ICS 35.240.01
CCS L 80

团 体 标 准

T/CEATEC XXX-2025

电商用户隐私数据安全处理规范

Specifications for secure processing of e-commerce user privacy data

2025-X-XX 发布 2025-X-XX 实施

中国欧洲经济技术合作协会 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。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件主要起草单位：。

本文件主要起草人：。

本文件为首次编制。

电商用户隐私数据安全处理规范

1 范围

本文件规定了电子商务活动中用户隐私数据安全处理的基本原则、数据分类与分级、全生命周期安全要求、安全管理保障以及评估与改进。

本文件适用于电子商务平台运营者、平台内经营者以及为电子商务提供数据处理的第三方服务商在处理用户隐私数据过程中的安全保护活动。

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 22239 信息安全技术 网络安全等级保护基本要求
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
GB/T 44588 数据安全技术 互联网平台及产品服务个人信息处理规则
GB/T 45392 数据安全技术 基于个人信息的自动化决策安全要求
GB/T 45574 数据安全技术 敏感个人信息处理安全要求
GB/T 45577 数据安全技术 数据安全风险评估方法

3 术语和定义

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

3.1

电商用户隐私数据 e-commerce user privacy data

电子商务活动中收集的，能够单独或者与其他信息结合识别特定电商用户身份或反映特定电商用户活动情况的各种信息。

3.2

电商平台数据处理者 e-commerce platform data processor

电子商务平台运营者、平台内经营者以及为电子商务提供数据处理的第三方服务商的统称，能够确定电商用户隐私数据处理目的和处理方式。

3.3

个人信息主体 personal information subject

电商用户隐私数据所标识或关联的自然人。

3.4

明示同意 explicit consent

个人信息主体通过书面声明或主动做出肯定性动作，对其特定个人信息进行处理所表示的明确授权。

3.5

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，无法识别特定个人信息主体的过程。

3.6

自动化决策 automated decision-making

通过计算机程序自动分析、评估个人的行为习惯、兴趣爱好或经济、健康、信用状况等，并进行决策的活动。

3.7

数据安全风险评估 data security risk assessment

对数据在处理全过程中的安全风险进行识别、分析和评价的活动。

4 基本原则

4.1 合法合规原则

电商用户隐私数据处理应当遵循法律、行政法规的规定，遵循网络安全与个人信息保护相关国家标准的要求，具体安全技术与管理要求应满足 GB/T 22239 的相关规定，不得从事法律法规禁止的活动。

4.2 权责一致原则

电商平台数据处理者对其处理的用户隐私数据安全负责，承担相应保护责任，采取必要安全保障措施，防止数据泄露、损毁、丢失、篡改。

4.3 目的明确原则

具有明确、具体、合法的数据处理目的，不应超出实现处理目的的最小范围收集和使用用户隐私数据。

4.4 公开透明原则

以明确、易懂和合理的方式公开数据处理规则，明示处理的目的、方式、范围以及数据安全保护措施等信息。

4.5 确保安全原则

采取必要措施保护用户隐私数据安全，包括技术防护措施和安全管理措施，确保数据在处理全过程中的保密性、完整性、可用性。

4.6 主体参与原则

保障个人信息主体对其隐私数据的知情权、决定权、查询权、更正权、删除权、撤回同意权等合法权利。

5 数据分类与分级

5.1 数据分类体系

电商用户隐私数据分类应符合表1要求：

表1 电商用户隐私数据分类表

大类	小类	示例	保护要求
个人基本资料	身份信息	姓名、身份证号、护照号	加密存储、访问控制
	生物识别信息	人脸、指纹、声纹	加密存储、访问控制、单独授权
个人财产信息	账户信息	银行账号、第三方支付账号	加密传输、加密存储
	交易记录	订单金额、消费记录	访问控制、安全审计
个人位置信息	精准位置信息	GPS 定位、详细地址	去标识化、目的限制
	大概位置信息	城市、区域	访问控制
个人行为信息	浏览记录	商品浏览、页面停留	用户授权、退出机制
	搜索记录	关键词、搜索时间	用户授权、去标识化
设备信息	设备标识	IMEI、MAC 地址、Android ID	加密存储、访问控制
	应用列表	安装应用信息	明示同意、最小必要

5.2 数据分级标准

5.2.1 数据分级

根据数据遭到篡改、破坏、泄露或非法利用后，对国家安全、公共利益、个人权益、企业合法权益造成的潜在影响程度，将电商用户隐私数据分为三个级别，分级方法参照GB/T 45577，数据分级应符合表2要求：

表2 电商用户隐私数据分级表

级别	影响程度描述	典型示例	加密要求	访问控制	审计要求
1 级（敏感级）	一旦泄露可能导致个人信息主体的人格尊严受到侵害或人身、财产安全受到严重危害	身份证号、银行账号、生物识别信息、精准位置信息	国密算法 SM4/AES-256 及以上	双因子认证、动态权限	完整记录、留存 3 年
2 级（重要级）	一旦泄露可能导致个人信息主体受到歧视或人身、财产安全受到一般危害	姓名+手机号、订单记录、消费偏好、设备信息	国密算法 SM4/AES-128 及以上	角色权限控制	关键操作记录、留存 2 年
3 级（一般级）	除 1 级、2 级外的其他用户隐私数据	大概位置信息、脱敏后的浏览记录	传输加密 TLS1.2 及以上	基础身份验证	重要操作记录、留存 1 年

5.2.2 数据分级管理

数据分级实行动态管理，电商平台数据处理者应当至少每12个月对数据分级进行复查和更新，当业务模式、法律法规、技术环境发生变化时，应当及时调整数据级别。

6 全生命周期安全要求

6.1 数据收集

6.1.1 电商平台数据处理者在收集用户隐私数据前，应当以显著方式、清晰易懂的语言真实、准确、完整地向个人信息主体告知下列事项：

a) 电商平台数据处理者的身份和联系方式；
b) 数据处理的目的、方式、种类、保存期限；
c) 个人信息主体行使权利的方式和程序；
d) 其他应当告知的事项。

6.1.2 收集用户隐私数据应当取得个人信息主体的明示同意，在个人信息主体充分知情的前提下，自愿、明确作出同意表示。禁止通过误导、欺诈、胁迫等方式获得同意。

6.1.3 收集用户隐私数据应当遵循最小必要原则，只处理满足数据处理目的的最小范围的用户隐私数据，不得过度收集。在 App、网站等界面中，不应将多项个人信息捆绑在一起要求个人信息主体一次性接受，而应当就各项个人信息逐一获取同意。

6.1.4 直接收集用户隐私数据时，应当采用安全可靠的渠道和方式，确保数据在传输过程中的安全。传输敏感个人信息时，应当使用 TLS1.2 及以上协议进行加密传输，加密密钥长度不低于 128 位，其技术实现与强度测试应遵循 GB/T 44588 中关于传输安全的要求。

6.2 数据存储

6.2.1 电商平台数据处理者应当根据数据分级结果，采取相应的安全存储措施。对于 1 级（敏感级）数据的加密存储与访问控制，其安全措施的保护强度不应低于 GB/T 45574 中规定的技术要求。

a) 1 级数据应当加密存储，并采取技术隔离措施单独存储；
b) 2 级数据应当加密存储；
c) 3 级数据应当采取访问控制措施保护。

6.2.2 加密存储应当采用国家密码管理部门批准的加密算法，加密密钥应当由电商平台数据处理者严格控制，并定期更换，密钥更换周期不应超过 12 个月。

6.2.3 用户隐私数据的存储期限应当为实现处理目的所必需的最短时间，法律行政法规另有规定的除外。存储期限届满后，应当对相应的用户隐私数据进行删除或匿名化处理。

6.2.4 在我国境内运营中收集和产生的用户隐私数据应当在境内存储，确需向境外提供的，应当通过国家网信部门组织的安全评估，并按照相关法律法规执行。

6.3 数据使用

6.3.1 电商平台数据处理者在使用用户隐私数据前，应当核对授权范围，确保使用行为与收集时声明的目的直接相关，超出授权范围的使用应当重新获取同意。

6.3.2 数据展示环节应当采取脱敏措施，防止用户隐私数据的过度暴露。在内部业务系统中展示用户隐私数据时，应当根据业务需求和岗位职责，对敏感信息进行脱敏展示。

6.3.3 电商平台数据处理者采用自动化决策机制进行个性化推荐或商业营销时，应符合 GB/T 45392 的规定，具体要求如下：

a) 保证决策的透明度和结果公平、公正；
b) 不得对交易价格等交易条件实施不合理的差别待遇；
c) 向个人信息主体提供针对其个人特征的选项，或者提供便捷的拒绝方式；
d) 定期审核自动化决策的算法机制和结果。

6.3.4 用户画像和个性化展示应当符合以下要求：

a) 用户画像方向应当与电商服务有直接关联；
b) 应当使用准确的数据标签和适当的算法模型；
c) 应当设立人工干预机制，防止基于用户画像的歧视性待遇；

d) 在向个人信息主体提供电子商务服务过程中，应当同时提供不针对其个人特征的选项。

6.4 数据共享与委托处理

6.4.1 电商平台数据处理者共享、转移用户隐私数据时，应当充分评估接收方的数据安全保护能力，通过合同等方式明确双方的安全责任和义务。

6.4.2 共享、转移 1 级数据前，应当取得个人信息主体的单独同意，并向个人信息主体告知接收方的身份、联系方式、处理目的、处理方式和个人信息的种类。

6.4.3 委托处理用户隐私数据时，应当与受托人约定委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务，并对受托人的数据处理活动进行监督。

6.4.4 电商平台数据处理者应当建立用户隐私数据共享、转移的安全评估机制，评估内容包括但不限于：

a) 共享、转移的目的是否明确、合法；
b) 共享、转移的数据范围是否必要；
c) 接收方的数据安全保护能力是否达标；
d) 法律责任和风险承担机制是否明确。

6.5 数据销毁

6.5.1 电商平台数据处理者应当建立用户隐私数据销毁策略和流程，明确销毁的条件、方法和技术要求。

6.5.2 数据销毁应当确保用户隐私数据不可恢复，销毁方法包括物理销毁和逻辑销毁：

a) 物理销毁包括销毁存储介质、纸质文件粉碎等；
b) 逻辑销毁包括数据擦除、覆盖等。

6.5.3 数据销毁过程应当保留相关记录，包括销毁的数据内容、销毁时间、销毁方式、操作人员、监督人员等信息，销毁记录至少保存 3 年。

6.5.4 存储介质需要报废或重新利用时，应当采用不可恢复的方式清除介质中的用户隐私数据，确保数据无法被恢复。

7 安全管理保障

7.1 组织架构

7.1.1 电商平台数据处理者应当建立与数据处理规模、安全风险等级相适应的数据安全管理组织架构，明确数据安全负责人和管理部门。

7.1.2 数据安全负责人应当具备数据安全专业知识和管理经验，全面负责数据安全保护工作，履行下列职责：

a) 组织制定数据安全保护计划并督促落实；
b) 组织开展数据安全风险评估，督促整改安全隐患；
c) 向主管部门报告数据安全保护和风险处置情况；
d) 受理处理数据安全相关投诉、举报。

7.1.3 电商平台数据处理者应当设立数据安全应急响应团队，负责安全事件的监测、预警、响应和处置。

7.2 人员管理

7.2.1 电商平台数据处理者应当对接触用户隐私数据的岗位人员进行背景审查，签订保密协议，明确数据安全保护责任。

7.2.2 定期对相关人员开展数据安全法律法规、专业知识、技能和意识的培训教育，培训频次每年不少于 2 次，每次不少于 8 学时。

7.2.3 建立数据安全责任考核机制，将数据安全保护情况纳入岗位绩效考核指标，对违反数据安全规定的行为进行责任追究。

7.3 安全事件应急响应

7.3.1　电商平台数据处理者应当制定数据安全事件应急预案，明确事件分级、处置流程、沟通机制和补救措施，并定期组织演练。

7.3.2　发现用户隐私数据泄露、篡改、丢失的，应当立即采取补救措施，并按照规定及时告知用户和向主管部门报告。

7.3.3　数据安全事件应急响应应当遵循以下流程：

a）　确认事件发生并启动应急响应；

b）　评估事件影响范围和危害程度；

c）　采取技术措施控制事态发展；

d）　调查事件原因并收集证据；

e）　消除安全隐患，恢复系统运行；

f）　记录事件处理全过程，总结经验教训。

8　评估与改进

8.1　合规性评估

8.1.1　电商平台数据处理者应当建立数据安全合规性评估机制，定期或不定期对用户隐私数据处理活动进行检查评估，评估频次每年不少于 1 次。

8.1.2　合规性评估内容包括但不限于：

a）　数据处理活动的合法合规性；

b）　数据安全保护措施的有效性；

c）　数据安全管理制度执行情况；

d）　数据安全风险评估和处置情况。

8.1.3　合规性评估应当形成评估报告，评估报告应当客观、真实、完整地反映评估情况，并提出整改建议和改进措施。

8.2　监测与持续改进

8.2.1　电商平台数据处理者应当建立数据安全风险监测机制，通过技术手段对用户隐私数据处理活动进行实时监测，及时发现异常行为和安全风险。

8.2.2　鼓励电商平台数据处理者采用人工智能、大数据等技术提升数据安全防护能力，实现数据安全风险的智能识别和自动处置。

8.2.3　电商平台数据处理者应当建立数据安全保护持续改进机制，根据技术发展、业务变化和风险评估结果，及时调整数据安全策略和措施。

8.2.4　数据安全绩效监测指标应当包括但不限于：

a）　数据安全事件数量及处置成功率；

b）　数据安全风险评估覆盖率；

c）　数据安全防护措施覆盖率；

d）　员工数据安全培训完成率；

e）　数据主体投诉处理及时率。

各项指标的具体定义、目标值及监测方法应符合表3要求：

表3 数据安全风险评估指标表

评估维度	评估指标	目标值	测量方法	监测频率
技术防护	加密技术应用覆盖率	≥95%	技术检测	季度
	访问控制有效性	≥98%	渗透测试	半年
管理控制	安全制度完善率	100%	文档审查	年度
	员工培训覆盖率	≥90%	记录检查	半年

评估维度	评估指标	目标值	测量方法	监测频率
合规性	授权同意合规率	100%	抽样检查	季度
	数据主体投诉率	≤0.5%	统计分析	月度
应急响应	应急演练完成率	100%	记录检查	年度
	事件响应及时率	≥95%	记录统计	月度