ICS 35.240
CCS L 80

团　体　标　准

T/CIQA 105—2024

数字产品数据安全和隐私保护要求

Data security and privacy protection requirements for digital products

2024-12-20 发布　　2024-12-20 实施

中国出入境检验检疫协会　发 布

目录

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这些专利的责任。

本文件由中国出入境检验检疫协会网络安全标准化技术委员会（CIQA/TC16）提出并归口。

本文件起草单位：北京时代新威信息技术有限公司、中国汽车工程研究院股份有限公司、四川省电子产品监督检验所、中国软件评测中心（工业和信息化部软件与集成电路促进中心）、力鸿检验控股有限公司、中移物联网有限公司、吉林省电子信息产品检验研究院。

本文件主要起草人：王新杰、杨玉忠、潘文博、全代勇、谢天瀛、邓刚、刘海涛、张德馨、张学扬、张晓华、张一沛、刘利军、文远、张家铭、刘天慧。

本文件是首次发布。

数字产品数据安全和隐私保护要求

1 范围

本文件规定了数字产品针对用户信息的收集、存储、使用、加工、是供、公开、出境等数据处理活动的安全要求。

本文件适用于数字产品提供者规范数据处理活动，也可为监管部门、第三方评估机构对数字产品中数据处理活动进行监督、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 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

GB/T 41391 信息安全技术 移动互联网应用程序（App）收集个人信息基本要求

GB/T 41479 信息安全技术 网络数据处理安全要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

数字产品 digital products

数字产品是指支撑数字信息处理的终端设备或高度应用数字化技术的智能设备，主要包括：智能办公产品、智能娱乐产品、智能健康产品、智能穿戴产品、智能车联网产品、智能监控设备、智能无人机、智能机器人等。

3.2

数据 data

信息的可再解释的形式化表示，以适用于通信、解释或处理。

注：数据可以由人工或自动的方式加工处理。

[来源：GB/T 18391.1-2009，定义3.2.6]

3.3

用户信息 user information

与个人、法人或其他组织有关的信息，以及定义和描述此类信息的数据。

注：用户信息包括个人信息，用户生成的文档、程序、多媒体资料，用户通信的内容、地址、时间，产品的配置、运行及位置数据，系统运行过程产生的日志等。

[来源：ISO/IEC 17027:2014，2.56]

3.4

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来识别特定自然人身份或者反映其活动情况的各种信息。

注1：个人信息包括姓名、出生日期、公民身份号码、个人生物特征信息、住址、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：个人信息控制者通过个人信息或其他加工处理后形成的信息，例如，用户画像特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映特定自然人活动情况的,也属于个人信息。

[来源：GB/T 25069-2022，3.196]

3.5

隐私 privacy

隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

[来源《中华人民共和国民法典》第一千零三十二条第二款]

3.6

隐私信息 privacy information

是指自然人或个人不愿意公开的与个人身份、行为、通信、财务状况、健康状况等相关的信息。这些信息包括但不限于：

个人身份信息：如姓名、身份证号码、护照号码、社会保险号码等。

联系信息：如家庭地址、电话号码、电子邮箱地址等。

金融信息：如银行账户信息、信用卡信息、交易记录等。

健康信息：包括医疗记录、健康检查结果、遗传信息等。

在线活动信息：如浏览历史、搜索记录、社交媒体账户、商品和服务交易信息等。

通信内容：如电子邮件、短信、即时通讯应用中的消息内容等。

位置数据：通过GPS或其他技术收集的个人位置信息。

其他：国家法律法规规定的其他信息。

3.7

个人信息主体 personal information subject

个人信息所标识或关联的自然人。

[来源：GB/T 35273-2020，定义3.3]

3.8

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。

注:个人信息经匿名化处理后所得的信息不属于个人管息

[来源：GB/T 35273—2020，定义3.147]

3.9

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/T35273-2020，定义3.157]

3.10

数据安全 data security

数据安全，是指通过采取必要措施，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。

3.11

隐私保护 privacy protection

为保护隐私而采取的措施，如对个人信息的收集、处理和使用加以保护。

4 数据安全和隐私保护原则

数字产品提供者应遵循以下原则：

a) 同步原则：在数字产品设计、安装和运行维护过程中，以及数据从收集到销毁的全生命周期中，数字产品提供者应对用户数据安全与隐私保护进行同步规划、同步建设、同步使用；

b) 公开透明原则：用户信息或隐私的收集、处理与利用，组织必须获得个人的明确同意，并应公开信息处理规则，明示处理目的、方式和范围，信息处理者的名称或姓名和联系方式，可能披露个人数据的第三方的类型或身份以及披露目的，用户个人权利等；

c) 最少必需原则：在数据的收集、存储、使用、加工、传输、提供、公开、销毁等活动中,所使用的数据类型及数据范围仅限定为实现产品功能所必需的最小范围，且具有合法、正当、必要的目的；隐私信息的保存期限应当为实现处理目的所必要的最短时间；

d) 安全性原则：数字产品提供者应确保用户信息或隐私的处理安全,包括防止未经授权或非法的处理以及防止意外损失、毁损或损坏。数字产品提供者应采取适当的技术或组织措施来保护用

户隐私及信息免受可能的威胁。这些措施应根据最新技术水平、相关成本以及处理的性质、范围、背景和目的,以及对个人权利的风险进行评估。

e) 分类分级原则：对数据进行分类分级,根据数据安全风险程度采取相应的安全保护措施，保障数据安全；

f) 覆盖产品生命周期原则：数据安全保护措施应覆盖数据从产生到销毁的生命周期全过程。

5 数据收集

5.1 个人信息、隐私信息的收集

数字产品提供者收集个人信息、隐私信息应满足以下要求：

a) 收集个人信息、隐私信息时，应当依法取得，不得非法收集个人信息；

b) 收集个人信息、隐私信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

c) 收集不满十四周岁未成年人个人信息、隐私信息的，还应当制定专门的个人信息、隐私信息处理规则。

5.2 告知数据处理规则

数字产品提供者在处理个人信息、隐私信息之前，应将个人信息、隐私信息处理规则集中公开展示，包括但不限于下列内容：

a) 个人信息、隐私信息处理者的名称或者姓名和联系方式；

b) 处理个人信息、隐私信息的目的、方式、种类，处理个人信息的必要性以及对个人权益的影响；

c) 个人信息、隐私信息保存期限和到期后的处理方式，保存期限难以确定的，应当明确保存期限的确定方法；

d) 个人查阅、复制、转移、更正、补充、删除、限制处理个人信息以及注销账号、撤回同意的方法和途径等。

e) 向第三方提供或共享个人信息、隐私信息前，应向用户告知接收方的名称或者姓名、联系方式、处理目的、处理方式和信息的种类，告知处理的必要性及对个人权益的影响，并取得用户（个人信息主体）的单独授权同意

5.3 授权同意

数字产品提供者处理个人信息、隐私信息应满足以下要求：

a) 收集用户个人信息、隐私信息前应取得用户（个人信息主体）的授权同意；

b) 处理生物识别、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时，应当取得个人的单独同意；

c) 处理不满十四周岁未成年人个人信息、隐私信息时，应当取得未成年人的父母或者其他监护人的同意；

d) 不得在个人明确表示不同意处理其个人信息、隐私信息后，频繁征求同意；

e） 个人信息、隐私信息的处理目的、方式、种类发生变更的，应当重新取得个人同意。

6 数据存储和传输

数字产品提供者存储、传输数据时,应满足以下要求：

a） 个人信息、隐私信息存储期限应为实现信息处理目的所必需的最短时间，超出存储期限应对个人信息、隐私进行删除或匿名化处理，法律法规另有规定的除外；

b） 如超出个人信息存储期限,但法律、行政法规规定的保存期限未届满,或者删除个人信息从技术上难以实现的，应停止除存储和采取必要的安全保护措施之外的处理；

c） 存储和传输个人信息、隐私信息时，应采用密码技术对信息进行加密；个人信息、隐私信息应独立加密存储；

d） 传输过程中应采用数据校验算法确保数据完整性；

e） 不应存储用户原始个人生物识别信息以及用户验证码、银行卡密码等信息；

f） 个人信息、隐私信息应存储于中华人民共和国境内，如需出境应遵循国家相关规定。

7 数据使用和加工

7.1 数据的访问控制

访问个人信息、隐私信息时,应满足以下要求：

a） 数字产品提供者内部使用的业务系统，应授予管理用户所需的最小权限,实现管理用户的权限分离。

b） 应遵循最少必需的原则,按照数据分级建立相应的数据访问控制措施和访问权限申请审批流程，将数据分级与数据访问权限进行关联标识，访问权限应明确数据查阅、更正、删除、下载等操作；

c） 应确保访问隐私信息的合法性、安全性以及可控性。访问控制技术宜向细粒度、多安全等级、跨域的方向延伸发展，授权依据面向主、客体的安全属性，采用基于信任、基于属性和基于行为等一系列基于安全属性的新型访问控制模型以及管理模型；

d） 基于属性的访问控制应将各类属性包括用户属性、资源属性、环境属性等组合起来用于用户访问权限的设定。

7.2 数据加工

数字产品提供者加工、处理个人信息、隐私信息时，应满足以下要求：

a） 未经用户单独授权同意,不应对用户个人信息、隐私信息进行分析挖掘；

b） 不应根据用户的网上活动（如收藏列表、关注列表、交易记录、搜索记录、点击记录、浏览记录等）实施不合理的差别待遇；

c） 根据用户的网上活动或操作提供个性化推荐（如广告、商品推荐等）功能时，应允许用户自主选择，并满足以下要求：

1） 应提供不针对其个人特征的选项,或向个人提供便捷的拒绝方式；

2） 应向用户提供设置、修改针对用户特征的个性化推送参数的功能；

3） 应向用户提供针对自动化决策结果的便捷有效的投诉渠道；

4） 在涉及用户资金交易的自动化决策时，应提前向用户详细说明并取得用户单独授权同意。

d） 不得通过自动化决策方式向未成年人进行商业营销。

8 数据提供和公开

8.1 数据提供

数字产品提供者向第三方提供数据时，应满足以下要求：

a） 应对第三方的数据安全保护能力进行评估，并以协议等方式约定双方的数据保护责任；

b） 应与第三方约定数据处理规则，并在用户网络活动中同步告知用户；

c） 应向用户告知第三方的名称或者姓名、联系方式、处理目的、处理方式和信息的种类，并取得用户的单独授权同意；

d） 向商品交易、物流等第三方服务提供者提供数据时，应仅限于相关活动的订单范围；

e） 因兼并、重组、破产等原因需要转移数据的,应采取安全保护措施，确保数据的完整性和保密性，数据接收方应继续履行数据安全保护责任和义务。

f） 国家监管机构、执法部门依法需要调取数据，应当予以配合。

8.2 数据公开

数字产品提供者经法律授权或具备合理事由确需公开披露时,应符合以下要求：

a） 事先开展个人信息安全影响评估,并依评估结果采取有效的保护个人信息主体的措施；

b） 向个人信息主体告知公开披露个人信息、隐私信息的目的、类型、内容,并事先征得个人信息主体单独授权同意，且对个人信息、隐私信息进行匿名化或脱敏处理后方可公开；

c） 对用户个人信息、隐私信息公开披露的情况进行记录,包括公开披露的日期、规模、目的、范围等；

d） 承担因公开披露个人信息对个人信息主体合法权益造成损害的相应责任；

e） 不应公开披露个人生物识别信息。

9 数据删除

数字产品提供者删除数据应满足以下要求：

a） 个人请求删除其个人信息、隐私信息，或者要求注销账号、撤回同意的，数据产品提供者应及时删除个人信息、隐私信息，不得设置不合理条件限制个人的合理请求；

b） 用户发现数字产品提供者违反法律、行政法规的规定或者双方的约定处理其个人信息、隐私信息并请求删除时，数字产品提供者应及时删除。

c） 数字产品停止服务或产品生命周期结束，应对持有的个人信息、隐私信息进行删除；

d） 删除前应对数据进行加密，确保即使数据被恢复后仍无法读取内容；

e） 对存储设备进行物理删除，对需要报废的存储设备进行销毁处理；

f） 应保存数据删除活动的记录，包括但不限于删除的数据类型、方式、时间、责任人等。

10 数据出境

数字产品提供者确需向境外提供个人信息、隐私信息时，应当满足以下条件：

a）通过国家网信部门组织的数据出境安全评估；

b）按照国家网信部门的规定经专业机构进行个人信息保护认证；

c）符合国家网信部门制定的关于个人信息出境标准合同的规定；

d）为订立、履行个人作为一方当事人的合同，确需向境外提供个人信息；

e）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息；

f）为履行法定职责或者法定义务，确需向境外提供个人信息；

g）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息；

h）法律、行政法规或者国家网信部门规定的其他条件。

11 数据安全事件应急处置

数字产品提供者处置数据安全事件时应满足以下要求：

a）建立健全数据安全事件应急预案；

b）发生数据安全事件时，应当立即启动预案，采取措施防止危害扩大，消除安全隐患，并按照规定向有关主管部门报告；

c）应及时将安全事件和风险情况、危害后果、已经采取的补救措施等，以电话、短信、即时通信工具、电子邮件或者公告等方式通知受影响的用户；难以逐一告知的，应当采取合理、有效的方式及时发布相关警示信息；

d）在处置数据安全事件过程中发现涉嫌违法犯罪线索的，应当按照规定向公安机关、国家安全机关报案，并配合开展侦查、调查和处置工作。

参 考 文 献

[1] 中华人民共和国网络安全法 （2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过）

[2] 中华人民共和国密码法(2019 年 10 月 26 日第十三届全国人民代表大会常务委员会第十四次会议通过)

[3] 中华人民共和国数据安全法（2021 年 6 月 10 日第十三届全国人民代表大会常务委员会第二十九次会议通过）

[4] 中华人民共和国个人信息保护法（2021 年 8 月 20 日第十三届全国人大常委会第三十次会议通过）

[5] 未成年人网络保护条例（中华人民共和国国务院令第 766 号，2023 年 10 月 16 日）

[6] 网络数据安全管理条例（中华人民共和国国务院令第 790 号，2024 年 9 月 24 日）

[7] 数据出境安全评估办法（2022 年 7 月 7 日国家互联网信息办公室令第 11 号）