ICS 点击此处添加 ICS 号
点击此处添加中国标准文献分类号

中华人民共和国国家标准

GB/T XXXXX—XXXX

电子商务平台数据开放 总体要求

Data Open for E-Commerce platform：General Requirement

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目 次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由，由全国电子业务标准化技术委员会（SAC/TC 83）提出并归口。

本标准的主要起草单位：阿里巴巴（中国）有限公司、中国标准化研究院。

本标准的主要起草人：

电子商务平台数据开放 总体要求

1 范围

本标准规定了电子商务数据开放模型及数据的开放原则，并从数据生命周期的维度针对数据开放平台及第三方软件系统提出了总体的技术层面和管理层面要求。

本标准适用于电子商务活动中的电子商务平台服务商和第三方软件提供商，用于指导其进行相关系统的研发、部署和运维。

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，仅所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 18811 电子商务基本术语

GB/T 25069-2010 信息安全技术 术语

3 术语和定义

3.1

电子商务 E-commerce

以电子形式进行的商务活动。它在供应商、消费者、政府机构和其他业务伙伴之间通过任一电子方式实现标准化的非结构化或结构化的业务信息的共享，以管理和执行商业、行政和消费活动中的交易。

3.2

用户 user

使用电子商务交易平台的机构或自然人，以注册的 ID 与用户信息为判断依据。

3.3

商户 merchants

租用电子商务平台进行经营活动的法人、法人委派的行为主体、其它组织机构或自然人。

3.4

网络交易 network transaction

发生在企业（或其他组织机构）之间、企业（或其他组织机构）与消费者之间、消费者之间通过网络手段缔结的商品或服务交易。

3.5

加密 encipherment/encryption

对数据进行密码变换以产生密文的过程。一般包含一个变换集合，该变换使用一套算法和一套输入参量。输入参量通常被称为密钥。

3.6

安全事件 security event

电子商务安全事件，不仅包括网络上出现的攻击造成的安全事件，也包括电子商务业务应用中出现的欺诈、盗号、违禁等恶意行为。

3.7

安全级别 security level

有关敏感信息访问的级别划分，以此级别加之安全范畴能更精细地控制对数据的访问。[GB/T 25069]

3.8

安全分级 security classification

根据业务信息和系统服务的重要性和受损影响，确定实施某种程度的保护，并对该保护程度给以命名。依据访问数据或信息需求，而确定的特定保护程度，同时赋予相应的保护等级。例：“绝密”、“机密”、“秘密”。[GB/T 25069]

3.9

订单 order

消费者向单一商户同一时间拍下单款或多款商品或服务的合约

3.10

第三方软件 the third party software

在本规范中，第三方软件特指商户采购或使用的，非电子商务平台服务商提供的软件和服务，主要用于辅助电子商务的开展，如订单管理及营销推广等。

3.11

回滚 rollback

程序或数据处理错误，将程序或数据恢复到上一次正确状态的行为。回滚包括程序回滚和数据回滚等类型。

3.12

业务 business

在本规范中，特指电子商务活动中所所需处理的各种事务

3.13

用户数据 user data

用户数据是指用户的基本信息和用户提供给电子商务平台或第三方软件使用的数据，如：例如个人信息（姓名、生日、出生地、信用卡号、身份证号等）、商品详情、交易评价等用户输入数据。

3.14

业务数据 business data

业务数据是指业务开展所需要的数据，例如用户的行为数据、根据用户数据和用户行为数据加工获得的数据。

3.15

脱敏 desensitization

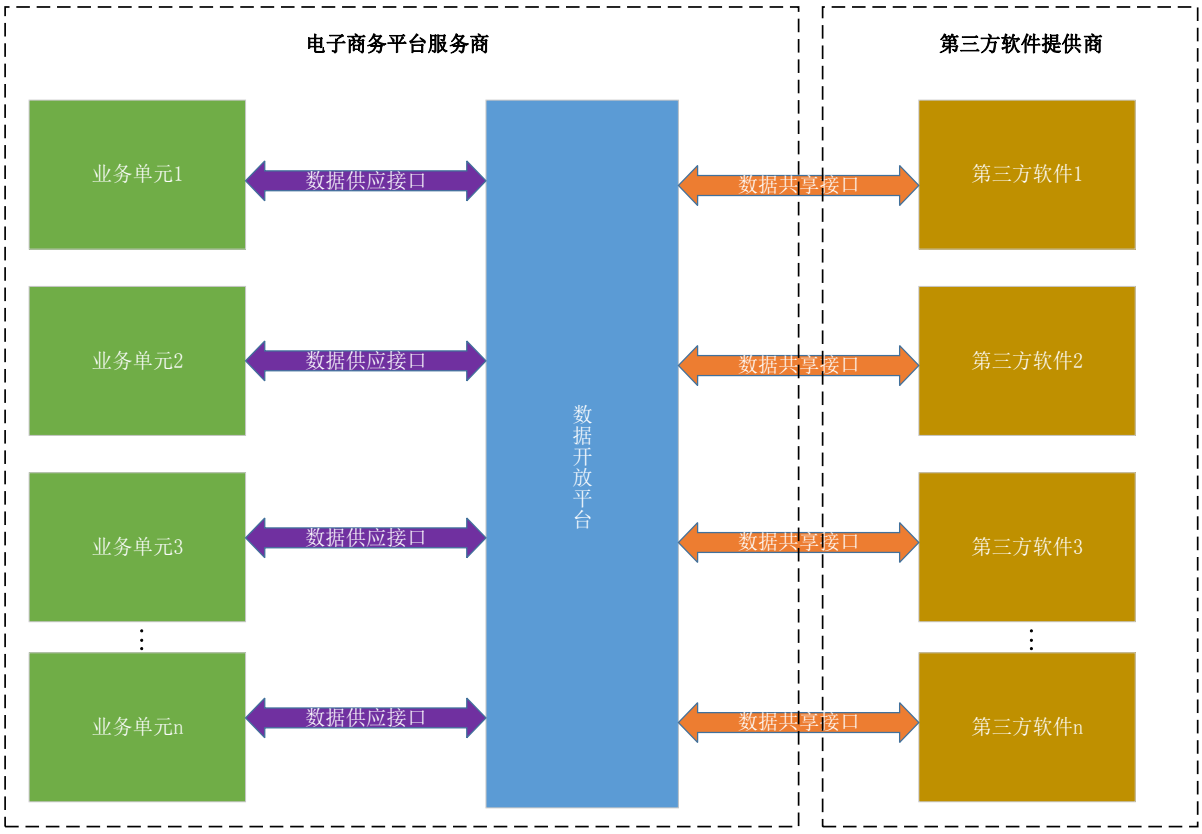
通过模糊化等方法处理原始数据，以实现屏蔽敏感数据且屏蔽后的数据不可逆向恢复的数据保护方式。

4 电子商务数据开放模型

4.1 模型框架

在本规范中，电子商务数据开放涉及电子商务平台服务商及第三方软件提供商，涵盖业务单元、数据开放平台、第三方软件以及数据供应和数据共享两类接口。电子商务的数据开放模型见图1所示。

图1 电子商务数据开放模型



4.2 角色与职责

4.2.1 电子商务平台服务商

电子商务平台服务商负责搭建与运营电子商务业务单元及电子商务数据开放平台，实施对电子商务业务数据的生命周期管理，保证数据的真实性、保密性、完整性、可用性及可追溯性。

电子商务平台服务商的职责应包括但不限于：

a) 审核第三方软件提供商的企业资质，管理接入的第三方软件提供商；
b) 根据 5.2 章的原则，划分数据的安全等级，并基于数据安全等级实施相应的保护；
c) 确定数据开放的粒度和范围，管理数据开放的权限，控制数据访问的风险；
d) 跟踪数据流向，确保数据访问的可追溯。

4.2.2 第三方软件提供商

第三方软件提供商研发和运营第三方软件，负责管理从数据开放平台获取的授权数据，并防止数据泄露。第三方软件提供商的职责应包括但不限于：

a) 第三方软件提供商需向电子商务平台服务商提交应用审核申请，申请内容包括公司资质、应用功能、希望访问的数据级别等，便于平台服务商确定应用的合法性和相应的权限。
b) 第三方软件提供商从数据开放平台访问用户数据前需明确获得用户的授权。
c) 第三方软件提供商应通过运营和技术手段防止用户数据泄露。

4.3 模块与接口

4.3.1 业务单元

业务单元是用户在电子商务平台上进行特定电子商务活动的系统单元，记录并存储与电子商务活动相关的数据，并为数据定义开放的策略，如数据分级。

4.3.2 数据开放平台

数据开放平台是由电子商务平台服务商建设并运营的平台系统，是第三方软件访问业务单元的入口，并集中管理数据的访问权限。

其与业务单元间通过数据供应接口通信，向第三方软件开放数据。

4.3.3 第三方软件

第三方软件是基于数据开放平台开发的软件或服务，向用户提供电子商务的辅助服务，如增强消费者的购物体验，或者协助商家进行店铺管理、营销推广、数据分析等服务。

4.3.4 数据供应接口

数据供应接口是业务单元与数据开放平台之间的通信接口，用于电子商务活动相关数据在平台与业务单元之间的双向交互。

4.3.5 数据共享接口

数据开放平台通过数据共享接口对第三方软件提供经用户授权的电子商务活动数据；第三方软件通过数据共享接口向数据开放平台传递应用产生的数据，如物流状态数据。

5 数据开放原则

5.1 全生命周期管理原则

电子商务平台服务商和第三方软件提供商应对数据全生命周期管理和监控，涵盖数据产生、数据存储、数据使用、数据共享和数据销毁等各个环节。

5.2 数据分级原则

业务单元应根据数据类型、数据保密性要求、数据访问授权的对象不同，对数据的安全级别进行划分，实施不同的开放共享策略。数据参照表 1 可划分为以下 4 个等级：

表1 数据分级

级别 / 项目	一级	二级	三级	四级
类型	可公开数据	可共享的用户数据及业务单元内部数据	用户隐私数据及业务保密数据	机密数据
开放程度	公开	授权公开	需脱敏	禁止

5.2.1 一级数据

指可公开的数据，包括：

a) 用户可公开数据：即对所有人可见的用户信息。例如卖家的商品信息、店铺基本信息、客服联系方式等。

b) 业务可公开数据：可以被公共访问和对外发布的数据，并且公开数据可以自由散布而不会产生任何安全或法律问题。例如卖家的层级、活动招商规则、前台类目数据。

5.2.2 二级数据

指包含有经数据所有者授权方可共享的数据，二级数据主要包括两类：

a) 用户可共享数据：任何其所有者已经授权可对指定人群公开的数据。例如只对家庭成员可见的相册，只对朋友可用的博客。

b) 业务内部数据：仅限组织内部人员访问的与电子商务业务运营相关的数据（如成交总额），如果泄露，可能会对局部业务产生负面影响，或对商家和用户造成较低程度的损失或影响。

5.2.3 三级数据

指包含有用户隐私或业务敏感信息的数据，在相关数据开放前需要做对应的模糊化处理，避免泄露用户隐私或业务秘密。包括：

a) 用户隐私数据：任何只对用户本人可用的或者关于用户本人的信息，该类信息属于用户未在网站上直接公开的自然、资质和行为信息。该类信息的泄露会给用户带来骚扰，影响用户的正常生活、工作等影响，一般可细分为以下两类:

1) 个体属性隐私数据: 可定位到个体身份的数据，如:地址、电话、电子邮箱、身份证号码等

2) 个体行为隐私数据: 可以追溯并锁定个人与电子商务业务关联产生的行为隐私数据(如购买行为、浏览行为、收藏行为和聊天行为等等)。如:购买纪录、收货人详细信息和聊天记录等。

b) 业务保密数据：仅限组织内部特定人群访问，如果非授权的泄露将直接或间接对电子商务平台用户或者员工造成不利影响。造成经济损失、商业损失，破坏电子商务平台的声誉，并可能发生潜在的法律责任。例如类目的各种交易明细/排名，类目产品的业务数据，后台类目、物流数据、类目财务数据。

5.2.4 四级数据

四级数据是指包含用户或业务机密信息的数据，此类数据一旦泄露可能对用户及服务商权益造成严重不利影响的数据。此类数据包括：

a) 用户机密数据：用户进行商务交易的身份凭证及认证凭据类数据，包括密码，信用卡号码，银行帐号，密码提示问题及答案，身份证等。

b) 业务机密数据：非授权的泄露会对电子商务平台服务商或第三方软件提供商造成严重影响。

6 对电子商务平台服务商的要求

6.1 技术要求

6.1.1 数据产生

6.1.1.1 授权许可

业务单元在记录用户录入的数据时必须获得用户明确的授权许可。

第三方软件通过数据开放平台获取用户数据时，必须向平台提供用户的授权凭证。

6.1.1.2 数据分级

业务单元在处理电子商务活动，记录并生成相关数据时，应基于数据分级开放准则为所有数据标识级别。

电子商务数据开放平台仅向第三方软件提供一级、二级和三级的数据。

6.1.2 数据存储

6.1.2.1 数据加密

对于三级及四级数据，业务单元或数据开放平台宜支持加密存储。

6.1.2.2 备份与恢复

业务单元或数据开放平台应对存储其上数据进行备份。备份方式包括本地备份和异地备份，数据开放平台应至少支持其中一种备份方式。

业务单元或数据开放平台应宜支持增量数据备份和数据恢复的功能。

6.1.3 数据使用

6.1.3.1 访问控制

第三方软件通过数据开放平台获取用户数据时，必须向平台提供用户的授权凭证。

数据开放平台在返回数据给第三方软件前，应验证数据调用方的身份，并确保该软件具备对应的数据权限，并获得了用户授权。

数据开放平台应保证不同用户之间的数据相互隔离。

6.1.3.2 回滚

数据开放平台中执行的数据操作应支持操作回滚。

6.1.4 数据共享

6.1.4.1 数据接口权限

数据共享接口应能基于数据的等级对第三方软件的访问执行访问控制。

6.1.4.2 数据脱敏

数据开放平台在向第三方软件传输三级数据时，应对数据进行脱敏处理。

6.1.4.3 数据传输安全

数据开放平台及第三方软件应具备数据传输安全保护能力，保证数据的完整性、机密性、可用性及不可抵赖性。

6.1.4.4 权限管理

数据开放平台需要具备如下能力。

a) 数据开放平台能封闭第三方软件的账号。

b) 数据开放平台应有能力撤销用户对第三方软件的授权。

c) 数据开放平台应定期验证用户身份。

6.1.4.5 数据流向追踪

数据开放平台应具备数据流向查询和流向异常预警的能力。

6.1.5 数据销毁

执行数据计算和存储的设备在弃置、转售或捐赠前需将其上所有数据彻底删除，并无法复原。

6.2 管理要求

6.2.1 系统部署

电子商务平台服务商负责研发和部署数据开放相关的应用和支撑系统时，应保障系统生命周期的安全，实施安全需求分析、安全设计、代码安全审计、安全测试及发布安全审核等活动。

6.2.2 服务运维

电子商务平台服务商运营数据开放服务时，应涵盖以下活动：

a) 漏洞管理：电子商务平台服务商应建立漏洞管理机制，监控系统漏洞及风险，如定期的系统安全扫描；若发现漏洞，应及时处理并修复。

b) 应急响应：电子商务平台服务商应设立应急响应的组织，建立相应的流程和机制，制定应急响应计划，处理安全事件，如数据泄露事件。

c) 事件追查：对于所发生的针对数据开放平台的安全事件，应建立机制保证攻击可溯源。

7 对第三方软件提供商的要求

7.1 技术要求

7.1.1 数据产生

第三方软件需通过数据开放平台的用户授权机制，获取访问用户数据的授权；所获取的用户数据只能返回给授权用户。

第三方软件应保证不同用户的数据的隔离，防止非授权访问。

7.1.2 数据存储

第三方软件获取并保存的三级及四级数据宜支持加密存储。

7.1.3 数据使用

不同安全等级的数据的使用需要在不同等级的运行环境（如表2所示）中进行。

表2 运行环境类别

环境等级	数据等级
一般环境	一级数据
可监视环境	只读的二级数据及三级数据
可控环境	可写的二级数据及三级数据

可监视环境要求：

- 用户对应用数据的所有操作应写入日志，以支持审计和监控。
- 相关软件需通过严格的安全测试，并定期扫描。

可控环境要求：

- 包含所有可监视环境要求；
- 该环境需运行于隔离的网络下，只能通过限定的流通和管理通道与公众网络交互。

7.1.4 数据共享

7.1.4.1 数据返回

第三方软件与数据开放平台间应建立双向通道，第三方软件一方面从数据开放平台获取授权数据，另一方面第三方软件在数据状态发生改变后将更新的数据通过数据共享接口返回给数据开放平台。以订单处理为例，第三方订单管理软件从数据开放平台获取商户的订单数据，当订单状态变更，其应向数据开放平台返回更新的订单状态数据。

7.1.4.2 第三方软件间的数据共享

数据开放平台应向第三方软件提供标准的应用间数据交换服务，第三方软件之间应通过数据开放平台的数据交换服务实现第三方软件间的数据共享。

7.1.4.3 数据流向追踪

第三方软件应记录访问数据的用户端来源、用户信息、时间、数据等信息。

如果第三方软件自动传递数据到其它系统，应记录数据传递的目的地、时间、数据等信息。

第三方软件应返回数据流向信息给数据开放平台。

7.1.5 数据销毁

计算机或设备在弃置、转售或捐赠前必须将其所有数据彻底删除，并无法复原，以免造成信息泄露。

7.2 管理要求

7.2.1 系统部署

第三方软件提供商应保障软件的生命周期安全，开展安全需求分析、安全设计、代码安全审计、安全测试及发布安全审核等活动。

7.2.2 服务运维

第三方软件提供商在通过第三方软件向商户提供服务时，应涵盖以下活动：

a) 漏洞管理：应建立漏洞管理机制，监控第三方软件及系统的漏洞和风险，如定期的系统安全扫描；若发现漏洞，应及时处理并修复。
b) 应急响应：第三方软件提供商应设立应急响应组织，建立相应的流程和机制，应对可能发生的安全事件，如数据泄露事件，避免安全影响的进一步扩散。
c) 事件追查：对于已爆发的针对应用的的安全事件，应建立机制保证对攻击溯源。