门个人信息保护机构或指定个人信息保护负责人，负责处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送履行个人信息保护职责的部门。

8.2.2　个人信息保护管理制度

8.2.2.1　个人信息处理者应制定和发布个人信息保护管理制度和操作规程，严格执行并定期评审更新。内容包括个人信息分类管理、权限管理、个人信息保护影响评估、合规审计、儿童个人信息保护等。
8.2.2.2　宜每年按要求制定个人信息保护工作计划，并组织按时完成，留存相关记录，留存时间符合法律法规的要求。

8.2.3　个人信息保护人员管理与教育培训

8.2.3.1　应对接触个人信息或敏感个人信息人员进行资格审查、签署保密协议、审批和登记，并明确岗位职责、数据访问范围、操作权限、人员调离保密要求、保密期限、违约责任等，定期审查其行为，有效约束其数据操作行为。

8.2.3.2　对处理大量个人信息或敏感个人信息的人员，应每年开展个人信息安全培训考核，依据考核结果确定任职资格。

8.2.4　个人信息保护投诉举报管理

8.2.4.1　应向个人信息主体提供针对自动化决策结果的投诉渠道，并支持对自动化决策结果的人工复核。

8.2.4.2　应要求涉及个人信息的第三方产品或服务方建立响应个人信息主体请求和投诉机制，以供个人信息主体查询、使用。

8.2.5　个人信息安全应急处置

8.2.5.1　个人信息处理者应制定个人信息安全事件应急预案，发生个人信息安全事件或发生个人信息安全事件风险明显加大时，应立即启动应急预案，采取相应的应急处置措施及补救措施，及时以电话、短信、邮件或信函等方式告知个人信息主体及相关权利人，并记录事件全过程。

8.2.5.2　发生 10 万人及以上个人信息数据泄露、毁损、丢失等数据安全事件时，应按规定及时向市级网信部门和有关主管部门报告事件情况，包括涉及的个人信息数量、类型、可能的影响、已经或拟采取的处置措施等，并在事件处置完毕后 5 个工作日内报告事件原因、危害后果、责任处置、改进措施等情况。

8.2.6　个人信息保护认证

宜开展个人信息保护认证工作，通过认证方式提升个人信息保护能力。

8.2.7　个人信息保护合规审计

处理个人信息应定期（处理超过100万人个人信息的应每年至少一次，其他每两年至少一次）对个人信息保护政策、相关规程和安全措施的有效性及合规性进行审计，及时处理审计过程中发现的个人信息违规使用、滥用等情况，并留存审计记录。

8.3　个人信息处理安全要求

8.3.1　个人信息收集安全

8.3.1.1　应遵循合法、正当、必要和诚信原则，不收集与其提供的服务无直接或无合理关联，或超出个人信息主体明示同意期限的个人信息，且遵守以下收集要求：

a)　应制定和公开个人信息保护保护政策并严格遵守，政策内容应符合 GB/T 35273—2020 中 5.5 的要求；
b)　收集前明示政策，征得主体同意（GB/T 35273—2020 中 5.6 规定情形除外）；
c)　改变及时告知，修改政策并重新征得同意，改变涵盖目的、类型、范围、用途；
d)　明示产品服务类型，不得以用户不同意收集非必要个人信息为由拒绝服务；
e)　不应以改善服务质量、提升用户体验、定向推送信息、研发新产品等为目的，强制要求、误导用户同意收集；
f)　收集敏感个人信息前，应取得主体单独同意，确保完全知情、意愿自主；

g) 收集不满 14 周岁未成年人个人信息前，应向未成年人及其监护人告知处理目的、处理方式、处理必要性及个人信息种类、所采取的防护措施，并取得监护人单独同意；
h) 开启自主选择功能，仅在主体自主选择后才开始收集个人信息；
i) 要求提供方说明个人信息来源与主体授权同意的范围。

8.3.1.2 应采取加密、访问控制等安全措施保证数据收集过程中个人信息不被泄露。

8.3.1.3 个人信息处理者在公共场所安装图像采集、个人身份识别设备的，应确保是为维护公共安全所必需，并设置显著提示标志，若用于维护公共安全以外用途的，应取得个人单独同意。

8.3.2 个人信息存储安全

8.3.2.1 个人信息存储期限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。

8.3.2.2 存储个人生物识别信息（如样本、图像等）时，应仅存储摘要信息，并将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，应遵守 GB/T 35273－2020 中 6.3 b)和 c)的要求及生物特征识别信息保护相关国家标准要求）。

8.3.2.3 境内收集的个人信息应在境内存储。

8.3.2.4 应加密存储敏感个人信息。

8.3.2.5 个人信息应去标识化存储，并将可用于恢复识别个人的信息与去标识化后的信息分开存储并加强访问和使用的权限管理。

8.3.3 个人信息使用安全

8.3.3.1 不应超出收集个人信息时明示的目的、范围使用个人信息，需要超出范围使用的应取得再次同意。

8.3.3.2 应对被授权访问个人信息的人员，建立最小授权的访问控制策略。

8.3.3.3 对个人信息传输接口的调用应采取严格的审批程序和访问控制。

8.3.3.4 对个人信息的批量修改、拷贝、删除、下载等重大操作行为，应设置内部审批和审计流程，执行并记录操作行为。

8.3.3.5 应在对角色权限控制的基础上，对敏感个人信息的访问、修改、删除、导出等操作行为，按照业务流程的需求触发操作授权，并定期针对敏感个人信息的访问、修改、删除、导出等操作进行日志审计。

8.3.3.6 确因工作需要，需授权特定人员超权限处理个人信息的，应经个人信息保护负责人或个人信息保护工作机构进行审批，并记录在册。

8.3.3.7 应对需展示的个人信息采取去标识化处理等措施，降低个人信息在展示环节的泄露风险。

8.3.3.8 自动化决策机制的使用应保证决策的透明度和结果公平、公正，同时应满足以下要求：

a) 使用前及使用期间（至少每年一次）开展个人信息安全影响评估；
b) 向个人进行信息推送、商业营销等应同时提供不针对其个人特征的选项或者向个人提供便捷的拒绝方式；
c) 提供针对自动化决策结果的投诉渠道，并支持对自动化决策结果的人工复核；
d) 使用用户画像时，应消除明确身份指向性，尽量避免精确定位到特定个人（宜使用间接用户画像）；不应包含色情、赌博、迷信、恐怖、暴力及表达对民族、种族、宗教、疾病歧视等内容的特征描述；不应侵害公民、法人和其他组织的合法权益，危害国家安全和公共利益。

8.3.4 个人信息加工安全

委托加工处理个人信息的，应通过合同方式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，准确记录和存储委托处理个人信息的情况，对受托人的个人信息处理活动进行监督、审计，不得超出已征得个人信息主体授权同意的范围。

8.3.5 个人信息传输安全

传输个人敏感信息时，应该采取加密等安全措施。

8.3.6 个人信息提供安全

8.3.6.1 个人信息对外提供场景包括委托处理、共享、转让、交易、出境等场景。

8.3.6.2 个人信息处理者对外提供个人信息时，应与接收方签订合同或协议，约定提供数据的目的、期限、方式及个人信息的种类、接收方应当采取的技术措施和管理措施、双方的权利义务等；

8.3.6.3 个人信息处理者对外提供个人信息时，应向个人信息主体告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类、存储期限、数据接收方的身份和数据安全能力以及可能产生的后果，并取得个人信息主体同意（GB/T 35273—2020 中 9.5 规定情形除外）。

8.3.6.4 接收方应在双方约定的处理目的、处理方式和个人信息的种类等范围内处理个人信息。变更处理目的、处理方式的，应依照法律、行政法规规定重新取得个人同意。

8.3.6.5 个人信息处理者对外提供敏感个人信息时，应建立数据提供审批流程，并视具体场景采取脱敏、加密等安全防护措施。

8.3.6.6 个人信息处理者在委托处理个人信息时，应采取定期检查等方式，对受托方的个人信息处理活动进行监督，以确保委托处理个人信息的活动符合法律规定。

8.3.6.7 当委托合同不生效、无效、被撤销或者终止时，受托人应将个人信息返还个人信息处理者或者予以删除。

8.3.6.8 个人信息处理者存在因合并、重组、分立、解散、被宣告破产等原因需要转移个人信息情形的，应向个人信息主体告知接收方的名称或者姓名和联系方式，接收方变更原先处理目的、处理方式的，应依照法律、行政法规有关规定重新取得个人同意。

8.3.6.9 个人信息处理者向境外提供个人信息时，除满足 7.6.1.7 的要求外，还应满足下列要求：

a) 明确个人信息出境业务场景，并严格遵守国家法律、行政法规数据出境安全监管要求，根据符合的情形，提前开展个人信息出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证等工作（可豁免出境场景除外），严禁未授权个人信息出境行为；
b) 向外国司法或者执法机构提供存储于中华人民共和国境内的个人信息必须经过中华人民共和国主管机关批准；
c) 不得违规向被列入限制或者禁止个人信息提供清单的组织和个人提供个人信息；
d) 个人信息处理者向境外提供个人信息，应当采取必要措施，保障境外接收方处理个人信息的活动达到法律法规要求的个人信息保护标准。

8.3.7 个人信息公开安全

8.3.7.1 个人信息不应公开披露，取得个人单独同意的除外。经法律授权或具备合理事由确需公开披露的，应遵循 GB/T 35273—2020 中 9.4 规定要求。

8.3.7.2 个人信息处理者处理已公开个人信息的，不应对已公开个人信息进行以下违规行为：

a) 向已公开个人信息中的电子邮箱、手机号等发送与其公开目的无关的信息；
b) 利用已公开的个人信息从事网络暴力活动；
c) 处理个人明确拒绝处理的已公开个人信息；
d) 未取得个人信息主体同意处理已公开个人信息对个人权益造成重大影响。

8.3.8 个人信息删除与销毁安全

8.3.8.1 符合 GB/T 35273—2020 中 8.3 的要求或符合以下情形时，应及时对个人信息做删除或者匿名化处理：

a) 个人信息超出双方约定的存储期限；
b) 网络产品和服务停止运营；
c) 个人信息主体注销账号，或者当用户撤回同意。

8.3.8.2 存储个人信息的介质进行报废处理时，应采用物理损毁等方式销毁介质，以确保个人信息不能被恢复。

8.3.8.3 当个人信息处理者停止运营产品或服务时，应及时停止收集个人信息，以逐一送达或公告的形式通知个人信息主体，并及时删除或匿名化处理所持有的个人信息。

8.3.9 个人信息共同处理安全

两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的，应通过合同等形式约定各自的权利和义务，明确应共同满足的安全要求、双方分别承担的责任和义务等，并向个人信息主体明确告知。

8.3.10 个人信息保护影响评估

8.3.10.1 应建立个人信息保护影响评估及风险处置机制。当处理敏感个人信息、利用个人信息自动化决策、汇聚融合、委托处理、向他人提供（含境外）或公开个人信息，及其他对个人权益有重大影响等个人信息处理活动时，应事先开展个人信息保护影响评估，形成评估报告，并采取有效的措施进行处置，使安全风险降低到可接受水平。

8.3.10.2 在使用个人信息自动化决策过程中，应定期（至少每年一次）开展个人信息安全影响评估，并依评估结果改进保护个人信息主体的措施。

8.3.10.3 个人信息保护影响评估报告及处理情况记录应保存至少三年。

8.3.11 大型互联网平台

运营大型互联网平台时，应明确平台内产品或者服务提供者处理个人信息的规范和保护个人信息的义务并对其做好监督管理，对严重违规者停止提供服务，并定期（至少每年一次）发布个人信息保护社会责任报告，接受社会监督。

8.4 个人信息主体的权利

应建立个人信息主体权利保护的渠道，遵从GB/T 35273—2020中8的要求，为个人信息主体提供以下功能服务：

a) 提供查询个人信息的类型、来源、用途目的及已获取的第三方；
b) 提供请求更正或补充个人信息的方法；
c) 提供注销账户的方法，且方法简便易操作；
d) 提供撤回收集、使用其个人信息的授权同意的方法；
e) 提供获取个人信息基本资料、身份信息、健康生理信息、教育工作信息副本的方法；
f) 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。

参 考 文 献

[1] GB/T 20984—2022 信息安全技术 信息安全风险评估方法
[2] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[3] GB/T 22240—2020 信息安全技术 网络安全等级保护定级指南
[4] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型
[5] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[6] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
[7] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[8] GB/T 43697—2024 数据安全技术 数据分类分级规则
[9] TC260-PG-20231A 网络安全标准实践指南—网络数据安全风险评估实施指引