|  |  |
| --- | --- |
| ICS | 35.110 |
| CCS |

|  |
| --- |
|  |

L 80  |

团体标准

T/ZS XXXX—2024

网络支付服务数据安全规范

Data Security Specification for Internet Payment Services

（征求意见稿）

2024-xx-xx发布

2024-xx-xx实施

浙江省产品与工程标准化协会  发布

目次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 概述 1

5 基本要求 2

6 数据安全服务内容 2

参考文献 5

1. 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。

本文件起草单位：杭州乒乓智能技术有限公司。

本文件主要起草人：XXX。

网络支付服务数据安全规范

* 1. 范围

本文件规定了网络支付服务数据安全的概述、基本要求、服务内容等内容。

本文件适用于网络支付服务数据的安全管理。

* 1. 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 35273-2020 信息安全技术 个人信息安全规范

GB/T 37988 信息安全技术 数据安全能力成熟度模型

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

GB/T 41460 非银行支付机构支付业务设施技术要求

GB/T 41479 信息安全技术 网络数据处理安全规范

GB/T 42015 信息安全技术 网络支付服务数据安全要求

JR/T 0171 个人金融信息保护技术规范

* 1. 术语和定义

GB/T 42015界定的以及下列术语和定义适用于本文件。

网络支付服务 internet payment service

收款方或付款方通过计算机、移动终端等电子设备，依托互联网远程传输支付指令完成直接或间接货币资金转移的经营活动。

网络支付服务平台 internet payment service platform

通过互联网网络为收款方和付款方提供网络支付服务，同网络支付服务账务平台交互完成资金划拨的信息系统。

网络支付服务账务平台 internet payment service accounting platform

为网络支付服务提供账户管理、资金划拨、账务核算等服务的信息系统。

网络支付服务提供者 internet payment service provider

通过网络支付服务平台，提供网络支付服务的组织。

网络支付服务数据 internet payment service data

网络支付服务提供者在开展网络支付服务过程中收集和产生的数据。

注：网络支付服务数据包括用户数据和业务数据，不包括网络支付服务提供者内部管理数据。

网络支付服务用户 internet payment service user

使用网络支付服务的个人或组织，包括收款方和付款方。

注：本文件中简称用户。

* 1. 概述

网络支付服务业务功能主要包括用户注册/登录/注销、绑定银行卡、充值/提现、实名认证、生成支付订单、购汇/结汇、支付和对账结算等。

网络支付服务的相关方包括收款方、付款方、网络支付服务平台和网络支付服务提供者。其中，网络支付服务提供者运营网络支付服务平台，网络支付服务平台接收付款方的支付请求，将支付结果返回收款方，并与网络支付服务账务平台安全交互实现账务处理、完成网络支付服务。

网络支付服务数据应包括以下内容：

1. 用户数据：网络支付服务提供者在提供网络支付服务过程中收集和产生的个人及组织用户数据，如个人自然信息、个人身份鉴别信息等；
2. 业务数据：在网络支付服务业务开展过程中处理的用于保障业务正常运行的数据，如商户签约信息、支付结算信息等。
	1. 基本要求
		1. 业务管理合规性

网络支付服务数据处理活动应符合GB/T 41479中规定的要求。

网络支付服务业务操作应符合中国人民银行关于《非银行支付机构网络支付业务管理办法》的相关规定。

应根据实际业务操作场景，制定网络支付服务业务的规范化流程，确保业务操作的安全性和合规性。

应制定与网络支付服务业务相关的商户管理规范。

* + 1. 数据安全性

个人信息处理活动应符合GB/T 35273-2020中规定的要求，网络支付App个人信息收集活动应符合GB/T 41391-2022及JR/T 0171-2020中规定的要求。

网络支付服务提供者的数据安全能力至少符合GB/T 37988三级能力要求。

网络支付服务平台应符合GB/T 22239三级要求；对于核心支付系统，应达到GB/T 22239四级要求。

应结合数据处理活动的实际情况，按照有关国家标准定期开展数据安全风险评估。

* + 1. 技术安全性

网络支付服务的设施设备的基本要求应符合GB/T 41460的规定。

应建立主机安全管理制度，内容包括但不限于系统安全、数据库安全等。

应建立应用安全管理制度，内容包括但不限于代码安全、安全漏洞等。

应建立网络安全管理制度，内容包括但不限于网络隔离、流量检测等。

应建立数据安全管理制度，内容包括但不限于数据分级分类、数据加密保护等。

* + 1. 操作服务便捷性

网络支付服务的操作界面应简洁直观，方便用户进行支付操作。

应制定用户操作手册和常见问题解答，方便用户了解和使用网络支付服务。

* 1. 数据安全服务内容
		1. 数据收集

收集个人信息：网络支付服务提供者收集个人信息应符合GB/T 35273-2020要求。

用户授权：在收集用户数据前，应明确告知用户数据收集的目的、范围和使用方式，并取得用户的明确授权。

因业务需求需要更改数据用途前，应告知用户并得到用户同意。

* + 1. 数据存储和传输

网络支付服务提供者存储、传输数据，应在符合GB/T 35273-2020中第6章的要求基础上，遵守以下要求：

1. 应对用户数据进行分级分类，针对不同的等级采取不同的保护策略；
2. 存储和传输敏感个人信息时，应采用密码技术进行保护；应支持国家密码局发布的SM2及SM4国密算法；
3. 应对加密密钥进行保护，并对加密密钥进行定期轮换；
4. 因业务需要存储用户银行卡有效期的，应取得用户和网络支付服务账务平台的授权；并做好对有效期数据的加密保护；
5. 应至少使用本地备份、异地备份及场外备份中的两种方式对网络支付服务数据进行备份；
6. 应使用加密通道或数据加密的方式进行传输个人身份鉴别信息、可识别特定个人信息主体身份与资产状况的个人信息以及其他用于网络支付服务的关键信息；
7. 应采用密码技术保护个人身份鉴别信息的安全性。
	* 1. 数据使用和加工

数据展示

网络支付服务提供者数据展示应在符合GB/T 35273-2020中第7章的要求基础上，遵守以下要求：

1. 用户处于未登录状态时，不应展示用户信息；
2. 用户处于已登录状态时，应脱敏展示除银行卡有效期外的用户个人信息，如用户选择明文展示，应在展示前对用户身份进行验证；
3. 展示账单信息时，应仅展示用户支出和收入金额、费用发生时间、费用发生主体，未经用户明示同意，不应展示账户绑定的银行卡信息、账户余额信息、账单详情；
4. 如需展示账户绑定的银行卡信息、账户余额信息、账单详情等敏感信息，需对用户身份进行二次认证。

数据访问

网络支付服务提供者对用户个人信息的访问控制，应在符合GB/T 35273-2020中7.1的要求基础上，遵守以下要求：

1. 应遵循最少够用、职责分离的原则，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；
2. 对于涉及用户个人信息的操作，应通过建立审批流程、限制数据访问范围等措施，限制批查查询、导出用户个人信息的操作功能；
3. 需保存对于个人敏感信息的访问日志记录，并定期进行审计；
4. 应有机制保障在数据访问使用完毕后，及时删除个人敏感数据。

数据加工

网络支付服务提供者应在符合GB/T 35273-2020中7.4、7.5、7.7的要求基础上，遵守以下要求：

1. 未经用户单独同意，不应对用户交易记录进行分析挖掘；
2. 利用通过网络支付服务收集的个人信息进行自动化决策时，应允许用户自主选择；
3. 依据交易记录进行账单分类时，不应对用户购买商品的明细内容进行分析，取得用户单独同意的除外；
4. 应使用加密传输技术对数据加工传输过程中的用户敏感信息进行加密保护。
	* 1. 数据提供和公开

数据提供

网络支付服务提供者向第三方提供数据，应在符合GB/T 35273-2020中9.2、9.3要求的基础上，遵守以下要求：

1. 涉及向第三方提供用户个人信息的：
2. 应向用户告知第三方的名称或姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；
3. 应在提供前进行个人信息保护影响评估；
4. 应对第三方进行信息安全能力评估，确保第三方有效保护用户敏感信息。
5. 通过在网络支付平台中接入第三方应用或嵌入第三方软件开发工具包（SDK）的形式对外提供数据时：
6. 应符合GB/T 41391-2022中6.6规定的要求；
7. 用户跳转至第三方应用时，应提醒用户关注第三方应用的个人信息收集使用规则，涉及提供身份证件号码、地址等敏感个人信息的，宜在相关页面以具体活动规则或其他适当途径向用户告知个人信息收集使用规则；
8. 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数据保护责任。
9. 通过在第三方应用中嵌入网络支付服务软件开发工具包（SDK），提供网络支付服务时，不应将用户账户余额、银行卡绑定信息、个人身份鉴别信息、与当次支付行为无关的用户交易记录等数据提供给第三方应用。

数据公开

网络支付服务公开用户数据，应符合GB/T 35273-2020中9.4的要求。

* + 1. 数据删除

网络支付服务提供者删除数据，应符合GB/T 35273-2020中6.1和8.3的要求。

支付相关数据需满足监管要求的保存期限，在保存期限之内的数据不应删除。

* + 1. 数据出境

网络支付服务提供者如提供跨境支付服务，在境外商户消费、向境外汇款/接收境外汇款、为用户提供跨境支付结算服务等场景下，涉及数据出境、网络支付服务提供者数据出境应符合以下要求：

1. 不涉及处理跨境支付业务的，不应向境外提供个人信息等数据；
2. 出境数据应仅限为处理跨境支付业务所需的必要信息；
3. 应建立数据出境记录，包括但不限于出境时间、数据类型、数量、目的地、境外接收方等，相关记录至少保存五年；
4. 需按照国家互联网信息办公室《数据出境安全评估办法》要求开展数据出境风险自评估及数据出境安全评估申报。

参考文献

[1] 《非银行支付机构网络支付业务管理办法》（中国人民银行令〔2020〕第2号）

[2] 《数据出境安全评估办法》（国家互联网信息办公室令第11号）

