ICS
L80

CICASME

中 国 中 小 企 业 国 际 合 作 协 会 团 体 标 准

T/ZXGJXH XXX—2021

中小企业数据安全合规准则

Data security compliance guidelines for small and medium-sized enterprises

2021-11-4

（草稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国中小企业国际合作协会发布

目　次

前　言

本标准按照GB/T1.1-2009《标准化工作导则 第1部分：标准的结构和编写》给出的规则起草。

本标准由中国中小企业国际合作协会提出并归口。

本标准起草单位：

本标准主要起草人：

中小企业数据安全合规准则

1 范围

本标准规定了中小企业利用网络收集、存储、使用、加工、传输、提供、公开、删除数据的安全技术与管理要求。

本标准适用于中小企业开展数据处理活动，也适用于第三方评估机构对中小企业数据处理活动的安全合规性进行评估。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是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—2010 信息安全技术 术语

GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T XXXXX—XXXX 信息安全技术 重要数据识别指南

3 术语和定义

GB/T 25069—2010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

通过网络收集、存储、传输、处理和产生的各种数据。

3.2

数据处理 data process

包括数据的收集、存储、使用、加工、传输、提供、公开、删除等。

3.3

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。

3.4

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，也不包含国家秘密信息。

3.5

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，不包括匿名化处理后的信息。

3.6

敏感个人信息 sensitive personal 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。

3.7

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。

3.8

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

3.9

匿名化 anonymization

通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。

4 网络安全基本要求

4.1 二级系统安全保护要求

4.1.1 身份鉴别

数据处理者应：

a) 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
b) 提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
c) 强制用户首次登录时修改初始口令；
d) 在用户身份鉴别信息丢失或失效时，采用技术措施保证鉴别信息重置过程的安全。

4.1.2 访问控制

数据处理者应：

a) 提供访问控制功能，对登录的用户分配账户和权限；
b) 重命名或删除默认账户，修改默认账户的默认口令；
c) 及时删除或停用多余的、过期的账户，避免共享账户的存在。

4.1.3 安全审计

数据处理者应：

a） 提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b） 在审计记录中记录事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c） 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

4.1.4 数据备份恢复

数据处理者应：

a） 对本组织认定的敏感或重要的数据提供本地数据备份与恢复功能；
b） 对本组织认定的敏感或重要的数据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。

4.1.5 剩余信息保护

数据处理者应确保鉴别信息所在的存储空间被释放或重新分配前得到完全清除。

4.1.6 其他

数据处理者应满足 GB/T 22239—2019 对物理和环境安全、网络和通信安全、设备和计算安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理提出的第二级安全要求。

涉及云计算、移动互联、物联网、工业控制系统的，还应满足 GB/T 22239—2019 对相应技术和应用提出的第二级安全要求。

4.2 三级系统安全保护要求

4.2.1 身份鉴别

数据处理者应：

a） 对登录的用户进行身份标识和鉴别，身份标识具有唯一性，鉴别信息具有复杂度要求并定期更换；
b） 提供并启用登录失败处理功能，多次登录失败后应采取必要的保护措施；
c） 强制用户首次登录时修改初始口令；
d） 在用户身份鉴别信息丢失或失效时，采用技术措施保证鉴别信息重置过程的安全；
e） 采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对用户进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

4.2.2 访问控制

数据处理者应：

a） 提供访问控制功能，对登录的用户分配账户和权限；
b） 重命名或删除默认账户，修改默认账户的默认口令；
c） 及时删除或停用多余的、过期的账户，避免共享账户的存在；
d） 授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系；
e） 由授权主体配置访问控制策略，访问控制策略规定主体对客体的访问规则；
f） 使访问控制的粒度应达到主体为用户级，客体为文件、数据库表级、记录或字段级；
g） 对敏感信息资源设置安全标记，并控制主体对有安全标记信息资源的访问。

4.2.3 安全审计

数据处理者应：

a) 提供安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计；
b) 在审计记录中记录事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等；
d) 对审计进程进行保护，防止未经授权的中断。

4.2.4 数据备份恢复

数据处理者应：

a) 对本组织认定的敏感或重要的数据提供本地数据备份与恢复功能；
b) 提供异地实时备份功能，利用通信网络将本组织认定的敏感或重要的数据实时备份至备份场地；
c) 对本组织认定的敏感或重要的数据处理系统提供热冗余，保证系统的高可用性。

4.2.5 剩余信息保护

数据处理者应：

a) 确保鉴别信息所在的存储空间被释放或重新分配前得到完全清除；
b) 确保存有本组织认定的敏感或重要的数据的存储空间被释放或重新分配前得到完全清除。

4.2.6 其他

数据处理者应满足 GB/T 22239—2019 对物理和环境安全、网络和通信安全、设备和计算安全、安全策略和管理制度、安全管理机构和人员、安全建设管理、安全运维管理提出的第三级安全要求。

涉及云计算、移动互联、物联网、工业控制系统的，还应满足 GB/T 22239—2019 对相应技术和应用提出的第三级安全要求。

5 数据安全主要活动

5.1 安全管理制度

数据处理者应当建立健全全流程数据安全管理制度，并满足以下要求：

a) 涵盖数据收集、存储、使用、加工、传输、提供、公开、删除等过程；
b) 对数据安全管理制度形成文档，并进行变更管理；
c) 建立制度的实施、考评、奖惩机制，定期检查跟踪制度实施情况。

5.2 安全保护计划

数据处理者应当制定本组织的数据安全保护计划，并满足以下要求：

a) 建立本组织数据安全保护策略，明确数据安全保护目标和原则；
b) 明确本组织的数据安全保护技术机制，形成完整的数据安全保护技术方案；
c) 明确数据安全保护技术方案实施的时间表，明确任务分工；
d) 建立数据安全保护计划的定期评审和动态调整机制；
e) 与数据安全管理制度有效衔接，并涵盖数据分类分级、应急处置等数据安全主要活动。

5.3 机构和负责人

数据处理者处理重要数据和一百万人以上个人信息的，应成立数据安全管理机构，明确数据安全负责人，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、数据安全应急预案并督促落实；
b）研究提出数据安全相关重大决策建议；
c）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；
d）处置数据安全事件；
e）依法向有关部门报告数据安全保护和事件处置情况；
f）定期开展数据安全宣传教育培训、应急演练；
g）组织受理和处置数据安全投诉、举报。

5.4 人员管理

数据处理者应：

a）明确数据处理关键岗位，提供岗位职责要求；
b）明确数据安全保护岗位及职责，并提供人力资源保障；
c）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。

处理重要数据和一百万人以上个人信息的处理者，还应当对数据处理关键岗位和数据安全保护岗位的人员进行背景审查，重点关注无犯罪记录、个人信用、奖惩、工作履历等情况。

5.5 个人信息识别

数据处理者应识别数据处理中涉及的个人信息。

个人信息包括但不限于姓名、出生日期、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，表1列举了个人信息的示例。

判定某项信息是否属于个人信息，可考虑以下两条路径：一是识别，由信息本身的特殊性识别出特定自然人，有助于识别出特定个人的信息即为个人信息。二是关联，如已知特定自然人，由该特定自然人在活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

表1. 个人信息举例

个人基本资料	个人姓名、生日、性别、民族、国籍、家庭关系、住址、个人电话号码、电子邮件地址等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、出入证、社保卡、居住证等
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
个人健康生理信息	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信息，如体重、身高、肺活量等
个人教育工作信息	个人职业、职位、工作单位、学历、学位、教育经历、工作经历、培训记录、成绩单等

个人财产信息	银行账户、鉴别信息(口令)、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、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
个人通信信息	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
联系人信息	通讯录、好友列表、群列表、电子邮件地址列表等
个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
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/Android ID/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
个人位置信息	包括行踪轨迹、精准定位信息、住宿信息、经纬度等
其他信息	婚史、宗教信仰、性取向、未公开的违法犯罪记录等

5.6 敏感个人信息识别

数据处理者应识别数据处理中涉及的敏感个人信息。

敏感个人信息包括但不限于身份证件号码、个人生物识别信息、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。表2列举了敏感个人信息的示例。

判定某项信息是否属于敏感个人信息，可考虑信息在发生泄漏、非法提供、滥用后，是否可能对个人信息主体权益带来重大风险。例如，个人信息主体的身份证复印件被他人用于手机号卡实名登记、银行账户开户办卡，将健康信息用于保险公司营销和确定个体保费数额等。

表2. 敏感个人信息举例

个人财产信息	银行账户、鉴别信息口令 、存款信息（包括资金数量、支付收款记录等）、房产信息、信贷记录、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
个人健康生理信息	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
个人生物识别信息	个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等
个人身份信息	身份证、军官证、护照、驾驶证、工作证、社保卡、居住证等
其他信息	性取向、婚史、宗教信仰、未公开的违法犯罪记录、通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

5.7 重要数据识别

数据处理者应按照GB/T XXXXX-XXXX识别数据处理中涉及的重要数据。

数据处理者应按照表3给出的格式编制重要数据目录。

表3. 重要数据目录格式

分类			监管要求	重要性描述			产生、使用与保护				备注
地区/部门	类	子类	适用的现有管理政策	影响	面临的主要安全威胁	时效	来源	用途	共享情况	保护情况	

a）“地区/部门”指重要数据所在的地区或部门。

b）“类”是重要数据的第一级分类，由重要数据所在的地区、部门确定。

c）“子类”是重要数据的第二级分类，由重要数据所在的地区、部门确定。根据具体情况，有的重要数据还可划分二级子类。

d）“适用的现有管理政策”指重要数据的安全保护需要遵循的地区、部门已有的管理政策。

e）“影响”指重要数据对国家安全、公共利益的影响，即重要数据之所以“重要”的理由。

f）“面临的主要安全威胁”指重要数据在保密性、完整性、可用性、真实性等方面可能面临的安全威胁。

g）“时效”指重要数据维持“重要性”的时间长度。原则上，重要数据的时效不超过国家秘密的保密期限。时效过后，便不再属于重要数据。

h）“来源”指重要数据如何收集或产生。

i）“用途”指使用重要数据的目的以及具体方式方法。

j）“共享情况”指与其他组织共享、交易、委托处理重要数据的情况，含数据出境情况。

k）“保护情况”指对重要数据采取的安全保护措施。

l）“备注”用于描述其他需要说明的事项。

5.8 数据分类

除个人信息、敏感个人信息、重要数据外，数据处理者还应根据行业管理政策、合同规定和业务运营需要，识别数据处理中涉及的其他数据，并进行分类和分级。

数据处理者应当认定本组织的敏感或重要的数据，包括但不限于个人信息、敏感个人信息、重要数据，并形成数据保护目录。

5.9 数据处理合规风险评估

数据处理者应当在开展以下活动前进行风险评估，并留存风险评估和处置报告至少3年以上：

a）数据出境；

b）个人信息处理目的变更；

c）个人信息匿名化和去标识化；

d）利用个人信息进行自动化决策；

e）重要数据和个人信息委托处理、转让、共享或公开披露。

风险评估的内容包括但不限于：

a）数据处理的目的、方式、范围等是否合法、正当、必要；

b）对国家安全、公共利益和个人权益的影响及安全风险；

c）数据被泄露、毁损、篡改、滥用的风险；

d）所采取的保护措施是否合法、有效并与风险程度相适应；

e）个人或组织维护合法权益的渠道是否通畅；

f）相关的合同是否列出了关于数据安全的要求，是否可以有效约束各方履行数据安全义务。

5.10 教育培训

数据处理者应当组织开展数据安全教育培训，培训对象包括但不限于高层管理人员、数据处理岗位人员、数据安全保护岗位人员等。

处理重要数据和一百万人以上个人信息的处理者，应确保每年的培训时间不少于20小时。

5.11 应急处置

数据处理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，采取断开链接、限制访问等措施防止危害扩大，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。

5.12 投诉举报处置

数据处理者应建立投诉、举报受理处置制度，公布联系方式和处置流程，处理关于数据安全和信息内容安全的投诉、举报。

收到通过其平台编造、传播虚假信息，泄露个人信息，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。对于查实的投诉、举报，数据处理者应当依法采取停止传输、消除等处置措施。

5.13 便利行权

数据处理者应建立渠道和机制，接收个人信息主体查阅、复制、更正、撤回同意、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—2020 8.7有关响应个人信息主体请求的要求。

数据处理者应当提供便捷的支持个人信息主体查阅、复制、更正、撤回同意、删除其个人信息及用户注销账号的功能。

收到个人信息主体查阅、复制、更正、撤回同意、删除其个人信息及用户注销账号的，应当在15个工作日内处理并反馈，法律另有规定的从其规定。

5.14 年度安全自评估

重要数据处理者应自行或委托数据安全服务机构每年开展一次数据安全评估，并按规定于当年末或第二年年初经评估报告搞有关部门。年度安全自评估报告的内容包括：

a) 处理重要数据的情况；
b) 发现的数据安全风险及处置措施；
c) 数据安全管理制度，采取的安全防护措施及其有效性；
d) 落实国家数据安全法律法规和标准的情况；
e) 发生的数据安全事件及处置情况；
f) 向第三方和境外提供数据情况；
g) 与重要数据安全相关的投诉及处理情况。

6 数据处理规则

6.1 收集

数据处理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的范围和期限的个人信息，且符合以下要求：

a）应制定和公开个人信息处理规则，涵盖隐私政策、与数据有关的算法策略和平台规则，以显著方式、清晰易懂的语言真实、准确、完整地向个人告知下列事项：
   1）数据处理者的名称或者姓名和联系方式；
   2）以清单形式逐一列出每种服务收集个人信息的目的、方式、种类、频次或者时机、保存地点等，以及拒绝处理个人信息对个人信息主体的影响；
   3）个人信息存储期限或者个人信息存储期限的确定方法、到期后的处理方式；
   4）个人行使权利的方式和程序；
   5）以集中展示等便利用户访问的方式说明产品服务中嵌入的所有涉及个人信息处理功能的第三方代码、插件的名称，以及每个第三方代码、插件处理个人信息的目的、方式、种类、频次或者时机，及其个人信息处理规则；
   6）向第三方提供个人信息情形及其目的、方式、种类，可能的个人信息接收方相关信息等；
   7）个人信息安全风险及保护措施；
   8）法律、行政法规规定应当告知的其他事项。
b）按照服务类型分别向个人申请收集个人信息的同意，不应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该核心业务功能服务，也不得降低改服务的质量；
c）限于实现处理目的最短周期、最低频次，采取对个人权益影响最小的方式；
d）不应仅以改善服务质量、提升用户体验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；
e）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，重新征得个人信息主体同意；
f）收集个人敏感信息前，应征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）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的授权同意范围，并按照本文件的要求履行安全保护义务。数据提供方应在确保其数据安全的基础上提供数据。

6.2 存储

数据处理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，应采用加密、安全存储、访问控制、安全审计等安全措施；
b）存储个人信息，不应超过与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，法律法规另有规定的除外；
c）存储个人生物识别信息，应满足GB/T 35273—2020 6.3 b）和c）的要求；
d）已实现个人信息处理目的或实现个人信息处理目的不再必要，达到与用户约定或个人信息处理规则明确的存储期限，或者终止服务或个人注销账号的，数据处理者应当在15个工作日内删除个人信息，或进行匿名化处理；
e）删除个人信息在技术上难以实现，或者因业务复杂等原因，在15个工作日内删除个人信息确有困难的，数据处理者不应开展除存储和采取必要的安全保护措施之外的处理，并应向个人信息主体作出合理解释。

6.3 使用

6.3.1 定向推送及信息合成

数据处理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：

a) 征得用户单独同意；
b) 设置易于理解、便于访问和操作的一键关闭定向推送选项，允许用户拒绝接受定向推送信息，允许用户重置、修改、调整定向推送参数；
c) 允许用户删除定向推送服务收集产生的个人信息；
d) 定向推送商业广告的，应当通过显著标识提示用户；
e) 同时提供非定向推送信息的服务选项。

在向个人信息主体提供新闻、博客类信息服务的过程中，数据处理者利用算法自动合成文字、图片、音视频等信息，应当明确告知用户。

6.3.2 第三方应用

数据处理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）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）应督促和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）数据处理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。

6.3.3 反不正当竞争或限制

数据处理者应当依法经营，不得从事下列与数据利用有关的活动：

a）利用平台收集掌握的用户数据，无正当理由对交易条件相同的用户实施产品和服务差异化定价等损害用户合法权益的行为；
b）利用平台收集掌握的平台内经营者数据，在产品推广中实行最低价销售等损害公平竞争的行为；
c）利用数据误导、欺诈、胁迫用户，限制用户对其数据被收集、处理、使用的决定权，违背用户意愿处理用户数据。

6.4 加工

数据处理者开展转换、汇聚、分析等数据加工过程中，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，并根据相关法律法规按要求向有关部门报告。

6.5 传输

数据处理者应对数据传输活动采取安全措施，包括：

a）传输重要数据和个人信息时，应采用加密、脱敏等安全措施；
b）向数据接收方传输数据时，应在合同中约定双方的数据安全保护责任和义务，并采取安全防护措施。

6.6 提供

数据处理者向他人提供数据前，应进行合规风险评估，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，应告知向他人提供的目的、类型、方式、范围、用途、存储期限、存储地点，并征得个人信息主体单独同意，经过匿名化处理的除外；
b）应与数据接收方约定数据处理的目的、范围、处理方式，数据安全保护措施等，通过合同等形式明确双方的数据安全保护责任和义务，并对数据接收方的数据处理活动进行监督；
c）采取加密、脱敏等措施保障数据提供过程中的安全；
d）委托开展数据加工活动的，应与受托方通过合同等形式明确双方的保护责任和义务，并要求受托方以合同中约定的形式返还、删除接收和产生的数据；
e）发生兼并、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，应对数据作删除处理。

6.7 公开

数据处理者公开数据时，应：
a）事先开展合规影响评估，对公开的事由、后果、保护措施进行研判，确保合法合规、符合合同约定；
b）涉及个人信息的，向个人信息主体告知公开个人信息的目的、类型、内容，并事先征得个人信息主体明示同意；
c）涉及重要数据的，征得重要数据行业主管监管部门的批准；
d）准确记录和存储数据的公开情况，包括公开的日期、规模、目的、公开范围等；
e）承担因公开数据对公共利益、个人信息主体合法权益造成损害的相应责任。

6.8 删除

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，或者当用户撤销同意后，网络运营者应及时对个人信息做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。

7 数据出境安全

7.1 出境前自评估

数据被传输到境外，或者数据被外资审计、认证机构或境外组织、人员访问的，应开展自评估，重点评估以下内容：
a）数据出境的必要性、合法性；
b）数据接收方所在国家或地区的数据保护法律环境；
c）数据出境后被非授权访问、篡改、滥用的风险；
d）境外数据接收者的背景、数据安全保护能力；
e）个人信息出境是否征得了个人同意，或者是否属于同意例外的情况；
f）重要数据出境是否征得了行业主管监管部门批准；
g）数据出境合同是否公平、合理并明确了双方责任义务。

7.2 出境条件

重要数据出境，关键信息基础设施运营者掌握的个人信息出境，或者十万人以上个人信息出境的，应通过国家网信部门组织的安全评估。

其他数据出境的，可以采取以下三种出境方式：

a) 数据发送方和接收方通过国家网信部门指定的认证机构的认证；
b) 按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；
c) 位于不同国家和地区的分支机构之间、总部与分支机构之间跨境传输数据的，可按照国家网信部门批准的约束性组织规则进行数据传输。

7.3 出境安全管理责任

数据处理者向境外提供重要数据的，应：

a) 按照国家网信部门批准的或风险评估报告中明确的目的、范围、方式和数据类型、规模等实施数据出境；
b) 在合同中约定数据出境后的安全保护要求以及再转移事项；
c) 数据发送方应承担数据出境安全主体责任，接受和处理数据出境所涉及的用户投诉；
d) 数据接收方对公民个人权益造成损害的，数据发送方应协助公民进行维权，并根据法律的要求承担相应的赔偿责任；
e) 留存相关日志记录5年以上；
f) 国家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，以明文、可读方式予以展示。

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] 网络数据安全管理条例（征求意见稿）
[5] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
[6] GB/T XXXXX—XXXX 信息安全技术 数据出境安全评估指南
[7] EU General Data Protection Regulation，2015