ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 41479—2022

信息安全技术　网络数据处理安全要求

Information security technology—Network data processing security requirements

2022-04-15 发布　　2022-11-01 实施

国家市场监督管理总局
国家标准化管理委员会　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。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国网络安全审查技术与认证中心、中国电子技术标准化研究院、清华大学、国家信息中心、国家计算机网络应急技术处理协调中心、公安部第三研究所、中国信息通信研究院、陕西省网络与信息安全测评中心、中电长城网际系统应用有限公司。

本文件主要起草人：魏昊、吴晓龙、程瑜琦、上官晓丽、胡影、刘贤刚、闵京华、金涛、王佳慧、郑礼雄、任卫红、陈湉、徐羽佳、张宇光、张剑、魏立茹、陈世翔、樊华、杨向东。

信息安全技术　网络数据处理安全要求

1　范围

本文件规定了网络运营者开展网络数据收集、存储、使用、加工、传输、提供、公开等数据处理的安全技术与管理要求。

本文件适用于网络运营者规范网络数据处理，以及监管部门、第三方评估机构对网络数据处理进行监督管理和评估。

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 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

3　术语与定义

GB/T 25069 和 GB/T 35273—2020 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。

示例：个人信息、重要数据等。

3.3

数据处理　data processing

数据的收集、存储、使用、加工、传输、提供、公开等。

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

网络运营者　network operator

网络的所有者、管理者和网络服务提供者。

注：本文件中的网络为开放公共网络。

3.6

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：个人信息包括姓名、出生日期、公民身份号码、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。

注2：不包括匿名化处理后的信息。

[来源：GB/T 35273—2020，3.1，有修改]

3.7

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。

3.8

个人信息主体　personal information subject

个人信息已识别或者可识别的自然人。

[来源：GB/T 35273—2020，3.3，有修改]

3.9

重要数据　important 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：重要数据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。

3.10

私人信息　private information

个人发送给特定对象不可转发给其他人的信息。

3.11

数据接收方　data receiver

数据处理中接收数据的组织或者个人。

3.12

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。

3.13

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。

4　数据处理安全总体要求

4.1　数据识别

网络运营者应识别数据处理中涉及的数据，包括个人信息、重要数据和其他数据，形成数据保护目

录，并及时更新。

4.2 分类分级

网络运营者应按照相关国家标准，根据合同规定和业务运营需要，对所识别的数据进行分类分级管理。

4.3 风险防控

网络运营者开展数据处理时，应按照合同约定履行数据安全保护义务，开展数据处理活动应加强风险监测，发现数据安全缺陷、漏洞等风险时，应采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强数据安全防护，保护数据免受泄露、窃取、篡改、损毁、不正当使用等；对重要数据和敏感个人信息进行重点保护，应按照规定对其数据处理活动定期开展风险评估，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的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等。

应建立数据安全管理责任和评价考核制度，制定数据安全保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训。

4.4 审计追溯

网络运营者应对数据处理的全生存周期进行记录，确保数据处理可审计、可追溯。

5 数据处理安全技术要求

5.1 通则

网络运营者在开展数据处理时应进行影响分析和风险评估，采取必要的措施对识别的风险进行控制，以保障数据安全。在发生突发公共卫生事件时，数据处理还应遵守附录 A 的要求。影响或者可能影响国家安全的数据处理活动应接受国家安全审查。

5.2 收集

网络运营者为提供服务而必需处理个人信息的，应遵循合法、正当、必要的原则，不应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，且遵守以下要求：

a) 应制定和公开个人信息保护政策并严格遵守，个人信息保护政策应符合 GB/T 35273—2020 中 5.5 要求；

b) 收集个人信息前，应明示个人信息保护政策，并征得个人信息主体同意；

注： GB/T 35273—2020 中 5.6 规定的情形除外。

c) 改变处理个人信息的目的、类型、范围、用途的，应及时告知个人信息主体，修改个人信息保护政策，并重新征得个人信息主体同意，涉及个人信息保护政策变动的应修改个人信息保护政策；

d) 明示所提供产品或服务的类型，以及该产品或服务所必需的个人信息，不应因用户不同意或撤回同意，提供该产品或服务所必需个人信息以外的信息，而拒绝提供该产品或服务；

e) 不应仅以改善服务质量、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、误导用户同意收集个人信息；

f) 收集敏感个人信息前，应取得个人信息主体的单独同意，确保单独同意是在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示；

g) 收集不满十四周岁未成年人个人信息前，应取得未成年人的父母或其他监护人的单独同意；

h) 从个人信息主体以外的其他途径获得个人信息的，应了解个人信息来源、个人信息提供方已获得的个人信息处理授权同意范围，并按照本文件的要求履行安全保护义务。

5.3 存储

网络运营者应对数据存储活动采取安全措施，包括：

a) 存储重要数据和个人信息等敏感网络数据，应采用加密、安全存储、访问控制、安全审计等安全措施；

b) 存储重要数据和个人信息，不应超过与重要数据和个人信息主体约定的存储期限或个人信息主体授权同意有效期；

c) 存储个人生物特征识别信息的，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。

数据接收方存储数据时，应按要求采取安全措施并以合同进行约定。

5.4 使用

5.4.1 定向推送及信息合成

网络运营者在为用户提供定向推送或信息合成服务时的要求如下：

a) 网络运营者利用个人信息和算法为用户提供定向推送信息服务的，同时应提供非定向推送信息的服务选项；

注：宜参照 GB/T 35273—2020 的 7.5。

b) 在向个人信息主体提供新闻、博客类信息服务的过程中，网络运营者利用算法自动合成文字、图片、音视频等信息，应明确告知用户。

5.4.2 第三方应用管理

网络运营者应对接入或嵌入其产品或服务的第三方应用加强数据安全管理，包括：

a) 应通过合同等形式，明确双方的数据安全保护责任和义务；

b) 应监督第三方应用运营者加强数据安全管理，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；

c) 网络运营者知道或者应知道第三方应用利用其平台侵害用户民事权益，未采取必要措施的，应与第三方应用运营者承担连带责任；

d) 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。

5.5 加工

网络运营者在开展转换、汇聚、分析等数据加工活动的过程中，知道或者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。

5.6 传输

网络运营者在应对数据传输活动采取安全措施，包括：

a) 传输重要数据和敏感个人信息时，应采用加密、脱敏等安全措施；

b) 向数据接收方传输数据时，应按要求采取安全措施并以合同进行约定。

5.7 提供

5.7.1 向他人提供

网络运营者向他人提供数据前，应进行安全影响分析和风险评估，可能危害国家安全、公共安全、经济安全和社会稳定的，不应向他人提供。要求如下：

a) 向他人提供个人信息，应向个人信息主体告知接收方的名称、联系方式、处理目的、处理方式、个人信息的种类、存储期限，并取得个人信息主体同意；

b) 共享、转让重要数据，应与数据接收方通过合同等形式明确双方的数据安全保护责任和义务，采取加密、脱敏等措施保障重要数据安全；

c) 委托第三方开展数据处理活动的，应通过合同等形式明确约定委托处理的目的、期限、处理方式、数据的种类、保护措施、双方的权利和义务，以及第三方返还或删除数据的方式等，要求第三方以合同中约定的形式返还、删除接收和产生的数据，并对数据处理活动进行监督；

d) 发生收购、兼并、重组、破产时，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，应删除数据。

5.7.2 数据出境

网络运营者向境外提供个人信息或者重要数据的，应遵循国家相关规定和相关标准的要求。

境内用户在境内访问境内网络的，其流量不应路由至境外。

5.8 公开

网络运营者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。

5.9 私人信息和可转发信息的处理方式

即时通信等社交平台运营者宜为用户提供发送私人信息和可转发信息的选项，并按照以下方式处理：

a) 宜对以私人选项发送的信息予以严格保护，不提供转发功能；

b) 宜对以可转发选项发送的信息，或者转发此类信息的，同时发送信息始发者在该平台上的账号名称，该账号名称唯一且不可更改。

5.10 个人信息查阅、更正、删除及用户账号注销

网络运营者应建立渠道和机制，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，不应对请求设置不合理条件，应遵守 GB/T 35273—2020 中 8.7 有关响应个人信息主体请求的要求。

5.11 投诉、举报受理处置

网络运营者应建立投诉、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、举报的，自

接受投诉举报起，受理时间不超过 3d。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。

5.12 访问控制与审计

网络运营者开展数据处理活动时，应：

a) 基于数据分类分级，明确相关人员的访问权限，防止非授权访问。

b) 对重要数据、个人信息的关键操作（例如批量修改、拷贝、删除、下载等），设置内部审批和审计流程，并严格执行。

5.13 数据删除和匿名化处理

符合 GB/T 35273—2020 中 8.3 的要求或符合以下情形时，网络运营者应及时对个人信息做删除或匿名化处理：

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。

存储重要数据和个人信息的介质进行报废处理时，网络运营者应采用物理损毁等方式销毁介质，以确保重要数据和个人信息不能被恢复。

6 数据处理安全管理要求

6.1 数据安全责任人

网络运营者开展经营和服务活动，处理重要数据和敏感个人信息的，应明确数据安全责任人，并为其提供必要的资源保障，保证其独立履行职责。数据安全责任人应具备数据安全专业知识和相关管理工作经历，参与有关数据处理的重要决策，履行以下职责：

a) 组织确定数据保护目录，制定数据安全保护计划并督促落实；

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) 依法向有关部门报告数据安全保护和事件处置情况；

d) 组织受理和处置数据安全投诉、举报。

6.2 人力资源保障与考核

在人力资源保障与考核方面，网络运营者应：

a) 明确数据安全保护岗位及职责，并提供人力资源保障。

b) 建立人力资源考核制度，明确数据安全管理考核指标和问责机制，对相关人员特别是重要岗位人员的履职情况进行考核。出现数据安全重大事件时，对直接负责的主管人员和其他直接责任人员进行问责。

6.3 事件应急处置

网络运营者应建立数据安全事件应急响应机制，并根据数据安全计划的变化而及时调整，确保数据安全事件得到及时有效处置。

a） 应急响应机制包括：

1） 数据安全事件分级；

2） 启动条件；

3） 启动所需的资源，如人员、设备、场所、工具、资金等；

4） 流程、人员安排和操作手册。

b） 配备应急响应所需的资源，确保应急响应机制能够有效实施。

c） 制定应急演练计划，按计划或者在应急响应机制发生变化后，组织开展应急演练，检验和完善应急响应机制，提高实战能力。

发生数据安全事件时，网络运营者应立即启动应急响应机制，采取相应的补救和防范措施。涉及个人信息的，及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的按相关要求向有关部门报告。

附　录　A
（规范性）
突发公共卫生事件个人信息保护要求

A.1　概述

本附录所称突发公共卫生事件，是指依据突发公共卫生事件专项预案启动Ⅰ级（特别重大）、Ⅱ级（重大）响应的事件。

A.2　个人信息服务协议

为应对突发公共卫生事件，由国务院卫生健康行政部门或者省级人民政府有关部门指定的机构（以下称“指定机构”），利用个人信息为社会提供位置、行踪查询等信息服务时，应按照与国务院卫生健康行政部门或者省级人民政府有关部门签订的服务合同或者其他有约束力的协议，履行个人信息保护要求，承担违约责任等。

A.3　个人信息收集

突发公共卫生事件应对中，指定机构收集个人信息的要求包括：

a）　应坚持最小化原则，一般只限于个人信息主体的联系方式、位置、行踪信息；

b）　收集个人信息应遵守本文件 5.2 b）规定的要求，为控制事件扩大、减轻事件危害，不能及时征得个人信息主体同意而必须收集的，应告知收集目的、数据类型、收集方式、存储期限等信息，实现个人信息主体查询、更正、删除，以及获取个人信息副本等权利的途径，由指定机构依法实施并经相关应急指挥部门或者国务院卫生健康行政部门同意。

A.4　个人信息调用

为控制事件扩大、减轻事件危害，指定机构确需调用已经收集的个人信息，应坚持最小化原则，根据应对突发公共卫生事件实际需要，严格限定调用个人信息的范围、规模、数量以及行踪信息的回溯时间跨度。应经相关指挥部门同意，或者由国务院卫生健康行政部门会同相关行业管理部门同意，并明确调用个人信息的范围、类型及程序，并告知个人信息主体。

A.5　人脸识别验证

指定机构在提供信息服务过程中，以人脸识别作为身份验证方式时，宜提供其他身份验证方式供用户选择。

利用人脸识别信息进行身份验证的，不宜留存可提取人脸识别信息的原始图像。

A.6　信息查阅服务

指定机构提供信息查阅服务，应通过境内手机号码等能够确认身份的方式核验查阅人身份，防止非授权查阅他人个人信息。

A.7　公开、向他人提供个人信息及改变个人信息用途

指定机构收集掌握的个人信息，未经个人信息主体同意，不得公开或者非法向他人提供，不得改变

用途。确需公开、向他人提供或者改变用途的，应征得个人信息主体同意，紧急或不便征得同意时报应急指挥部门或者国务院卫生健康行政部门同意，并及时告知个人信息主体。

指定机构不应利用已掌握的个人信息或者提供信息服务的便利条件谋取商业利益，包括进行市场营销、定向推送广告等。

A.8 应对工作结束后的个人信息处理

突发公共卫生事件应对工作结束后，指定机构应停止收集、调用个人信息，并在 60d 内或者国务院卫生健康行政部门规定的时限内删除在突发公共卫生事件应对中已收集、调用的个人信息。

A.9 日志留存

指定机构应保存个人信息收集、调用、使用活动的日志，保存期限不少于突发公共卫生事件应对工作结束后的 6 个月。

参 考 文 献

[1] GB/T 22080—2016 信息技术 安全技术 信息安全管理体系 要求

[2] GB/T 29246—2017 信息技术 安全技术 信息安全管理体系 概述和词汇

[3] GB/T 30146—2013 公共安全 业务连续性管理体系 要求

[4] GB/T 31168—2014 信息安全技术 云计算服务安全能力要求

[5] ISO/IEC 20000-1:2018 Information technology—Service management—Part1:Service management system requirements

[6] Business Continuity Glossary,DRI International

[7] NIST SP 800—34 Contingency Planning Guide for Information Technology System

[8] Professional Practices for Business Continuity Planners,DRI International

[9] SS 507:2008 SINGAPORE STANDARD for Business continuity/disaster recovery (BC/DR) service providers