ICS

T/GXDSL

团　　体　　标　　准

T/GXDSL 293—2025

客户数据隐私保护管理规范

Specification for Customer Data Privacy Protection Management

征求意见稿

2025 - - 发布　　2025 - - 实施

广西电子商务企业联合会　发布

目　　次

前　言

本文件依据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。

本文件由广西产学研科学研究院提出。

本文件由广西电子商务企业联合会归口。

本文件起草单位：

本文件主要起草人：

本文件为首次发布。

客户数据隐私保护管理规范

1 范围

本标准规定了客户数据隐私保护的管理体系、数据全生命周期（收集、存储、使用、传输、共享、销毁）的管控要求、安全技术保障、合规审计与风险应对、责任追究等内容。

本标准适用于各类组织（包括企业、事业单位、社会团体等）在经营管理活动中涉及客户数据处理的全流程管理，涵盖线上线下各类数据采集渠道、数据处理场景，可作为组织建立客户数据隐私保护体系、开展合规管理的依据，也可作为第三方评估机构进行合规性评估的参考。

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 35273-2022 信息安全技术 个人信息安全规范

GB/T 38642-2020 信息安全技术 数据安全治理指南

GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求

《中华人民共和国个人信息保护法》

《中华人民共和国数据安全法》

《中华人民共和国网络安全法》

ISO/IEC 27001:2022 信息安全管理体系要求

ISO/IEC 27701:2019 隐私信息管理体系扩展要求

3 术语和定义

3.1 客户数据

指组织在与客户进行业务交互过程中收集、生成的与客户相关的各类数据，包括但不限于客户个人信息（姓名、身份证号、联系方式、生物识别信息等）、交易数据（购买记录、支付信息、消费偏好等）、行为数据（访问记录、操作日志、位置信息等）、账户数据（账号、密码摘要、权限信息等）。

3.2 数据隐私保护

指通过技术、管理、法律等手段，确保客户数据在收集、存储、使用、传输、共享、销毁等全生命周期过程中，不被非法收集、泄露、篡改、滥用，保障客户对其数据的知情权、决定权、访问权、更正权、删除权等合法权益。

3.3 数据控制器

指决定客户数据处理目的、方式的组织或个人。

3.4 数据处理者

指在数据控制器的授权范围内，具体执行客户数据处理操作的组织或个人。

3.5 敏感客户数据

指一旦泄露、非法提供或滥用，可能危害客户人身、财产安全，损害客户名誉、权益，或导致社会公共利益受损的客户数据，包括但不限于身份证号、银行账户信息、支付密码、生物识别信息、健康医疗数据、未成年人信息等。

3.6 数据脱敏

指通过对客户数据进行修改、替换、屏蔽等处理，使数据无法识别特定客户，且无法还原原始数据的技术手段。

3.7 数据最小化

指仅收集为实现特定业务目的所必需的客户数据，不收集超出业务需求的额外数据。

4 管理体系要求

4.1 组织与职责

4.1.1 组织应建立健全客户数据隐私保护组织架构，明确决策层、管理层、执行层的职责分工。决策层负责审批隐私保护战略、制度和重大决策；管理层负责制定隐私保护制度、规划实施计划、监督执行情况；执行层负责具体落实隐私保护措施、开展日常管理工作。

4.1.2 组织应指定专门的隐私保护负责人，全面统筹客户数据隐私保护工作，具备相应的法律知识、数据安全知识和管理能力，直接向组织决策层汇报工作。

4.1.3 组织应设立隐私保护工作小组，成员包括业务部门、技术部门、法务部门、合规部门等相关人员，负责协同推进隐私保护各项工作。

4.1.4 组织应明确各部门、各岗位的客户数据隐私保护职责，将隐私保护要求纳入岗位职责说明书，确保责任到人。

4.2 制度建设

4.2.1 组织应制定完善的客户数据隐私保护管理制度体系，包括但不限于总则、数据收集管理办法、数据存储管理办法、数据使用管理办法、数据传输管理办法、数据共享管理办法、数据销毁管理办法、敏感数据专项管理办法、应急响应预案、合规审计办法、责任追究办法等。

4.2.2 管理制度应符合相关法律法规和本标准要求，结合组织业务特点和数据处理场景，明确具体管理要求和操作流程，具有可操作性。

4.2.3 组织应定期对管理制度进行评审和修订，根据法律法规更新、业务变化、技术发展等情况，及时调整完善制度内容，确保制度的有效性和适用性。

4.2.4 组织应将客户数据隐私保护管理制度向全体员工公示，确保员工知晓并理解制度要求。

4.3 人员管理

4.3.1 组织应开展全员客户数据隐私保护培训，内容包括法律法规、管理制度、操作规范、风险防范知识等，新员工上岗前必须接受专项培训并考核合格，每年至少开展一次全员复训。

4.3.2 组织应对涉及客户数据处理的关键岗位人员进行背景审查，建立岗位权限清单，实行最小权限管理，定期开展权限复核。

4.3.3 组织应与员工签订保密协议，明确员工在客户数据处理过程中的保密义务和违约责任，员工离职时应办理数据交接手续，签订离职保密承诺书。

4.3.4 组织应建立客户数据隐私保护考核机制，将考核结果与员工绩效挂钩，对表现优秀的予以表彰奖励，对违反规定的予以处罚。

4.4 资源保障

4.4.1 组织应合理配置客户数据隐私保护所需的人力、物力、财力资源，确保隐私保护工作的顺利开展。

4.4.2 组织应投入必要的资金用于隐私保护技术研发、系统建设、设备采购、培训教育、合规审计等工作。

4.4.3 组织应配备具备相应专业能力的技术人员和管理人员，负责隐私保护技术实施、系统运维、风险评估等工作。

5 数据全生命周期管控要求

5.1 数据收集

5.1.1 数据收集应遵循合法、正当、必要、诚信的原则，不得通过欺诈、胁迫、误导等非法手段收集客户数据。

5.1.2 收集客户数据前，应向客户明确告知数据收集的目的、范围、方式、使用期限、共享范围、权利救济途径等信息，获得客户的明示同意。客户同意后，应提供便捷的撤回同意渠道。

5.1.3 收集敏感客户数据时，应单独获得客户的书面同意或通过其他明确可追溯的方式获得同意，并对

收集过程进行全程记录。

5.1.4 严格遵循数据最小化原则，仅收集实现业务目的所必需的客户数据，不得收集与业务无关的额外数据。

5.1.5 数据收集渠道应安全可靠，线上渠道应采用加密传输技术，线下渠道应建立规范的收集流程，防止数据丢失或泄露。

5.1.6 收集的客户数据应真实、准确、完整，及时纠正错误或不完整的数据，对于无法核实的无效数据应及时清理。

5.2 数据存储

5.2.1 客户数据存储应采用符合安全标准的存储设备和存储系统，具备数据备份、容灾恢复能力，定期开展备份数据的恢复测试，确保备份数据的可用性。

5.2.2 敏感客户数据应采用加密存储方式，加密算法应符合国家相关安全标准，密钥管理应遵循最小权限、定期更换、安全存储的原则。

5.2.3 客户数据存储期限应遵循最小必要原则，仅保留为实现业务目的所必需的最短时间，超出存储期限的数据应按照规定进行销毁或匿名化处理。

5.2.4 建立客户数据存储分级管理制度，根据数据敏感程度划分存储安全等级，采取相应的安全防护措施，高敏感数据应采取物理隔离、专人保管等强化保护措施。

5.2.5 存储系统应具备访问控制、日志审计功能，记录数据存储、访问、修改等操作行为，日志留存时间不少于 6 个月。

5.2.6 不得将客户数据存储在境外，确需向境外存储的，应按照相关法律法规规定进行安全评估和审批，并采取相应的安全保障措施。

5.3 数据使用

5.3.1 客户数据的使用应符合收集时告知的目的，不得超出授权范围使用，如需变更使用目的，应重新获得客户的明示同意。

5.3.2 使用客户数据时应遵循合法、合规、诚信原则，不得利用客户数据从事危害国家安全、公共利益，或侵害客户合法权益的活动。

5.3.3 处理敏感客户数据时，应采取强化保护措施，包括但不限于限制访问权限、全程监控使用过程、定期进行安全审计等。

5.3.4 严禁未经授权向内部无关人员或外部第三方提供客户数据，内部员工因工作需要使用客户数据的，应履行审批手续，遵循最小权限和按需分配原则。

5.3.5 利用客户数据进行数据分析、建模、算法应用等活动时，应确保分析过程不泄露客户隐私，分析结果不得识别特定客户，如需使用原始数据，应进行脱敏处理。

5.3.6 建立客户数据使用授权管理制度，明确授权流程、权限范围和有效期，定期对授权情况进行复核，及时回收过期或闲置权限。

5.4 数据传输

5.4.1 客户数据传输应采用加密传输技术，包括但不限于 SSL/TLS、VPN 等，确保传输过程中数据的保密性和完整性，防止数据被拦截、篡改。

5.4.2 建立数据传输审批制度，内部部门之间传输客户数据应履行审批手续，向外部传输客户数据应严格按照共享管理要求执行，确保传输行为合法合规。

5.4.3 数据传输前应对传输设备和传输通道进行安全检测，防止通过不安全的设备或通道传输数据，导致数据泄露。

5.4.4 敏感客户数据传输应采取额外的安全保障措施，如专线传输、二次加密、传输过程全程监控等。

5.4.5 建立数据传输日志记录制度，记录传输时间、传输方向、传输内容、传输人员等信息，日志留存时间不少于 6 个月，便于追溯核查。

5.5 数据共享

5.5.1 共享客户数据应遵循合法、必要、诚信原则，仅在获得客户明示同意或法律法规规定的情形下进行，不得擅自向第三方共享客户数据。

5.5.2 共享前应评估接收方的隐私保护能力，确保接收方具备相应的安全防护措施和管理水平，能够保障客户数据的安全。

5.5.3 与接收方签订数据共享协议，明确共享数据的范围、用途、使用期限、安全责任、保密义务等内容，约定数据共享后的后续管理要求。

5.5.4 共享敏感客户数据时，应采取脱敏处理、访问控制等安全措施，限制接收方的使用权限和使用范围，防止数据被滥用。

5.5.5 建立数据共享备案制度，对共享数据的情况进行详细记录，包括共享对象、共享内容、共享时间、审批情况等，定期进行合规审查。

5.5.6 发现接收方存在违规使用、泄露共享数据等情况时，应立即终止共享，并要求接收方采取补救措施，追究其违约责任，必要时向相关监管部门报告。

5.6 数据销毁

5.6.1 客户数据达到存储期限、实现业务目的或客户要求删除数据时，应及时进行销毁处理，确保数据无法被恢复。

5.6.2 数据销毁应根据数据存储介质的类型，采用相应的销毁方式：电子数据应采用数据覆盖、物理销毁存储介质等方式；纸质数据应采用粉碎、焚烧等方式。

5.6.3 建立数据销毁审批制度，数据销毁前应履行审批手续，明确销毁数据的范围、方式、责任人员等。

5.6.4 数据销毁过程应进行全程记录，包括销毁时间、销毁方式、销毁内容、参与人员、监销人员等信息，记录留存时间不少于 3 年。

5.6.5 委托第三方进行数据销毁的，应选择具备相应资质和能力的机构，签订销毁协议，明确安全责任和保密义务，并对销毁过程进行监督。

6 安全技术保障

6.1 访问控制技术

6.1.1 建立严格的身份认证机制，采用多因素认证、密码复杂度要求、定期密码更换等措施，确保数据访问者身份的真实性。

6.1.2 基于角色的访问控制（RBAC）模型，为不同岗位的员工分配相应的访问权限，实现最小权限管理，防止越权访问。

6.1.3 对敏感客户数据的访问进行严格控制，采用单独的访问审批流程，记录访问日志，包括访问时间、访问人员、访问内容、操作行为等。

6.1.4 定期对访问权限进行审计和清理，回收过期、闲置或离职人员的访问权限，确保权限与岗位职责匹配。

6.2 数据加密技术

6.2.1 对客户数据进行全生命周期加密保护，包括传输加密、存储加密、使用加密等，加密算法应符合国家密码管理相关标准。

6.2.2 敏感客户数据应采用高强度加密算法，密钥管理应遵循安全、可控的原则，建立密钥生成、存储、分发、更换、销毁等全流程管理制度。

6.2.3 采用加密机、加密卡等专用加密设备，提高加密运算的安全性和效率，防止密钥泄露。

6.2.4 定期对加密技术和加密算法进行评估和更新，应对加密技术面临的安全风险。

6.3 数据脱敏技术

6.3.1 对非必要场景下使用的客户数据进行脱敏处理，根据数据使用场景和敏感程度，选择合适的脱敏方式，包括替换、屏蔽、截断、混淆等。

6.3.2 脱敏处理应确保处理后的数据无法识别特定客户，且无法还原原始数据，同时保证数据的可用性，不影响业务正常开展。

6.3.3 建立数据脱敏规则库，明确不同类型客户数据的脱敏标准和操作流程，定期对脱敏规则进行评审和优化。

6.3.4 对脱敏处理过程进行全程监控和记录，确保脱敏操作的合规性和可追溯性。

6.4 安全审计技术

6.4.1 建立全面的安全审计系统，对客户数据全生命周期的操作行为进行实时监控和日志记录，包括数据收集、存储、使用、传输、共享、销毁等各个环节。

6.4.2 审计日志应包含操作时间、操作人员、操作对象、操作内容、操作结果等关键信息，日志留存时间不少于 6 个月，确保可追溯、可核查。

6.4.3 采用日志分析技术，对审计日志进行实时分析和异常检测，及时发现非法访问、数据泄露、篡改等安全事件，并发出告警。

6.4.4 定期对审计日志进行审查和分析，形成审计报告，为合规检查、风险评估、责任追究提供依据。

6.5 应急响应技术

6.5.1 建立客户数据安全应急响应系统，具备数据泄露检测、漏洞扫描、入侵检测等功能，能够及时发现和处置安全事件。

6.5.2 制定应急响应预案，明确应急响应流程、责任分工、处置措施、恢复方案等，定期开展应急演练，提高应急处置能力。

6.5.3 发生数据安全事件时，应立即启动应急响应预案，采取切断泄露源、控制影响范围、数据恢复等措施，减少损失。

6.5.4 建立安全事件报告制度，发生重大数据安全事件时，应及时向相关监管部门和客户报告，并配合开展调查处理工作。

7 合规审计与风险应对

7.1 合规审计

7.1.1 组织应定期开展客户数据隐私保护合规审计，审计频率不少于每年一次，可根据业务变化、法律法规更新等情况增加审计次数。

7.1.2 合规审计应涵盖管理制度执行情况、数据全生命周期管控情况、安全技术保障措施落实情况、人员培训情况等内容，采用现场检查、文档审查、技术检测等多种审计方法。

7.1.3 委托第三方机构开展合规审计的，应选择具备相应资质和专业能力的机构，明确审计范围和要求，审计结果作为改进隐私保护工作的重要依据。

7.1.4 建立合规审计档案，记录审计过程、审计结果、整改情况等信息，档案留存时间不少于 3 年。

7.1.5 对审计发现的问题，应制定整改计划，明确整改责任人和整改期限，跟踪整改落实情况，确保问题得到及时解决。

7.2 风险评估

7.2.1 组织应定期开展客户数据隐私保护风险评估，评估频率不少于每年一次，发生重大业务变更、系统升级、数据安全事件等情况时，应及时开展专项风险评估。

7.2.2 风险评估应识别数据处理过程中存在的安全风险，包括数据泄露、篡改、滥用、非法收集等风险，分析风险发生的可能性和影响程度，确定风险等级。

7.2.3 针对不同等级的风险，制定相应的风险应对措施，包括风险规避、风险降低、风险转移、风险接受等，明确措施实施责任人和实施期限。

7.2.4 建立风险评估档案，记录风险评估过程、评估结果、应对措施、实施效果等信息，档案留存时间不少于