ICS 35.040
L 80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 网络数据处理安全规范

Information security technology－Cyber-data process security specification

（征求意见稿）

本稿完成时间：2020 年 8 月 27 日

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX-XX-XX 发布　　XXXX-XX-XX 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。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件主要起草单位：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、中国科学院信息工程研究所、中国电子信息产业发展研究院、中国软件测评中心、陕西省网络与信息安全测评中心、北京优炫软件股份有限公司、陕西省信息化工程研究院、国家工业信息安全发展研究中心、北京北信源软件股份有限公司、浙江华途信息安全技术股份有限公司、北京神州绿盟科技有限公司、上海安言信息技术有限公司、四川无国界信息技术有限公司、全知科技、联想（北京）有限公司、成都思维世纪科技有限责任公司、中信银行股份有限公司、新华三技术有限公司、中国移动集团有限公司、赛迪（青岛）区块链研究院有限公司、广东移动通信有限公司、北京天融信网络安全技术有限公司、广州赛宝认证中心服务有限公司、科盈法律咨询（上海）有限公司、上海市方达(北京)律师事务所、启明星辰信息技术集团股份有限公司、中认信安（北京）技术服务有限公司、北京赛西认证有限责任公司等。

本文件主要起草人：魏昊、胡影、程瑜琦、刘贤刚、闵京华、金涛、任卫红、闫少敏、付艳艳、冷杉、陈立彤、曹宇、张宇光、徐羽佳、张剑、魏立茹、陈世翔等。

信息安全技术 网络数据处理安全规范

1 范围

本文件规定了网络运营者利用网络开展数据收集、存储、使用、加工、传输、提供、公开等数据处理活动应遵循的规范和安全要求。

本文件适用于网络运营者规范数据处理活动，提高数据安全管理和个人信息保护水平，也适用于主管监管部门对网络运营者数据处理活动进行监督管理，同时还可为第三方评估机构开展相关评估工作提供指导。

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 22080 信息技术 安全技术 信息安全管理体系 要求

GB/T 25069 信息安全技术 术语

GB/T 35273 信息安全技术 个人信息安全规范

3 术语和定义

GB/T 25069、GB/T 35273和GB/T 22080界定的以及下列术语和定义适用于本文件。

3.1

数据 data

本文件所称数据是指网络数据，即通过网络处理和产生的各种电子数据，如个人信息、重要数据等。

3.2

网络运营者 network operator

网络的所有者、管理者和网络服务提供者。

3.3

个人信息 personal information

以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息。

注：个人信息包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

[来源：GB/T 35273—2020，3.1，有修改]

3.4

个人敏感信息 personal sensitive information

一旦泄露、非法提供或者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者歧视性待遇等的个人信息。

注：个人敏感信息包括自然人的身份证件号码、生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪信息、住址、健康信息、交易信息、14 岁以下（含）儿童的个人信息等。

[来源：GB/T 35273—2020，3.2，有修改]

3.5

个人信息主体 personal data subject

个人信息能够识别或者关联到的自然人。

[来源：GB/T 35273—2020，3.3，有修改]

3.6

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，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。

3.7

数据提供方 data provider

数据处理活动中提供数据的组织或者个人。

3.8

数据接收方 data receiver

数据处理活动中接收数据的组织或者个人。

3.9

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的自动化工具，包括但不限于软件开发工具包（SDK等）、第三方代码、组件、脚本、接口、算法模型、小程序等。

3.10

匿名化 anonymization

是指对个人信息进行加工，使之无法识别特定个人且不能复原。

[来源：GB/T 35273—2020，3.14，有修改]

4 数据处理总体要求

4.1 数据识别

网络运营者应识别数据处理活动中涉及的数据，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 分级分类

网络运营者应按照法律法规、国家标准有关要求，根据业务运营需要，对所掌握的数据进行分级分类管理；采取加密、脱敏、访问控制等措施，对重要数据和个人信息进行重点保护。

4.3 风险防控

网络运营者开展数据处理活动，应按照有关法律法规的规定履行数据安全保护义务，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。

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活动的全生命周期进行记录，确保数据处理活动可审计、可追溯。

5 数据处理

5.1 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，不得收集与其提供的服务无直接关联的个人信息，且符合以下要求：

a) 制定、公开个个人信息保护政策并严格遵守，个人信息保护政策应满足GB/T 35273 5.5 有关个人信息保护政策的要求；
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，法律法规另有规定的除外；
c) 改变处理个人信息的目的、类型、范围、用途的，应修改个人信息保护政策，并重新征得个人信息主体同意；
d) 明示所提供产品和服务类型，以及该类产品和服务所必需的个人信息，不得因用户拒绝提供该类产品和服务所必需的个人信息以外的信息，而拒绝提供服务；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，强制要求用户同意收集个人信息；
e) 收集个人敏感信息前，应征得个人信息主体的明示同意，确保明示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；
f) 收集不满14周岁未成年人个人信息前，应征得其监护人的明示同意；
g) 从个人信息主体以外的其他途径获得个人信息的，应按照本标准的要求履行安全保护义务。

5.2 传输和存储

网络运营者应对数据传输、存储活动采取安全措施，包括：

a) 传输重要数据和个人敏感信息，应采用加密等安全措施；
b) 存储重要数据和个人敏感信息，应采用加密、安全存储、访问控制、安全审计等安全措施；
c) 存储个人信息，不应超出与个人信息主体约定的存储期限，法律法规另有规定的除外；
d) 存储生物识别信息，应满足GB/T 35273 6.3 b）c）的要求。

5.3 加工

网络运营者开展数据加工过程中，发现或者应发现可能危害国家安全、公共安全、经济安全和社会稳定的，应立即停止加工活动并按要求向网信部门和有关部门报告。

5.4 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，不得危害国家安全、公共安全、经济安全和社会稳定。

5.5 定向推送及信息合成

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，应同时提供非定向推送信息服务的选项。

注：可参照GB/T 35273 7.5。

网络运营者利用大数据、机器生产、人工智能等技术自动合成文字、图片、音视频的等信息，应以明显方式提示用户。

5.6 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，及时响应和处理个人信息主体查阅、复制、更正、删除其个人信息及用户注销账号的请求，不应对请求设置不合理条件，应满足GB/T 35273 8.7 有关响应个人信息主体请求的要求。

5.7 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) 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) 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。

5.8 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，应及时查实，并依法采取停止传输、消除等处置措施。

5.9 访问控制与审计

网络运营者开展数据处理活动时，应基于数据分级分类，明确相关人员的访问权限，防止非授权访问。

网络运营者开展数据处理活动时，对重要数据、个人信息的关键操作，如批量修改、拷贝、删除等，应设置内部审批和审计流程，并严格执行。

5.10 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，不得向他人提供。

a) 向他人提供个人信息，应告知向他人提供的目的、类型、方式、范围、用途、存储期限，并征得个人信息主体同意，但是经过匿名化处理的除外；
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加工活动，应与第三方通过合同等形式明确双方的保护责任和义务，要求第三方在委托业务结束时返还并删除接收和产生的数据；

d) 发生兼并、重组、破产，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，应对数据作删除处理。

5.11 数据删除和匿名化处理

当个人信息超出法律法规规定或者双方约定的存储期限，或者网络产品和服务停止运营，或者个人信息主体注销账号后，网络运营者应及时对个人信息作删除或者匿名化处理，法律法规、部门规章另有规定的除外。

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进行销毁，以确保重要数据和个人信息不能被恢复。

5.12 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。

境内用户访问境内网络的，其流量不应被路由至境外。

5.13 第三方应用

网络运营者应对接入其平台的第三方应用加强数据安全管理，包括：

a) 通过合同等形式，明确双方的数据安全保护责任和义务；
b) 督促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要求和责任的，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) 第三方应用之间、第三方应用和平台之间共享个人信息的，应满足本文件5.10a)的要求；

网络运营者对嵌入的第三方自动化工具，如软件开发工具包（SDK等）、第三方代码、组件、脚本、接口、算法模型等，宜开展技术检测确保其个人信息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。

6 安全管理

6.1 数据安全责任人

网络运营者开展经营和服务活动，收集重要数据和个人敏感信息的，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，参与有关数据处理活动的重要决策，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) 按要求向网信部门和有关部门报告数据安全保护和事件处置情况；
d) 组织受理处置数据安全投诉、举报。

6.2 人力资源保障与考核

网络运营者应明确数据安全保护岗位及职责，并提供人力资源保障。

网络运营者应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，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；
d) 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，同时按要求向网信部门和有关部门报告。

7 突发公共卫生事件个人信息保护

7.1 概述

本章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。

7.2 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，应当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。

7.3 个人信息收集

突发公共卫生事件应对中，收集个人信息应事先征得个人信息主体同意。但是，为控制事件扩大、减轻事件危害而必须收集的，由指定机构实施并经全国突发公共卫生事件应急指挥部（以下称“指挥部”）或者国务院卫生健康行政部门同意的除外。

7.4 个人信息调用

为控制事件扩大、减轻事件危害，指定机构确需调用关键信息基础设施运营单位已经收集的个人信息，应经指挥部同意，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。

7.5 收集、调用规则

指定机构收集、调用个人信息应坚持最小化原则，一般只限于个人信息主体的联系方式、位置、行踪信息；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。

7.6 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，原则上应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，原则上不留存可提取人脸识别信息的原始图像。

7.7 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。

7.8 公开、向他人提供个人信息和改变个人信息用途

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，应报指挥部或者国务院卫生健康行政部门同意。

指定机构不得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。

7.9 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60天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。

7.10 日志留存

指定机构应留存个人信息收集、调用、使用活动日志，并保存至突发公共卫生事件应对工作结束后不少于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（ISO 27001:2013，IDT）
[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（ISO 27000:2016，IDT）
[3] GB/T 30146—2013 公共安全 业务连续性管理体系 要求（ISO 22301:2012，IDT）
[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 20000:2011 Information technology— Service management—Requirements
[6] ISO/IEC 20243:2015 Information technology — Open Trusted Technology Provider Standard (O-TTPS) — Mitigating maliciously tainted and counterfeit products
[7] SS 507:2008 SINGAPORE STANDARD FOR Business continuity/disaster recovery (BC/DR) service providers
[8] NIST SP 800-34 Contingency Planning Guide for Information Technology System
[9] Professional Practices for Business Continuity Planners，DRI International
[10] Business Continuity Glossary，DRI International