ICS 35.030
CCS L80

中华人民共和国国家标准

GB/T XXXXX—XXXX

信息安全技术 网上购物服务数据安全指南

Information security technology— Data security guidelines for online shopping services

（征求意见稿）

（本稿完成时间：2021 年 2 月 7 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：标准的结构和编写》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。

本文件起草单位：阿里巴巴（北京）软件服务有限公司、中国电子技术标准化研究院、北京小米移动软件有限公司、北京京东尚科信息技术有限公司、苏宁易购集团股份有限公司、华为技术有限公司、上海寻梦信息技术有限公司、北京三快科技有限公司、联想（北京）有限公司、中电长城网际系统应用有限公司、国家计算机网络应急技术处理协调中心、中国信息通信研究院、上海观安信息技术股份有限公司

本文件主要起草人：朱红儒、白晓媛、陈舒、胡影、顾伟、陈林、李瑞卿、戚俊卿、严少敏、衣强、刘笑岑、闵京华、韩煜、陈晓桦、李汝鑫、余凌峰、舒敏、魏薇、陈湉、卢一宁、王莹、周晨炜、康琼、孙旭东、刘艾婧、张印泽、宋建、罗宇、陈勇、闫希敏、曹京、赵芸伟、谢江

信息安全技术　网上购物服务数据安全指南

1　范围

本文件规定了网上购物服务可以收集、存储、使用、交换、删除、出境的数据种类、范围、方式、条件等，以及数据安全保护要求。

本文件适用于网上购物服务运营者规范数据活动，也适用于主管监管部门、第三方评估机构对网上购物服务数据活动进行监督、管理、评估时参考。

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 25069-2010　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

GB/T AAAAA　信息安全技术　网络数据处理安全规范

GB/T BBBBB　信息安全技术　移动互联网应用（App）收集个人信息基本规范

3　术语和定义

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

3.1

网上购物服务　online shopping service

通过互联网等信息网络从事销售商品或者提供服务的经营活动。

[GB/T 38652—2020，定义 2.1]

3.2

网上购物服务平台　online shopping service platform

为交易的双方或多方提供信息发布、信息递送、数据处理等一项或多项服务，实现交易撮合目的的信息网络系统。

[GB/T 38652—2020，定义 2.2]

3.3

网上购物服务平台运营者　online shopping service platform operator

在网上购物服务中为交易双方或者多方提供网络经营场所、交易撮合、信息发布等一项或多项服务，供交易双方或者多方独立开展交易活动的法人或者非法人组织。

[GB/T 38652—2020，定义2.3.1]

3.4

平台内运营者 operator on online shopping service platform

通过网上购物服务平台销售商品或者提供服务的运营者。

[GB/T 38652—2020, 定义 2.3.2]

3.5

网上购物服务运营者 online shopping service operator

通过互联网等信息网络从事销售或者提供服务的经营活动的自然人、法人和非法人组织，包括网上购物服务平台运营者、平台内运营者以及通过自建网站、其他网络服务销售商品或者提供服务的运营者。

[GB/T 38652—2020, 定义 2.3]

3.6

跨境电子商务 cross-border e-commerce

分属不同关境的交易主体，通过互联网达成交易、进行支付结算，并通过物流送达商品、完成交易的经营活动。

[GB/T 38652—2020, 定义3.6]

3.7

卖家 seller

通过网上购物服务平台、自建网站、其他网络服务等信息网络从事销售商品或者提供服务的经营活动自然人、法人和非法人组织。

[GB/T 38652—2020, 定义4.5]

3.8

会员 registered member

在网上购物服务平台登记注册的组织或个人。

[GB/T 38652—2020, 定义4.1]

3.9

买家 buyer

顾客 customer

用户 user

在网上购物服务平台上购买商品或服务的会员。

[GB/T 38652—2020, 定义4.4]

4 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

App：移动互联网应用程序（mobile Internet Application）

CRM：客户关系管理（Customer Relationship Management）

ERP：企业资源计划（Enterprise Resource Planning）

SDK：软件开发工具包（Software Development Kit）

5 概述

5.1 网上购物服务组成

网上购物服务是通过自建或者第三方网站、小程序或者其他具有信息发布功能的网络服务（如社交网络），从事销售商品或者提供服务的经营活动。网上购物服务的运营者，包括网上购物服务平台运营者、平台内运营者以及通过自建网站、其他网络服务销售商品或者提供服务的运营者。

根据服务实现流程的不同，网上购物服务可分为网上商城购物服务（包括自营模式）、社交购物服务、线上线下融合购物服务。

网上商城购物服务是指通过网上商城平台提供的商品或服务信息发布、交易/事务处理、支付等功能向用户销售商品或提供服务的行为。参与者主要包括买家、商城平台运营者、卖家、第三方支付提供商、物流服务商等，如通过小程序进行购物，参与者还包括小程序应用平台运营者。

网上社交购物服务是指通过社交网络提供的商品或服务信息发布等功能向用户销售商品或提供服务的行为。参与者主要包括卖家、社交网络平台运营者、买家、第三方支付提供商、物流服务商等。

线上线下融合购物服务是指使用同一或相互关联的企业资源管理系统（ERP）和客户关系管理系统（CRM）系统将网上购物平台和线下实体门店的商户（供应商）、买家、商品和服务等资源汇总整合，并统一进行存储、分析、运用和管理，通过线上线下购物场景的有机融合，实现商品展示、搜索、下单、交付、售后等服务功能。参与者主要包括买家、商城平台运营者、线下商户、卖家、第三方支付提供商、物流服务商等。

5.2 网上购物服务数据范围

网上购物服务数据分为用户数据和业务数据两大类。具体数据类别与范围参见附录 A.1。

a) 用户数据是指网上购物服务运营者因提供网上购物服务收集、产生的个人信息，包括个人基本资料、个人身份信息、个人生物识别信息、网络身份标识信息、个人生理信息、个人财产信息、个人通信信息、联系人信息、个人上网记录、个人常用设备信息、个人位置信息、其他信息等。

b) 业务数据是指网上购物服务开展过程中收集和产生的数据，包括业务统计数据、业务经营数据、业务技术数据等。

依据数据的敏感程度、重要性以及一旦泄露、丢失、破坏造成的危害程度等因素，网上购物服务数据分为 4 个等级，具体分级规则参见附录 A.2。

5.3 网上购物服务数据活动

网上购物服务的数据活动围绕网上购物服务相关角色的活动开展，主要包括用户注册/登录，网上购物服务平台展示商品或服务信息，用户浏览、下单、支付，卖家发货、提供售后服务等。

网上购物服务相关角色、数据周期、数据相关活动示意如图1所示。

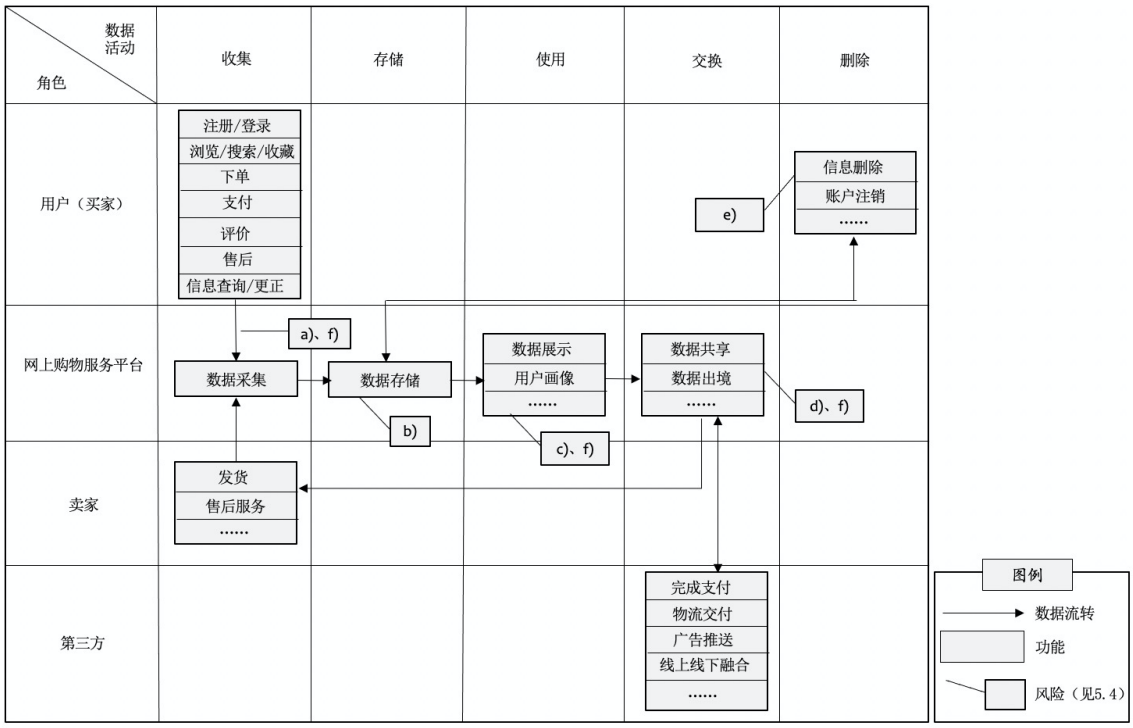

图1 网上购物服务数据活动示意图

5.4 网上购物服务数据安全风险

网上购物服务数据主要面临如下安全风险：

a) 在数据收集环节，网上购物服务运营者过度收集个人信息或者过度索取移动终端权限的风险；

b) 在数据存储阶段，因链路监听、攻击拖库和权限不当等带来的数据泄露或滥用风险；

c) 在数据使用环节，在数据展示时可能存在个人信息泄露或滥用的风险；

d) 在数据交换环节，可能存在超出必要限度与第三方共享数据的风险；

e) 在个人信息查询、删除、更正、注销账户等环节，可能存在无法保障个人信息主体权利的风险；

f) 无人店铺、基于位置的网上购物服务等特殊场景下，可能存在个人信息超范围收集、个人敏感信息泄露等风险。

6 基本要求

网上购物服务运营者应满足以下基本要求：

a) 网上购物服务的数据活动应符合GB/T AAAAA要求；

b) 网上购物服务的个人信息处理活动应符合GB/T 35273—2020要求，网上购物服务App的个人信息收集活动应符合GB/T BBBBB要求；

c) 网上购物服务运营者应识别数据活动涉及的数据，形成数据保护目录，并对网上购物服务数据进行分类分级保护。网上购物服务数据分类分级示例见附录A。

7 数据收集

7.1 数据最小化收集

网上购物服务运营者进行数据收集时，要求包括：

a) 应明确所提供的基本业务功能及相应的必要个人信息收集范围，参见 GB/T BBBBB 附录 A；

b) 对于网上购物服务可选业务功能，应明确其对应的个人信息收集范围及使用要求，参见附录 B。

7.2 系统权限

网上购物服务运营者所运营App中各项业务功能申请系统权限时应遵循最小必要原则。网上购物服务App各项业务功能所需系统权限参见附录C。

8 数据使用

8.1 数据展示

网上购物服务运营者进行数据展示时，要求包括：

a） 对于浏览历史记录、商品搜索记录，应在 App 内提供清除选项；

b） 用户利用网上购物服务平台提供的评论、晒单等功能公开发布信息时，应对用户名进行去标识化处理后进行展示，例如中文昵称仅保留第一个字，英文昵称仅保留第一个字母和最后一个字母，其余用*代替等；

c） 通过拼单 App、社交平台群接龙等方式进行社交购物的服务中，应对购买隐私商品或服务的用户头像和昵称进行去标识化处理后进行展示；

注：隐私商品或服务是指不愿为他人公开或知晓的商品或服务，例如情趣用品、保健品、内衣等；

d） 线上线下融合购物服务中，线下导购场景主要包括精准营销和代下单：

1） 精准营销通过营销工具和顾客进行互动，应对顾客姓名、电话号码等信息去标识化后展示，不可识别到具体个人；

2） 代下单环节中，导购代提交订单信息后，宜对订单信息中的个人信息进行隐藏或去标识化处理，并对后续查看和修改个人信息的行为进行日志记录；

3） 当发生相关售后服务时候，导购根据用户提供的信息到门店客服部门通过客服人员协助进行历史记录查询，应对查询操作行为进行日志记录；

e） 网上购物服务平台上的卖家仅可看到用户的收件人姓名、收件人电话、收件人地址、支付金额、发票信息、订单内容、备注信息、订单状态、物流状态；不应看到用户支付账号信息。

8.2 用户画像与个性化展示

网上购物服务运营者进行用户画像与个性化展示时，要求包括：

a） 在隐私政策中说明网上购物服务所提供的个性化推送或展示功能，以及个性化推送或展示功能所收集和使用的个人信息、退出个性化推荐的路径等；

b） 根据用户的兴趣爱好、消费习惯等特征向用户提供商品或者服务搜索结果的个性化展示的，同时提供不针对其个人特征的选项，例如提供按销量、价格等方式对搜索结果进行排序的功能；

c） 根据用户的兴趣爱好、消费习惯等特征向用户展示商品或服务的，应提供屏蔽对应商品或服务、商品或服务类别的功能等个人信息主体的自主控制机制；

d） 根据用户的兴趣爱好、消费习惯等特征向用户推送个性化广告的，应提供可退出个性化广告的选项，如广告标签管理、广告推荐按钮控制等方式；

e） 线上线下融合购物服务中，用户接到电话邀约后明确拒绝此类推销电话的，门店人员应对用户进行备注并不再对此类用户推送相关推销信息；

f） 网上购物服务用户画像中对用户的特征描述，不应包含隐私商品或服务。

9 数据交换

9.1 共享

网上购物服务运营者进行个人信息共享时，要求包括：

a) 为满足用户购买商品或服务的需要，共享给相关商品或服务提供者的信息应限于如下范围：下单账户名、收货人姓名、收货人电话、收货人地址、买家留言、商品信息、商品数量、金额、付款方式、订单号、下单时间、订单状态、发票信息；

b) 为帮助用户完成对商品或服务的支付，以及提供支付安全功能，将订单和支付信息共享给第三方支付机构的信息应限于如下范围：交易金额、商品或服务信息、订单号、流水号、支付号码、银行卡号；

c) 为向用户完成商品或服务的交付，将订单配送信息共享给第三方物流服务提供方应限于如下范围：收货人姓名、收货地址、收货人联系电话及其他面单所需信息；

d) 网上社交购物服务中，不应将用户在社交网络平台上的昵称、头像、性别、所属地区信息共享给卖家；

e) 网上社交购物服务中，不应将用户的拼单动态、购买的商品信息、商品评价等在用户未明示同意并授权的情况下，默认提供给他人；

f) 网上小程序购物服务中，小程序应用平台将收货地址信息共享给卖家应限于如下范围：收货人姓名、手机号、收货地址；

g) 线上线下融合购物服务中，如用户选择到门店自提商品的方式，商城平台共享给线下门店的信息应限于如下范围：商品信息、提货人姓名、手机号码、提货码；

h) 线上线下融合购物服务中，如用户未达成线上交易，线下门店进行定向营销时，商城平台共享给线下门店的信息应限于如下范围：匹配拟购买商品品类、账户名、手机号；

i) 线上线下融合购物服务中，线上商城平台给线下门店共享个人信息时，应对姓名、手机号进行去标识共享和展示；

j) 在为用户提供广告推送时，共享给分析数据的服务提供商的数据应限于如下范围：用户数量、地区分布、活跃情况及个人的IP地址、浏览记录、点击记录、设备信息、设备标识符；共享给广告服务伙伴的信息应限于：注册信息、会员等级信息、预约信息、下单信息；

k) 不应向广告、分析服务类数据接收方提供个人身份信息，或者应将这些信息进行去标识化处理后进行共享；

l) 未经用户授权不应向广告服务商共享用户的浏览记录、搜索记录。

9.2 数据出境

9.2.1 出境场景

除以下规定的场景外，其他场景不应出境，法律法规另有规定的除外。

a) 用户通过网上购物服务平台购买跨境商品或服务，网上购物服务运营者将订单信息中商品名称、购买数量、收货人姓名、手机号及收货地址等信息提供给跨境商品或服务的提供者（简称“境外卖家”），以实现交易及售后服务；

b) 为了向用户顺利、准确交付跨境商品或服务，为网上购物服务平台跨境商品购买服务提供物流信息系统服务的主体和/或境外卖家需要将订单相关配送信息提供给海外物流、海外仓储等第三方服务商；

c) 为满足商品的清关要求，将用户提供的个人身份信息及订单信息中与交易有关的必要信息提供给境外卖家、报关服务商、境内外海关等机构。

9.2.2 安全要求

网上购物服务运营者进行数据出境时，应满足相关法律法规及标准要求，同时还应满足以下要求：

a) 事先开展数据出境安全评估，并依评估结果采取有效的保护个人信息主体权利及数据安全的措施。数据出境安全评估应包括但不限于以下内容：
   1) 数据出境的合法性及必要性评估；
   2) 数据出境综合影响评估，包括数据类型、数量、范围、敏感程度、境外存储期限、出境目的以及接收方处理数据的目的、方式、范围等；

   注：出境数据仅限于 10.2.1 描述的场景。

   3) 数据安全保障能力评估，包括境内网上购物服务运营者数据安全保护措施、境外数据接收方数据安全保护措施，以及所在国家和地区的网络安全环境、数据保护法律体系的完善性等；

   注 1：通过数据出境合同、数据跨境传输协议、数据处理协议等明确境内网上购物服务运营者及境外数据接收方的责任与义务，保障个人信息主体合法权益。

   注 2：境外接收方已通过 ISO27001、ISO27017、ISO27018、ISO27701、ISO 29151 等国际及国内权威数据隐私安全认证体系的最新认证，并可提供有效的认证证明的，可认定为数据接收方具备完备且有效的管理制度，采用了较先进、完善和有效的数据安全保护措施，能有效防止数据泄露、毁损、篡改、滥用等事件发生。

   4) 根据数据出境的综合影响，以及境内网上购物服务运营者、境外数据接收方的数据安全保障能力，综合分析数据出境可能对国家安全、社会公共利益、个人合法利益带来的风险。
b) 当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，及时重新进行安全评估；
c) 建立个人信息出境记录；
d) 根据业务发展和运营情况，每年对数据出境至少进行一次安全评估。

10 数据存储和删除

网上购物服务运营者在数据存储和删除活动中，要求如下：

a） 应将会员数据、订单数据与用户生物识别信息在数据库表级分开存储；
b） 个人信息存储期限为实现授权用户使用的目的所必需的最短时间；
c） 网上购物服务的商品和服务信息、交易信息保存时间自交易完成之日起应不少于三年；
d） 网上购物服务其他信息保存时间要求参见附录 D。

11 个人信息主体权利

11.1 个人信息查询

网上购物服务运营者在给用户提供个人信息查询活动中，要求如下：

a) 应提供给个人信息主体访问和查询的个人信息包括：
   1) 用户通过主动填写的方式提交给网上购物服务运营者的相关个人信息，如个人账户信息、个人档案信息、收货人信息、发票信息等；
   2) 用户未主动删除的订单信息；
   3) 用户对商品或服务主动填写发布的评论信息；
b) 网上购物服务运营者可选择为个人信息主体提供的查询的相关信息，包括浏览记录、收藏商品或服务、关注店铺、会员权益等。

11.2 个人信息更正

网上购物服务运营者在给用户提供个人信息更正活动中，要求如下：

a) 个人信息主体可更正的个人信息包括：用户通过主动填写的方式提供给网上购物服务运营者的相关个人信息，如个人身份信息、收货人信息、发票信息等；

b) 网上购物服务运营者应提供追加评论的功能，实现个人信息主体对其评价信息的补充。

11.3 个人信息删除

网上购物服务运营者在给用户提供个人信息删除活动中，要求如下：

a) 个人信息主体可选择删除的信息为用户通过主动填写的方式提供给网上购物服务运营者的相关个人信息，如个人身份信息、个人档案信息、收货人信息、发票信息等。

b) 网上购物服务运营者不应删除个人信息主体的评价信息，含有下列内容的，可以采取屏蔽相关评价内容的方式消除评价信息的恶劣影响：

1) 评价信息中明显含有侵犯第三方知识产权及商业秘密的内容；

2) 评价信息中含有侵犯第三方个人隐私的内容；

3) 评价信息中含有诽谤、侮辱、淫秽色情、危害国家安全和公共安全等法律、行政法规禁止发布的内容；

4) 其他明显违反法律、法规的规定，需要屏蔽评价内容的情形。网上购物服务运营者经营者依照前款规定屏蔽评价内容的，应及时告知个人信息主体和网上购物服务运营者内经营者屏蔽信息的内容及理由，保存相关数据信息。

11.4 注销账户

网上购物服务运营者在给用户提供主席账户活动中，要求如下：

a) 应以显著方式提示用户注销账号后，其权益和资产可能受到的影响；

注：如账户信息、会员权益、虚拟资产无法恢复或无法享受相关在线售后服务。

b) 如有以下情形的，应提示用户无法注销的原因：

1) 在最近一个月内，账户有进行更改密码、更改绑定信息等敏感操作；

2) 不同意放弃账户在系统中的资产和虚拟权益自愿放弃、无拍卖保证金、无欠款；

3) 账户内有未完成的订单和服务；

4) 有使用账户激活店铺的记录；

5) 账户存在未解决的纠纷，包括投诉举报或被投诉举报；

6) 未对绑定的支付账户等关联账户解除关联；

7) 账户未解除与其他网站、其他 APP 的授权登录或绑定关系；

c) 账户如同时是网上购物服务运营者卖家店铺的绑定账户名，须先解除相关绑定。

12 网上购物服务典型场景数据安全要求

12.1 无人店铺数据安全保护

12.1.1 进店

网上购物服务运营者在无人店铺用户进店场景中，要求如下：

a) 用户进店前，应当明确告知店铺和进行身份识别的第三方支付工作分别收集和使用个人信息的类型、目的和方式，以及进行数据交互、传输的个人信息类型和目的；

b) 店铺仅可向第三方支付工具传输人脸信息等识别身份的必要信息，人脸信息宜传输特征值；

c) 店铺向第三方支付工具传输人脸、第三方支付工具向店铺返回用户身份识别标识符时（例如会员 ID、手机号码），应进行加密传输。

12.1.2 购买

网上购物服务运营者在无人店铺用户购买场景中，要求如下：

a） 应向用户显著提示已进入视频监控范围且行为会被记录；

b） 记录用户逛店、取货等店内行为时，不应使用手机号、身份证号等个人敏感信息作为用户身份标识，宜随机分配具有专属特性的身份识别标识符。

12.1.3 支付

网上购物服务运营者在无人店铺用户支付场景中，要求如下：

a） 支付时，店铺仅可向第三方支付工具共享用户身份识别标识符、商品名称/编码、数量、价格等用于支付的必要信息，不宜共享其他个人信息；

b） 店铺向第三方支付工具传输上述 a）信息时，宜进行加密传输。

12.2 基于位置的网上购物数据安全保护

12.2.1 位置信息的收集

对网上购物服务运营者收集位置信息的要求包括：

a） 不应强迫用户将授权位置权限作为使用服务的前提条件，应为选择拒绝的用户提供替代解决方案。

注：例如如果用户拒绝位置权限，可提供手动输入地址的功能

b） 未经用户同意，不应私自更改用户设置的位置权限状态。

注：用户设置的位置权限状态是指针对特定应用设置的可获取位置权限的状态，一般包括“始终允许”、“使用期间允许”、“从不允许”等。

12.2.2 位置信息的使用

网上购物服务运营者应与用户明确约定位置信息的处理目的和使用用途，超出必要范围的应该重新征得用户的授权同意。

12.2.3 位置信息的共享

非基于提供服务所必要不应共享用户的位置信息，获取用户明确同意的除外。

注:提供服务所必要一般指为用户提供基于地理位置的服务，包括外卖、出行、地图导航等。

附 录 A
（资料性）
网上购物服务数据分类分级示例

A.1 网上购物服务数据类别范围

网上购物服务数据是指提供网上购物服务过程中，经网上购物服务平台直接收集或产成的数据。网上购物服务数据可分为：用户数据、业务数据，具体内容如表 A.1 所示。

表A.1　网上购物服务数据类别与范围

数据类别	范围
用户数据	1)个人基本资料，包括姓名、生日、性别、头像、账户/会员等级、所在地区、收货地址、手机号码、电子邮件地址等； 2)个人身份信息，包括身份证、护照等； 3)个人生物识别信息，包括面部识别特征、声纹等； 4)网络身份标识信息，包括会员账号或会员名、昵称、IP地址等； 5)个人生理信息，包括身高、体重、三围、鞋码等； 6)个人财产信息，包括银行账户、鉴别信息、网络支付账户、交易和消费记录、会员积分等； 7)个人通信信息，包括与客服的通信/通话记录等； 8)联系人信息，包括代付款人姓名、手机号码、会员昵称，好友的昵称等； 9)个人上网记录，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、搜索记录、点击记录、收藏列表、关注店铺等； 10)个人常用设备信息，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）等个人常用设备基本情况的信息 11)个人位置信息，行踪轨迹、精准定位信息、经纬度等； 12)其他信息，用户纠纷记录、用户评价与被评价信息等。
业务数据	1)业务统计数据,包括各类目的交易明细/排名、类目的交易成交总额、页面浏览量、用户访问量等； 2)业务经营数据，包括卖家等级、活动规则、活动方案、类目数据、合作授权价格、优惠活动浮动区间等； 3)业务技术数据，包括算法模型、技术指标参数、技术方案等。

A.2 网上购物服务数据分级规则

根据数据重要程度、敏感程度、数据泄露造成的风险以及国家法律法规要求，可将网上购物服务数据分为4级：第1级为非敏感数据，第二级为较敏感数据，第三级为敏感数据，第四级为高敏感数据。

a) 第1级非敏感数据是指可以被公共访问和或被用户设置为公开发布的数据，此类数据的公开对网上购物服务用户或网上购物服务业务不会产生不良影响。具体包括：

1）.....用户非敏感数据：用户自行公开发布的合法数据，该数据的自由传播是促进相关网上购物服务活动开展的必要条件；

示例：交易评价等用户输入并公开的数据。

2）.....业务非敏感数据：网上购物服务平台运营者或平台内运营者公开发布的数据，该数据的自由传播不会产生任何安全或法律问题；

示例：卖家的等级、已发布的活动规则、已发布的商品类目。

b) 第2级较敏感数据是指大范围开放可能会对业务或用户造成较小或者不显著的负面影响，但因用户或业务要求需要对指定群体开放的数据。2级数据需经数据所有者授权在特定范围内开放，具体包括：

1） 用户较敏感数据：用户已授权可对指定人群公开的数据；

示例：与客服人员的通信/通话记录及相关内容。

2） 业务较敏感数据：仅限相关业务员工或签署了相应业务保密协议的第三方人员使用的数据，如果泄露，可能会对该局部业务、客户或者员工造成较小或者不显著的负面影响；

示例：业务交易成交总额。

c) 第3级敏感数据是指内部管理和业务运营需要且不应广泛公开的数据，具有较高商业价值，如果发生非授权的泄露，将直接或间接给用户和业务造成不利影响或损害。

1） 用户敏感数据：不能识别特定自然人，但能够与其他信息结合识别特定自然人身份的数据；

示例：电话、电子邮箱、购买记录。

2） 业务敏感数据：仅限组织内部相关业务员工使用的数据，如果泄露，会对业务或网上购物服务平台产生不利影响，造成经济损失、信誉破坏，并可能发生法律责任；

示例：核心业务的各种交易明细/排名。

d) 第4级高敏感数据是指具有极高商业价值的数据，即使极少量的泄露也将对业务、用户造成严重不利影响和损害。

1） 用户高敏感数据：个人敏感信息以及能够单独识别特定自然人身份的数据；

示例：身份证号、护照号、用户账户密码。

2） 业务高敏感数据：仅限组织内部极少数特点人员访问的数据，如果泄露，会对业务或网上购物服务平台产生严重不利影响，甚至是对业务造成毁灭性的影响，牵扯到重大法律责任的数据；

示例：合作授权价格、优惠活动浮动区间。

附 录 B
（资料性）
网上购物服务可选个人信息收集范围及使用要求

网上购物服务运营者可选个人信息收集范围及使用要求如表B.1所示：

表B.1 网上购物服务可选个人信息收集范围及使用要求

个人信息类型	使用要求
个人基本资料：姓名、性别、出生年月日、居住地、昵称、头像	仅用于为用户提供生日权益等附加会员服务
个人上网记录（仅限网上购物平台内部的上网记录）：业务功能使用记录、点击记录、收藏列表、关注列表	仅用于满足用户收藏、加购、关注等需求
个人身份信息：姓名、身份证件号码、身份证件照片 个人生物识别信息：人脸、声纹	仅用于实人会员认证服务、刷脸登录、用声音进行身份验证、语音购物服务，更好的保障账户安全
联系人信息：通讯录、好友列表	仅用于代付款、添加好友、从通讯录选择联系人作为收件人、通过读取通讯录的形式选择充值号码、社交分享等功能
个人通信信息：通信/通话记录	仅用于提供售后服务、改进服务质量的需求
个人基本资料：性别、职业 个人生理信息：身高、体重、三围、鞋码	仅用于网上购物服务中提供个性化服务的需求，如线上线下融合购物中线下导购根据用户资料进行商品推荐
其他信息：用户发布的评论信息	完成评论信息发布功能的需求

附 录 C
（资料性）
网上购物服务 App 相关系统权限申请范围及使用要求

网上购物服务 App 相关系统权限申请范围及使用要求如表 C.1、表 C.2 所示：

C.1 Android 权限范围

表C.1 Android App相关系统权限申请范围及使用要求

权限名称	使用要求
访问粗略位置 ACCESS_COARSE_LOCATION	仅用于本地生活服务、同城购物等分区域信息推荐等服务
访问精准定位 ACCESS_FINE_LOCATION	用户添加当前位置的收货地址、O2O 上门服务定位用户位置等服务
读取通讯录 READ_CONTACTS	仅用于添加联系人、选择联系人作为收件人、通过读取通讯录的形式选择充值号码等服务
读取外置存储器 READ_EXTERNAL_STORAGE	用于图片搜索商品、评论等服务
写入外置存储器 WRITE_EXTERNAL_STORAGE	用于存储拍摄的照片和视频
拍摄 CAMERA	扫描二维码/条形码、人脸认证、图片搜索商品、评论等服务
录音 RECORD_AUDIO	语音识别、音视频录制、语音搜索商品、与客服语音交流等服务
编辑日历 WRITE_CALENDAR	向用户提供购物或领取权益相关记录及提醒
读取日历 READ_CALENDAR	取消日历提醒，需要读取日历进行确认

C.2 iOS 权限范围

表C.2 iOS App相关系统权限申请范围及使用要求

权限名称	使用要求
麦克风 Microphone	仅用于语音识别、音视频录制、直播、语音搜索商品或购物、与客服语音交流等
通讯录 Contacts	仅用于添加联系人、选择联系人作为收件人、通过读取通讯录的形式选择充值号码等
始终访问位置 Location Always and When In Use	仅用于基于位置提供的服务
访问位置	仅用于基于位置提供的服务

权限名称	使用要求
Location	
使用期间访问位置 Location When In Use	仅用于基于位置提供的服务
相机 Camera	扫描二维码/条形码、人脸认证、图片搜索商品、评论、客服等服务
读取和写入照片库 Photo Library	更换头像、图片搜索商品、发表评论、与客服员沟通等服务
日历 Calendars	向用户提供购物或领取权益相关记录及提醒

附 录 D
（资料性）
网上购物服务数据保存期限及法律法规依据

表D 网上购物服务数据保持期限及法律法规依据

数据类型		法律规定的保存期限	法律法规依据
民事诉讼相关必要信息		不少于 3 年	民法典第 188 条
业务数据	商品和服务信息、交易信息	自交易完成之日起不少于 3 年	电子商务法第 31 条
	交易记录等其他信息记录备份	自交易完成之日起不少于 2 年	网络交易管理办法第 30 条
账号主体身份信息	经营者的营业执照或者个人真实身份信息记录	从经营者在平台的登记注销之日起不少于 2 年	网络交易管理办法第 30 条
电商直播内容信息	互联网直播服务使用者发布内容和日志信息	保存 60 日	互联网直播服务管理规定第 16 条
相关网络日志	相关的网络日志	不少于 3 年	网络安全法第 21 条
违法信息内容	违法信息内容	发现后保存	网络信息内容生态治理规定第 10 条
	法律、行政法规禁止发布或者传输的信息		网络安全法第 47 条

参 考 文 献

[1] GB/T 38652—2020 电子商务业务术语