ICS 03.160
CCS L 70

DB4403

深　　圳　　市　　地　　方　　标　　准

DB4403/T 564—2024

数据交易合规评估规范

Data transactions compliance assessment specification

2024-12-20 发布　　2025-01-01 实施

深圳市市场监督管理局　　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。

本文件由深圳市政务服务和数据管理局、深圳市司法局提出并归口。

本文件起草单位：深圳数据交易所有限公司、深圳市福田区司法局、中国电子技术标准化研究院、公安部第三研究所、深圳市北鹏前沿科技法律研究院、深圳市标准技术研究院、中兴通讯股份有限公司、蚂蚁区块链科技（上海）有限公司、华为云计算技术有限公司、深圳市腾讯计算机系统有限公司、普华永道管理咨询（上海）有限公司深圳分公司、荣耀终端有限公司、深圳华大基因科技有限公司、中国电子信息产业集团有限公司、比亚迪股份有限公司、阿里云计算有限公司、华润数科控股有限公司、天职国际会计师事务所（特殊普通合伙）、奇安信科技集团股份有限公司、OPPO广东移动通信有限公司、深圳市蓝海法律查明和商事调解中心、安永（中国）企业咨询有限公司、北京小米移动软件有限公司。

本文件主要起草人：王青兰、张平、张颖、王艺、陈一芊、胡婧卓、胡敏喆、南红玉、龙军、余灏、李兰兰、谭丽、肖声高、王显军、刘山泉、代旻、廖灏璘、李红光、古亮、张文娟、赵阳、王冠、赵亮、王腾。

引　言

数据要素市场化改革是深化改革开放中所面临的重点。随着数据要素市场化改革序幕的开启，各类数据交易逐渐浮出水面，数据交易合规难点也日渐凸显，如场外黑灰产盛行难以监管、数据交易合规具体规则缺失、数据交易合规人才稀缺导致入场成本高、数据权益保护与利用的两难等。

本文件针对数据交易主体、标的与流通过程中面临的合规要点，根据《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律法规，分别从合法、安全、诚信、权益保障四个维度辅助数据交易主体、第三方法律服务机构开展合规评估工作，旨在为数据交易活动提供一套较为全面的合规评估方法与标准，同时赋能数据交易主体参照合规标准，安全、合规、高效地开发和利用数据资源。对文件中的具体事项，法律法规等另有规定的，需遵照其规定执行。

数据交易合规评估规范

1 范围

本文件规定了数据交易合规评估的评估原则、评估框架、评估等级、主体合规评估要求、标的合规评估要求、流通合规评估要求以及评估过程要求。

本文件适用于主管部门和监督管理部门、交易主体、第三方法律服务机构、数据交易场所等数据交易相关方管理和实施的数据交易合规评估活动。

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—2019 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 33770.6—2021 信息技术服务 外包 第6部分：服务需求方通用要求

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 35295 信息技术 大数据 术语

GB/T 41479—2022 信息安全技术 网络数据处理安全要求

GB/T 43697—2024 数据安全技术 数据分类分级规则

DB4403/T 271—2022 公共数据安全要求

DB4403/T 439—2024 公共数据安全评估方法

3 术语和定义

GB/T 25069、GB/T 35295界定的以及下列术语和定义适用于本文件。

3.1

数据 data

任何以电子或其他方式对信息的记录。

注：数据在不同视角下表现为原始数据、衍生数据、数据资源、数据产品、数据资产、数据要素等形式。

3.2

个人信息 personal information

以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息。

[来源：中华人民共和国个人信息保护法，第4条]

注1：个人信息包括姓名、出生日期、身份证件号码、个人生物识别信息、住址、通信通讯联系方式、通信记录和内容、账号密码、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、个人上网记录（操作点击记录、浏览记录、收藏记录）、设备信息等，不包括匿名化处理后的信息。

注2：关于个人信息的判定方法、相关术语、子分类，参见GB/T 35273—2020附录A。

注3：个人信息处理者通过个人信息或其他信息加工处理后形成的信息，例如，用户画像或特征标签，能够单独或者与其他信息结合识别特定自然人身份或者反映自然人活动情况的，属于个人信息。

3.3

敏感个人信息 sensitive personal information

一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息。

注：包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

3.4

重要数据 important data

特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。

3.5

公共数据 public data

各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。

3.6

数据产品 data product

用于交易的加工处理后的数据衍生产品。

注：广义的数据产品是指基于数据加工形成的，可满足特定需求的数据加工品和数据服务。本文件中的数据产品是指狭义的数据产品。

3.7

第三方法律服务机构 third-party legal service provider

辅助数据交易活动有序开展，依法取得执业许可，为数据交易合规评估提供法律服务的法人或非法人组织。

3.8

交易主体 subject of transaction

数据交易活动中的数据卖方、数据买方和数据商。

注：数据卖方是指出售交易标的的法人或非法人组织。数据买方是指购买交易标的的法人或非法人组织。数据商是指从各种合法来源收集或维护数据，经汇总、加工、分析等处理转化为交易标的，向买方出售或许可；或为促成并顺利履行交易，向委托人提供交易标的发布、承销等服务，合规开展业务的企业法人。

3.9

数据主体 subject of data

个人信息所标识或关联的自然人、在生产经营活动中采集加工企业数据的各类市场主体，以及在依法履职或提供公共服务过程中产生、处理公共数据的各级党政机关、企事业单位。

3.10

交易标的 object of transaction

数据卖方或数据商与数据买方交易的对象。

注1：交易标的包括数据产品、数据服务、数据工具等。

注2：数据服务是指数据卖方或数据商提供数据处理（收集、存储、使用、加工、传输等）的服务。

注3：数据工具是指可实现数据服务的软硬件工具。

3.11

数据交易 data transaction

数据卖方和买方之间进行的，以数据或者数据各类形态为标的的交易行为。

3.12

数据交易场所 data transactions venue

按照相关法律法规和数据交易监督管理部门的规定等，为数据集中交易提供基础设施和基本服务的机构。

4 评估原则

4.1 合法原则

数据交易合规评估依法合规开展，维护国家安全、公共利益，保护组织和个人的合法权益。若法律法规对数据交易合规评估另有规定的，从其规定。

4.2 客观公正原则

数据交易合规评估真实和准确地反映数据交易活动现状，不带评估人员个人偏见，以确保评估意见仅建立在评估证据的基础上。

4.3 保密原则

评估人员审慎使用和保护在评估过程获得的信息。

4.4 安全防护原则

交易主体采取数据安全保护、检测和响应等措施，防止数据丢失损毁、泄露和篡改，确保数据安全。

5 评估框架

根据相关法律法规等规定，结合数据交易过程，数据交易合规评估首先针对交易主体的相关情况进行评估（见第7章），再针对交易标的的相关情况进行评估（见第8章），最后针对交易主体之间的交易标的流通相关情况进行评估（见第9章）。每个环节均会从合法、安全、诚信、权益保障四个维度进行评估，评估过程包括评估准备、评估实施、评估报告三个阶段（见第10章），评估框架见图1。

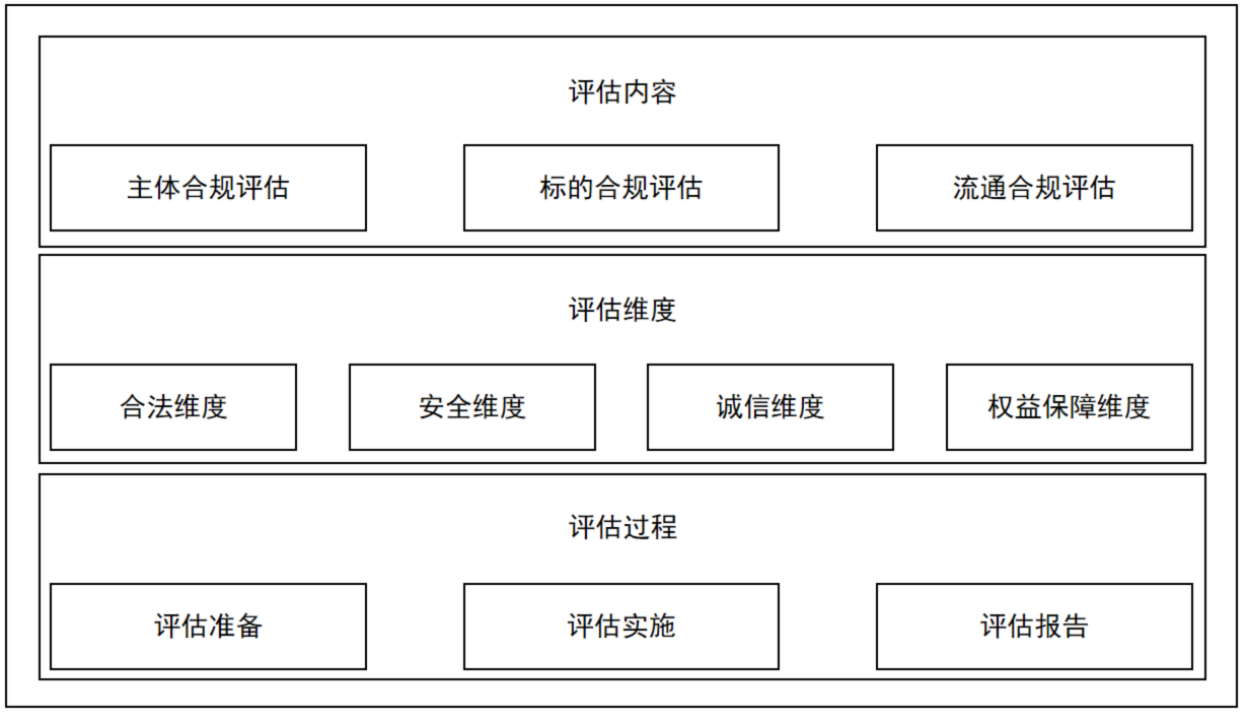

图1　数据交易合规评估参考框架图

6　评估等级

6.1　通则

6.1.1　数据交易合规评估涵盖数据交易的主体、标的和流通三个环节，每个环节均应满足合法、安全、诚信、权益保障四个维度的要求。合法维度不划分等级，为必选要求。其他维度根据对数据交易评估要素要求的叠加，依次递增并划分为A级、AA级、AAA级三个等级。

6.1.2　经合规评估，四个维度中有任一维度未达到A级要求的，评估结果为“不符合数据交易合规要求”。

6.2　第一级：A级

数据交易的主体、标的、流通三个环节在合法、安全、诚信、权益保障四个维度上均满足适用的法律法规等规定和强制性国家标准的要求。

6.3　第二级：AA级

数据交易的主体、标的、流通三个环节在合法、安全、诚信、权益保障四个维度上满足“A级”的全部要求，并满足适用的推荐性国家标准的要求。

6.4　第三级：AAA级

数据交易的主体、标的、流通三个环节在合法、安全、诚信、权益保障四个维度上满足“AA级”的全部要求，且额外采取了可以明显提升数据交易合规程度的措施。

7　主体合规评估

7.1 合法维度评估

7.1.1 交易主体应依法成立、有效存续并合法经营，满足以下要求：

a) 交易主体依法取得的营业执照或相关登记证书应合法有效，非中国大陆企业应提供同等类型合法证照；

b) 交易主体的经营业务若属于法律、行政法规规定须经批准或获取特定行业资质的项目，应依法经过批准或获取特定行业资质，且在有效期内；

c) 若在数据交易场所开展交易，数据卖方应通过数据交易场所认证为数据商，或通过已认证数据商保荐，方可在数据交易场所开展数据交易。

7.1.2 评估交易主体在合法维度所需的相关文件资料，可见附录 A。

7.2 安全维度评估

7.2.1 通则

7.2.1.1 交易主体应至少满足A级要求。

7.2.1.2 交易主体在满足A级要求的基础上，可以自主选择按照AA级、AAA级评估等级进行合规评估。交易主体选择AA级评估等级的，应同时满足A级和AA级标准要求；选择AAA级评估等级的，应同时满足A级、AA级和AAA级标准要求。各评估等级对应的安全要求见表1。

7.2.1.3 若数据商仅提供交易标的发布、承销等服务，不参与交易标的处理或交付环节的，可以不进行安全维度评估。

7.2.1.4 评估交易主体在安全维度所需的相关文件资料，可见附录A。

表 1 主体安全合规义务清单

级别	安全要求
A 级	A 级标准要求（第 7.2.2）
AA 级	A 级标准要求（第 7.2.2）、AA 级标准要求（第 7.2.3）
AAA 级	A 级标准要求（第 7.2.2）、AA 级标准要求（第 7.2.3）、AAA 级标准要求（第 7.2.4）

7.2.2 A 级标准

交易主体满足以下要求：

a) 交易主体应制定数据安全工作的总体方针，阐明组织数据安全工作的目标、范围、原则和安全框架等相关内容；

b) 交易主体应制定主要数据处理活动的安全管理制度；

注：主要数据处理活动是指主营业务涉及的数据处理活动，处理员工个人信息不属于此范围。

c) 交易主体应对数据管理人员或操作人员执行的日常工作建立操作规程；

d) 交易主体应按照国家和行业有关要求及 GB/T 43697—2024 第 7 章的数据分类分级流程对本单位的数据进行数据分类分级管理，识别可能涉及的个人信息、公共数据和重要数据等不同类型的数据；

e) 交易主体应明确对信息技术外包和数据处理供应商的监督管理要求；

f) 交易主体应制定安全应急预案，发生数据安全事件时，应立即采取处置措施，按照法律法规等规定的要求，及时告知相关方（例如数据主体）并向有关主管部门、监管部门、公安机关、国家安全机关报告、报案，在事件处置完毕后向有关主管部门、监管部门提交事件调查评估报告，配合开展侦查、调查和处置工作；
g) 交易主体应加强风险监测，发现数据安全缺陷、漏洞等风险时，应及时采取补救措施；
h) 交易主体应在管理及技术方面具有与当前业务及数据处理活动相适应的数据安全保障能力；
i) 需开展个人信息保护合规审计的交易主体应按照法律法规等规定的要求定期开展合规审计；
j) 交易主体应开展日常数据安全检查，主要内容包括数据平台运行情况、数据库漏洞、数据安全审计日志等；
k) 交易主体应采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；
l) 交易主体属于重要数据处理者的，应按照法律法规等规定的要求开展数据安全风险评估，并向省级以上有关主管部门报送风险评估报告；
m) 交易主体属于重要数据处理者或处理个人信息达到国家网信部门规定数量的，已设立数据安全管理部门、个人信息合规管理部门，明确重要数据安全负责人、个人信息保护负责人及其职责；
n) 交易主体应定期开展员工数据安全教育培训；
o) 需开展个人信息保护合规审计的交易主体应制定个人信息保护合规审计制度，每年开展一次合规审计，并且审计结果为无高危风险；
p) 交易主体应遵守国家和行业数据分类分级保护要求，进行数据分类分级，结合数据流通范围、影响程度、潜在风险，对不同级别的数据采用不同级别的授权使用和保护机制；
q) 交易主体应根据数据资产的重要程度对识别出的重要数据进行标识管理，根据法律法规实施必要的安全管理策略和保障措施。

7.2.3 AA 级标准

交易主体在满足 A 级标准的基础上，还满足以下要求：

a) 交易主体应设立数据安全管理部门、个人信息合规管理部门，明确重要数据安全负责人、个人信息保护负责人及其职责；
b) 交易主体应根据数据分类分级识别情况编制数据资产清单；
c) 交易主体应满足 GB/T 33770.6—2021 第 6 章的要求，实施信息技术外包和数据处理供应商的管理；
d) 交易主体应建立数据销毁安全管理制度，明确销毁对象和流程、不同类别和级别数据的销毁方式和销毁要求等，严格按照该管理制度执行且有相应的记录进行佐证；
e) 交易主体应制定数据供应链安全管理规范，明确数据供应链安全目标、原则和范围、数据供应商选择和管理等要求；
f) 交易主体若涉及重要数据处理的，应制定重要数据安全风险评估制度，每年至少开展一次重要数据安全评估，并且评估结果为无高危风险；
g) 交易主体若涉及重要数据处理的，应对重要数据的批量查询、批量修改、批量导出等高风险操作建立多层级的审批程序；
h) 交易主体若涉及重要数据处理的，应制定重要数据清单管理程序，规定清单的编制、审核、维护、更新等要求；
i) 交易主体若涉及重要数据处理的应对数据安全关键岗位人员录用或上岗前进行安全背景审查，审查通过方可录用和任职。

7.2.4 AAA 级标准

交易主体在满足 A 级、AA 级标准的基础上，还满足以下要求：

a) 交易主体应遵守国家和行业数据分类分级保护要求，能通过自动化手段识别出结构化的个人信息、公共数据、重要数据等不同类型的数据；
b) 交易主体应制定数据安全管理制度，制度应覆盖数据处理活动全生命周期，并分发至相关部门和人员；
c) 交易主体应制定数据安全风险评估制度，每年至少开展一次数据安全评估，按规定提交年度评估报告，报告内容包含风险处置的方式等，并且评估结果为无高危风险；
d) 交易主体的数据存储介质设备在报废或重用前，应确保设备已经完成完全清除或被安全覆盖，保证该设备上的敏感个人信息、商业秘密、重要数据等数据和授权软件无法被恢复重用。
e) 交易主体的数据安全关键事务处理岗位离职前，交易主体应对该员工在职期间的数据处理活动进行内部审计；
f) 交易主体应制定数据接口的全生命周期管理制度，对使用数据接口的申请、审批、开放、变更、注销等全生命周期进行管控和定期审计；
g) 交易主体应具备以技术手段对数据泄露源头进行定位的能力；
h) 交易主体应定期对相关供应链上下游数据处理活动安全风险和数据安全管理能力进行评估，并留存评估过程和评估结果材料；
i) 交易主体涉及数据处理平台处理数据的，应对重要数据使用或加工制定审批程序，对可能改变用途、范围的使用和加工等处理活动进行评估和审批；
j) 交易主体应根据相关标准识别重要数据，并对识别出的重要数据进行数据标记；
k) 交易主体应采取重复清除与覆盖，以及消磁、粉碎等相结合的数据销毁方法，防止被重标识、重关联或非授权使用和泄露等；
l) 交易主体应监测、分析、预测数据安全整体态势，实现对数据安全威胁的发现识别、理解分析和响应处置。

7.3 诚信维度评估

7.3.1 通则

7.3.1.1 交易主体应提交真实、准确的材料，确保相关情况的真实可信，如实披露其近三年网络安全、数据安全、个人信息保护相关的刑事处罚、行政处罚、被诉和被仲裁案件。

7.3.1.2 评估交易主体在诚信维度所需的相关文件资料，可见附录 A。

7.3.2 A 级标准

交易主体满足以下要求：

a) 若在数据交易场所开展交易，交易主体应根据数据交易场所的要求提交主体身份材料，并通过数据交易场所的审核登记；
b) 若在数据交易场所开展交易，数据商应根据数据交易场所的要求提交数据商主体准入材料和适格的数据交易承诺函，并通过数据交易场所的审核认证；
c) 交易主体不应存在与网络安全、数据安全、个人信息保护等方面相关的未整改完毕的重大刑事处罚、重大行政处罚案件；

注：重大案件的判断维度包括涉案金额、案件情节、影响范围、裁判结果、案件社会知名度和影响力（如属于最高法指导案例或各级法院发布的典型案例）等。

d) 若在数据交易场所开展交易，交易主体不应存在违反数据交易相关书面承诺或数据交易场所业务规则的情形。

7.3.3 AA 级标准

交易主体在满足A级标准的基础上，还满足以下要求：

a) 交易主体近三年不应存在网络安全、数据安全、个人信息保护相关的行政处罚、刑事处罚、已决的不利被诉或被仲裁案件；

注：关于“不利”的标准，从综合案件对交易主体市场声誉、商业活动的正常进行等维度进行判断。

b) 交易主体应具备数据交易经验，包括但不限于在数据交易场所或场外开展过数据交易活动。

7.3.4 AAA 级标准

交易主体在满足 AA 级标准的基础上，还应满足近五年不存在网络安全、数据安全、个人信息保护相关的行政处罚、刑事处罚、已决的不利被诉或被仲裁案件的要求。

7.4 权益保障维度评估

7.4.1 通则

7.4.1.1 交易主体应完善自身权益保障机制，同时保障数据主体及合作方的权益。

注：合作方是指交易主体在数据交易活动中任何与数据处理相关的合作方，包括数据来源方、数据处理受托方等。

7.4.1.2 评估交易主体在权益维度所需的相关文件资料，可见附录A。

7.4.2 A 级标准

交易主体满足以下要求：

a) 交易主体应建立数据主体权益保障机制，包括权利告知、权利请求响应和处理等；

b) 交易主体应与合作方在合作协议中就数据处理行为约定权益保障义务和责任。

7.4.3 AA 级标准

交易主体在满足A级标准的基础上，还应遵守与合作方签订的合作协议约定的内容，包括数据处理的授权范围以及其他约定，与合作方不存在数据相关的未决争议。

7.4.4 AAA 级标准

交易主体在满足 AA 级标准的基础上，还满足以下要求：

a) 交易标的涉及个人信息的，交易主体应通过建立隐私管理平台等形式，具备自动化响应个人信息主体权利请求的能力；

b) 交易主体应依照有关国家标准的要求，建立相应的规范或管理体系，并获得认证；

c) 交易主体应定期对合作方的数据安全保护能力、资质进行核验，了解其经营范围、资质证照、数据安全技术能力和管理能力、过往遵守相关法律法规等规定的情况、合作方所在国家/地区对数据安全的相关规定等，并留存对合作方资质审核的资料。

8 标的合规评估

8.1 合法维度评估

8.1.1 通则

8.1.1.1 交易标的来源、数据处理过程、内容应合法合规，不应存在违反法律法规等强制性规定、危害国家安全、公共安全、第三方合法权益、违反社会公序良俗的情形。

8.1.1.2 评估标的合规合法维度所需的相关文件资料，可见附录A。

8.1.2 来源合法

8.1.2.1 通用要求

交易标的来源满足以下要求：

a) 交易标的应具有真实合法的来源；

b) 交易标的为数据卖方自行生产的数据的，应在合法经营活动中产生，且能够证明数据具有独立来源，不存在侵犯第三方合法权益的情形，若无法证明的，应能够提交数据具有独立来源的书面承诺；

注：数据的独立来源是指，数据从数据卖方自身的经营、科研、生产等活动或设备、资产中产生，不涉及未经授权或许可的任何第三方的数据、资产或数据处理活动。

c) 交易标的为从公开渠道获取的数据的，应能够证明获取方式与过程的合法性；

d) 交易标的为从第三方采购或获得第三方授权运营的数据的，应能够证明采购或授权的合法性、真实性、完整性和有效性；

e) 交易标的获取过程、手段不应存在违反法律法规等强制性规定或者危害国家安全、公共安全或侵犯第三方合法权益的情形，且不应含有以欺诈、诱骗、误导等方式或从非法、违规渠道获取的数据。

8.1.2.2 公共数据

交易标的形成涉及对公共数据处理的，在满足通用要求的基础上，还满足以下要求：

a) 如公共数据为交易主体履行职责过程中自行制作、获取的，交易主体应取得内部的审批同意；

b) 如公共数据为交易主体经过授权运营、共享等方式获得的，交易主体应通过公共数据授权协议、其他形式取得有关主管部门的有效授权，或满足法律法规的相关要求；

c) 如公共数据为交易主体经过开放渠道获得的，交易主体应采用合法、正当的方式收集。

8.1.2.3 个人信息

交易标的形成涉及对个人信息进行处理的，在满足通用要求的基础上，还满足以下要求：

a) 交易主体处理个人信息行为应符合合法、正当、必要与诚信等原则的要求；

b) 交易主体处理个人信息前已取得个人信息主体授权同意或具有其他处理个人信息的合法性基础，处理不满十四周岁未成年人的个人信息，应取得其监护人的同意；

c) 交易主体已依照相关法律法规等规定的要求向个人信息主体公示个人信息处理规则，涉及不满十四周岁未成年人个人信息的，应制定专门的个人信息处理规则；

d) 符合法律法规等规定应进行个人信息保护影响评估情形的，交易主体应进行个人信息保护影响评估并留存评估报告至少三年；

e) 交易主体已按照法律法规等规定和本文件的要求，采取个人信息安全保护措施。

8.1.2.4 重要数据

交易标的涉及对重要数据进行处理的，在满足通用要求的基础上，还满足以下要求：

a) 如重要数据为交易主体自行产生的，交易主体应取得内部的审批同意或有关主管部门的审批同意；

b) 如重要数据是从第三方采购或获得第三方授权运营的数据的，交易主体应与数据提供方或授

权方通过签署相关协议、承诺书等方式，确保数据来源合法并明确双方法律责任。

8.1.3 处理合法

8.1.3.1 通用要求

数据处理满足以下通用要求：

a) 数据处理行为不存在违反法律法规等强制性规定，危害国家利益、社会公共利益或侵害第三方合法权益的情形；
b) 数据提供方或授权方对数据处理做出限制的，交易标的涉及的数据处理不应超出提供方或授权方对授权期限、类型范围、处理方式、目的等的限制，并履行法律法规等规定的数据处理强制性义务，遵循数据处理的合规要求。

8.1.3.2 公共数据

公共数据处理在满足通用要求的基础上，还满足以下要求：

a) 交易主体处理公共数据应遵守社会公序良俗，不违反社会公德；
b) 交易主体处理公共数据应遵循公共数据开发利用相关法律法规等规定、公共数据授权协议对公共数据处理的限制；
c) 交易主体为国家机关、关键信息基础设施运营者提供服务，或者参与其他公共基础设施、公共服务系统建设、运行、维护的，对公共数据的访问、获取、留存、使用、向他人提供或进行关联分析，应取得委托方同意。

8.1.3.3 个人信息

个人信息处理在满足通用要求的基础上，还满足以下要求：

a) 交易主体涉及处理个人信息的，应遵循合法、正当、必要和诚信原则，并具有明确合理的目的，采取对个人权益影响最小的方式，不应通过误导、欺诈、胁迫等方式处理个人信息；
b) 交易主体涉及处理个人信息的，应公开个人信息处理规则，明示处理的目的、方式和范围，保障个人信息质量，并采取必要措施保障个人信息安全；
c) 交易主体处理个人信息应取得个人信息主体的同意或具有其他处理个人信息的合法性基础；
d) 交易主体保存个人信息期限应为实现处理目的所必要的最短时间，在个人信息处理完毕或丧失合法性基础、处理必要性时依法删除、销毁个人数据，但法律法规等另有规定的除外；
e) 交易主体委托处理个人信息的，应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等，并对受托人的个人信息处理活动进行监督；
f) 交易主体处理不满十四周岁未成年人个人信息的，应取得未成年人的父母或者其他监护人的同意，并制定专门的个人信息处理规则；
g) 交易标的涉及处理敏感个人信息、利用个人信息进行自动化决策、委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息、向境外提供个人信息或其他对个人权益有重大影响的个人信息处理活动的，交易主体应开展个人信息保护影响评估并履行相应的合规义务。

8.1.3.4 重要数据

重要数据处理在满足通用要求的基础上，还满足以下要求：

a) 交易标的涉及对重要数据进行加工处理的，在根据法律法规等规定的要求进行数据安全风险评估的过程中，应对重要数据加工处理或流转的情况进行评估，并在向主管部门报送的数据

安全风险评估报告中予以体现；

b) 交易主体涉及处理工业和信息化领域重要数据的，应将本单位重要数据目录向本地区行业监管部门备案，备案内容发生重大变化的，应在发生变化的三个月内履行变更备案手续，备案内容包括但不限于数据来源、类别、级别、规模、载体、处理目的和方式、使用范围、责任主体、对外共享、跨境传输、安全保护措施等基本情况；

c) 交易主体涉及销毁工业和信息化领域重要数据的，不应以任何理由、任何方式对销毁数据进行恢复，引起备案内容发生变化的，应履行备案变更手续。

8.1.4 内容合法

交易标的满足以下要求：

a) 交易标的不应包含法律法规等规定禁止采集的数据类型；

注：如征信机构禁止采集个人宗教信仰、基因、指纹、血型、疾病和病史信息以及法律、行政法规禁止采集的其他个人信息。

b) 交易标的如涉及法律法规等规定限制采集、附条件处理的数据类型，应符合相应条件；

c) 交易标的不应存在危害国家安全、公共利益，侵犯第三方合法权益的内容，包括：

1) 交易标的不应存在危害国家利益、公共利益的可能性；

2) 交易标的不应存在违反与第三方的合作协议、侵犯第三方知识产权、商业秘密、隐私权等合法权益的可能性；

3) 交易标的不应存在对个人信息或商业秘密进行逆向识别的可能性。

c) 交易标的不应包含以欺诈、诱骗、误导等方式或从非法、违规渠道获取的数据；

d) 交易标的不应包含违法和不良信息的内容。

8.2 安全维度评估

8.2.1 通则

8.2.1.1 交易主体应根据交易标的所涉及的数据类型和重要程度采取不同级别的安全管理和技术措施，保障交易标的安全。

8.2.1.2 在评估包含重要数据的交易标的是否满足 AA 级标准的要求时，考察该交易标的是否同时满足 A 级标准中的通用要求和该标准下重要数据所列举的全部要求，以及 AA 级标准中的通用要求和该标准下重要数据所列举的全部要求。

8.2.1.3 评估标的安全维度所需的相关文件资料，可见附录 A。

8.2.2 A 级标准

8.2.2.1 通用要求

交易标的满足以下通用要求：

a) 交易标的所在的存储区域与其他区域之间应采取可靠的技术隔离手段；

b) 对访问交易标的进行身份标识和鉴别，身份鉴别信息具有复杂度要求并定期更换；

c) 存储交易标的应使用适当的技术保护措施，保证交易标的在存储过程中的完整性、保密性；

d) 交易标的涉及数据处理平台处理数据的，数据处理平台应按照等级保护的相关要求符合 GB/T 22239—2019 对应的系统级别；

e) 数据处理平台涉及算法模型的，应按照对应等级的保护要求部署管理措施和技术措施，如使用的算法模型根据法律法规等规定的要求需要进行备案的，应根据要求进行备案；

f) 应定期对访问交易标的的账号进行识别、梳理及分类，防止非法账号、闲置账号、过期账号

的存在；

g） 已按照法律法规等规定和本文件的明确要求，对交易标的采取安全保护措施。

8.2.2.2 公共数据

涉及公共数据的交易标的，在满足通用要求的基础上，还满足以下要求：

a） 应按照DB4403/T 439—2024的公共数据安全评估方法进行评估，且评估结果满足DB4403/T 271—2022中基本安全要求的规定；

b） 应满足GB/T 22239—2019中第二级要求关于数据完整性、数据保密性、数据备份恢复的内容。

8.2.2.3 个人信息

涉及个人信息的交易标的，在满足通用要求的基础上，还满足以下要求：

a） 应把个人生物识别信息与个人身份识别信息分开存储，并有单独的访问控制措施；

b） 应对交易标的的访问进行身份验证，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；

c） 除非取得个人信息主体同意，原则上宜采用去标识化等技术手段，对涉及的个人信息进行去标识化处理后再进行交易，且去标识化的效果宜满足GB/T 42460—2023中第2级的要求；

d） 数据卖方应在涉及个人信息的数据交易前，对涉及个人信息的交易活动开展个人信息保护影响评估，并采取相应措施控制个人信息泄露风险，并且评估结果为无高危风险；

e） 数据卖方涉及个人信息的数据交易的，应按照个人信息保护审计相关法律法规等规定的要求定期对个人信息合规进行审计。

8.2.2.4 重要数据

涉及重要数据的交易标的，在满足通用要求的基础上，还满足以下要求：

a） 如涉及脱敏后的重要数据交易，数据卖方应评价重要数据脱敏有效性，评估脱敏后的风险为无高危风险；

b） 涉及处理重要数据的，应满足国家相关法律法规等规定对重要数据处理的要求。

8.2.3 AA级标准

8.2.3.1 通用要求

交易标的在满足通用级标准的基础上，还应满足GB/T 22239—2019中第三级要求关于数据完整性、数据保密性、数据备份恢复、剩余信息保护的相关内容。

8.2.3.2 公共数据

在满足AA级标准通用要求和公共数据通用级标准的基础上，交易标的原则上宜满足DB4403/T 271—2022中规定的三级增强安全要求。

8.2.3.3 个人信息

在满足AA级标准通用要求和个人信息通用级标准的基础上，还满足以下要求：

a） 原则上宜采用去标识化等技术手段，对涉及的个人信息进行去标识化处理后再进行交易，并且去标识化的效果宜满足GB/T 42460—2023中第3级的要求；

b） 数据卖方应在涉及个人信息的数据交易前，对涉及个人信息的交易活动开展个人信息保护影

响评估，并采取相应措施控制个人信息泄露风险，并且评估结果为无中高危风险；

c) 数据卖方涉及个人信息的数据交易，应定期对个人信息合规进行审计，并且审计结果为无中高危风险；

d) 按照“原始数据不出域、数据可用不可见”的原则，交易标的应采用隐私计算方式进行个人信息加工处理。

8.2.3.4 重要数据

在满足AA级标准通用要求和重要数据通用级标准的基础上，还满足以下要求：

a) 涉及数据处理平台处理数据的，应采用密码技术保证从外部数据源导入重要数据存储的完整性、保密性，其中使用的密码技术，应符合国家密码管理主管部门的要求；

b) 如涉及脱敏后的重要数据交易，数据卖方应评价重要数据脱敏有效性，评估脱敏后的风险，结果为无中高危风险；

c) 涉及数据处理平台处理数据的，应采用隐私计算技术进行数据处理，防止原始重要数据泄露的风险。

8.2.4 AAA 级标准

8.2.4.1 通用要求

在满足AA级标准的基础上，交易标的还应满足GB/T 22239—2019中第四级要求中数据完整性、数据保密性、数据备份恢复、剩余信息保护的相关要求。

8.2.4.2 公共数据

在满足AAA级标准通用要求和公共数据AA级标准的基础上，交易标的原则上宜满足DB4403/T 271—2022中规定的四级增强安全要求。

8.2.4.3 个人信息

在满足AAA级标准通用要求和个人信息AA级标准的基础上，还满足以下要求：

a) 原则上宜采用去标识化等技术手段，对涉及的个人信息进行去标识化处理后再进行交易，并且去标识化的效果宜满足 GB/T 42460—2023 中 4 级不包含任何标识符的要求；

b) 交易标的为个人信息匿名化处理后数据的，应按照相关规定、标准的要求达到匿名化的效果，并确保数据交易相关方在合法合规的情形下，不借助额外信息无法识别特定自然人；

c) 按照“原始数据不出域、数据可用不可见”的要求，交易标的如采用隐私计算方式进行个人信息加工处理的情况，隐私计算平台应通过权威机构的安全检测，并获得相关证书。

8.2.4.4 重要数据

在满足AAA级标准通用要求和重要数据AA级标准的基础上，还满足以下要求：

a) 交易标的的存储应使用加密算法，保证交易标的在存储过程中的完整性、保密性，其中使用的密码技术，应符合国家密码管理主管部门的要求；

b) 如涉及脱敏后的重要数据交易，数据卖方应评价重要数据脱敏有效性，评估脱敏后的风险，并且能评估重要数据重关联或非授权使用和泄露等风险，应能防止数据交易相关方重标识重要数据；

c) 涉及数据处理平台处理数据的，如果采用了隐私计算技术进行数据处理，则隐私计算平台应通过权威机构的安全检测，并获得相关证书；

d) 数据交易相关方应保证存有重要数据的存储空间在被释放或重新分配前得到完全清除。

8.3 诚信维度评估

8.3.1 通则

8.3.1.1 交易标的的相关说明应真实、准确，相关情况真实可信。

8.3.1.2 评估交易标的诚信维度所需的相关文件资料，可见附录 A。

8.3.2 A 级标准

交易标的满足以下要求：

a) 交易主体提交的交易标的相关登记材料真实、准确、完整，数据卖方应依据实际情况披露交易标的的描述说明、适用范围、更新频率、计费方式等信息，并向数据交易场所提供产品或服务样例；

b) 交易标的相关说明文档、材料应内容完整、规范，并且与交易标的实际情况相一致；

c) 交易主体应向数据交易场所提交与数据交易相关的书面承诺；

注：例如，数据交易承诺函、同类数据产品上市承诺函、无重大风险变化承诺函等。

d) 交易标的不应存在违反与数据交易相关书面承诺或数据交易场所业务规则的情况；

e) 交易主体近三年不应存在因交易标的不符合网络安全、数据安全、个人信息保护等方面法律法规等规定的要求而被刑事处罚、行政处罚，且仍未整改完毕的情形。

8.3.3 AA 级标准

交易标的在满足A级标准的基础上，还满足以下要求：

a) 交易标的应具备在数据交易场所的交易记录，且不应存在违反数据交易场所业务规则的情形；

b) 交易主体近三年不应存在因交易标的不符合网络安全、数据安全、个人信息保护等方面法律法规等规定的要求而被刑事处罚、行政处罚的情形、已决的不利重大被诉或被仲裁案件。

8.3.4 AAA 级标准

交易标的在满足AA级标准的基础上，还满足以下要求：

a) 交易主体持有的其他与交易标的属于同类或类似数据产品应具备在数据交易场所的交易记录，且不应存在违反数据交易场所业务规则的情形；

b) 交易主体近五年不应存在因交易标的或同类、类似数据产品不符合网络安全、数据安全、个人信息保护等方面法律法规等规定的要求而被刑事处罚、行政处罚的情形、已决的不利重大被诉或被仲裁案件。

8.4 权益保障维度评估

8.4.1 通则

8.4.1.1 交易标的应具备权益保障机制。

8.4.1.2 评估交易标的在权益维度所需的相关文件资料，可见附录 A。

8.4.2 A 级标准

交易标的满足以下要求：

a) 交易标的涉及知识产权的，应具备数据相关知识产权的权利证明文件或存在知识产权相关协议，不存在侵犯第三方知识产权等合法权利、权益的情形；

b) 交易标的涉及处理个人信息且具有相应告知条件的，应以清晰显著方式告知相关主体权益并

设置便捷的权益主张渠道，包括权益告知、权益请求响应、权益异常处理等机制，以清晰方式公布数据主体主张权利路径及交易主体的联系方式等；

c) 交易标的涉及处理不满十四周岁未成年人个人信息且具有相应告知条件的，应依法公示未成年人个人信息保护规则，并提供适合未成年人使用条件与状况的服务版本。

8.4.3 AA 级标准

交易标的在满足A级标准的基础上，还满足以下要求：

a) 交易标的涉及个人信息且具有相应条件的，交易主体应就交易标的设置响应个人信息主体权益请求机制，并应满足 GB/T 35273—2020 第 8.7 条的要求；

b) 交易主体具有相应条件的应就交易标的设置投诉管理机制，明确处理流程、时限和反馈机制等内容，并对用户的投诉及时做出回应。

8.4.4 AAA 级标准

交易标的在满足AA级标准的基础上，已获得数据产权登记机构颁发的数据产权登记证书。

9 流通合规评估

9.1 合法维度评估

9.1.1 流通对象

数据交易流通对象满足以下要求：

a) 数据买方应满足本文件第 7 章的合法维度相关要求；

b) 数据买方应提供所属行业、数据需求内容、数据用途等信息，以确保采购需求真实、合法、合理，与其所在行业、业务需求相符；

c) 交易主体应在流通前取得相关主体对数据流通及数据使用的授权；

注：例如，涉及个人信息的，已取得个人关于数据流通、流通后数据使用的合法有效授权；例如涉及公共数据的，已取得相关主体对数据流通和数据使用的授权。

d) 数据买方应按照交易申报的使用目的、场景和方式，并按照买卖双方约定和数据授权使用的目的、范围以及限制，合法合规地使用数据。

9.1.2 流通内容

交易标的应具有可交易性，不应具有以下情形：

a) 流通可能危害国家安全、公共利益；

b) 流通可能侵犯第三方的合法权益；

c) 交易标的流通时含有未依法获得授权的个人信息或有不借助其他数据的情况下可以识别特定自然人的数据；

d) 交易标的流通时含有未依法公开、开放的公共数据；

e) 法律法规等规定禁止交易的其他情形。

9.1.3 流通程序

数据交易流通程序满足以下要求：

a) 数据交易涉及许可、备案等行政手续的，交易主体应向有关部门申请许可、履行备案或办理其他行政手续；

注：例如，涉及工业和信息化领域重要数据流通的，向相关监管部门履行备案手续。涉及出口管制物项及物项相关技术资料出境的，向国家出口管制管理部门申请许可。

b） 数据交易涉及数据出境的，交易主体应根据适用的法律法规等规定履行数据出境相关义务。

9.2 安全维度评估

9.2.1 通则

9.2.1.1 交易主体应根据数据交易标的类型和重要程度采取不同级别的安全管理措施和安全技术措施。相同级别标准的合规要求应首先满足本级别中通用要求的标准，再满足对应数据类型的合规要求。相同数据类型的合规要求应首先满足上一级别标准的同类型数据合规要求，再满足本级别标准的合规要求。

9.2.1.2 在评估包含重要数据的交易标的流通过程是否满足 AA 级标准的要求时，考察该交易标的同时满足 A 级标准中的通用要求和该标准下重要数据所列举的全部要求，以及 AA 级标准中的通用要求和该标准下重要数据所列举的全部要求。

9.2.1.3 评估流通合规在安全维度所需的相关文件资料，可见附录 A。

9.2.2 A 级标准

9.2.2.1 通用要求

交易流通满足以下通用要求：

a） 交易主体应开展数据交易安全风险评估，评估内容包含在数据交易过程中数据被篡改、破坏、泄露、丢失或者被非法获取、非法利用的风险，以及对国家安全、公共利益带来的风险，评估结果应为无高危风险；

b） 交易流通影响或者可能影响国家安全的，应当按照国家有关规定进行国家安全审查；

c） 应在数据交易流通前对交易主体进行身份验证，保证交易主体身份真实性；

d） 交易主体应采用安全的数据传输通道，采取加密、签名、防重放等措施，确保数据在传输过程中的保密性、完整性、不可否认性；

e） 交易数据交付完成后，数据卖方应立即关闭数据访问渠道；

f） 在数据交易结束后，交易主体应保存交易商品和服务信息、交易信息等，包括但不限于交易唯一标识、交易标的信息、交易时间、数据卖方、数据买方、交易结果等相关信息不少于三年，并确保信息的完整性、保密性、可用性。法律、行政法规另有规定的，依照其规定；

g） 交易主体应能配合监管部门调查访问交易日志、重要数据交易服务合约等相关过程文档资料，支持监管部门开展数据交易服务的安全审计工作；

h） 交易主体应对交付数据内容进行监测和核验，如发现异常情况，及时中断数据交易行为，并按照相关应急预案及时处理。发现违法违规事件，应及时上报相关主管部门、监督管理部门，并保留好相关日志证据。

9.2.2.2 公共数据

涉及公共数据流通的，在满足通用要求的基础上，交易主体还应在交易流通前进行身份验证，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

9.2.2.3 个人信息

涉及个人信息流通的，在满足通用要求的基础上，还满足以下要求：

a) 交易主体应在数据交易前，对涉及个人信息的交易活动开展个人信息保护影响评估，并采取相应措施控制个人信息泄露风险，并且评估结果为无高危风险；
b) 交易主体应在交易流通前进行身份验证，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
c) 交易主体应保存个人信息交易活动情况记录至少三年。

9.2.2.4 重要数据

涉及重要数据流通的，在满足通用要求的基础上，还满足以下要求：
a) 交易主体的数据安全负责人应对风险评估结果进行审核，确保数据可交易，并将评估结果和审批记录留存三年以上；
b) 交易主体应在交易流通前进行身份验证，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现；
c) 交易主体应对数据交易的全过程进行审计，并采用标记、数字水印、区块链等技术，确保数据交付过程所记录信息具有不可篡改性，并对相关方数据交易过程的审计进程进行保护、防止未授权的中断，具备对数据交易过程可追溯的能力；
d) 交易主体应在数据传输链路上部署交易数据监控工具，发现异常情况应能及时告警；
e) 交易主体应保存重要数据交易活动情况记录至少三年。

9.2.3 AA 级标准

9.2.3.1 通用要求

在满足 A 级标准要求的基础上，交易主体应在交易流通前进行身份验证，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现。

9.2.3.2 公共数据

在满足AA级标准通用要求和公共数据A级标准的基础上，交易主体应开展数据交易安全风险评估，评估内容包含在数据交易过程中数据被篡改、破坏、泄露、丢失或者被非法获取、非法利用的风险，以及对国家安全、公共利益带来的风险，评估结果为无中高危风险。

9.2.3.3 个人信息

在满足AA级标准通用要求和个人信息A级标准的基础上，还满足以下要求：
a) 数据卖方应在涉及个人信息的数据交易前，对涉及个人信息的交易活动开展个人信息保护影响评估，并采取相应措施控制个人信息泄露风险，并且评估结果为无中高危风险；
b) 原则上宜按照“原始数据不出域、数据可用不可见”的要求进行交易，如采用隐私计算等方式。

9.2.3.4 重要数据

在满足AA级标准通用要求和重要数据A级标准的基础上，还满足以下要求：
a) 交易主体应开展数据交易安全风险评估，评估内容包含在数据交易过程中数据被篡改、破坏、泄露、丢失或者被非法获取、非法利用的风险，以及对国家安全、公共利益带来的风险，评估结果为无中高危风险；

b) 交易主体应在数据传输链路上部署交易数据监控工具，具有完备的数据保护机制和数据泄露检测能力，发现被盗用、滥用等恶意行为应能及时阻断并告警。

9.2.4 AAA 级标准

9.2.4.1 通用要求

在满足AA级标准通用要求的基础上，交易主体应采用安全的数据传输通道，采取加密、签名、防重放等措施，确保数据在传输过程中的保密性、完整性、不可否认性。其中使用的密码技术，应符合国家密码管理主管部门的要求。

9.2.4.2 公共数据

公共数据无AAA级标准下的特别要求。

9.2.4.3 个人信息

在满足AAA级标准通用要求和个人信息AA级标准的基础上，如交易标的属于采用去标识化处理后的数据，还应评估交易后的个人信息被重标识的风险，即数据买方在合法合规的情形下，采购去标识化处理后的数据再融合买方其他数据无法重识别出个人信息主体。

9.2.4.4 重要数据

在满足AAA级标准通用要求和重要数据AA级标准的基础上，还满足以下要求：

a) 交易主体应在交易流通前采用双向认证方式验证交易相关方的身份，验证方式应采用口令、密码技术、生物技术等两种或两种以上组合的鉴别技术对双方进行身份鉴别，且其中一种鉴别技术至少应使用密码技术来实现，从而管控数据交易过程，防止数据被未授权访问和使用；
b) 在交易结束后，各交易主体应清除相关数据的缓存，并对清除记录及数据清除措施的有效性进行检查。

9.3 诚信维度评估

9.3.1 A 级标准

交易主体满足以下要求：

a) 数据交易活动真实开展，交易主体间已签署交易合同，交易合同约定内容应与数据交易的背景、目的情况说明等标的说明及标的内容一致；
b) 若在数据交易场所开展交易，交易主体应向数据交易场所提供标的交付验收清单、支付凭证、发票等交易过程资料，以证明数据交易真实发生；
c) 交易主体开展交易还应满足该主体内部相关审批、授权或采购程序要求；

注：例如，数据买方如使用本市财政资金进行采购，按照有关规定公开合同签订时间、合同价款、项目概况、违约责任等合同基本信息，但涉及国家秘密、商业秘密的除外。

d) 交易主体属于大型网络平台服务提供者的，应当每年度发布个人信息保护社会责任报告。

9.3.2 AA 级标准

若在数据交易场所开展交易，交易主体在满足A级标准的基础上，还应向数据交易场所提供完备的数据流通相关的记录、资料。

注：包括但不限于个人信息保护影响评估报告、流通日志记录、审计报告。

9.3.3 AAA 级标准

交易主体在满足AA级标准的基础上，还满足以下要求：

a) 若在数据交易场所开展交易，交易主体应向数据交易场所提供交易标的历史交易合同、发票、交易标的价值评估报告等资料，以证明交易标的定价的公允性；
b) 交易主体在交易标的交付环节不应存在任何质量、数量或其他合同方面的争议纠纷。

9.4 权益保障维度评估

9.4.1 A 级标准

交易主体满足以下要求：

a) 涉及个人信息的流通的，交易主体应依法保障个人信息主体的知情权，向个人信息主体告知行使个人信息权利的方式和程序；
b) 交易活动应获得交易主体必要的内部授权，不侵犯或违反对第三人的法定或约定义务；
c) 建立便捷的安全投诉、举报渠道，公布投诉、举报方式等信息；
d) 若在数据交易场所开展数据交易，相关合同应具备包含数据描述、数据用途、数据质量、交易方式、交易金额、数据使用期限、安全责任、交易时间、保密义务等条款。

9.4.2 AA 级标准

交易主体在满足A级标准的基础上，还满足以下要求：

a) 交易主体应满足 GB/T 41479—2022 第 5.11 条的要求，向个人信息主体告知申诉、投诉、举报途径和响应时限承诺；
b) 交易主体应进一步详细约定各方数据安全保护责任和义务，违反法律法规等规定和合同约定处理数据的补救措施、数据使用期限届满时的数据处理方式、接受监督的承诺和方式等条款。

9.4.3 AAA 级标准

交易主体在满足AA级标准的基础上，还满足以下要求：

a) 数据卖方建立了针对数据买方的监督审核机制，以确保数据买方按照交易合同约定的目的、范围及期限使用交易标的；
b) 若在数据交易场所开展交易，交易合同约定同意通过数据交易所争端解决机制维护双方合法权益。

10 评估过程要求

10.1 评估准备

评估准备工作包括：

a) 团队组建：交易主体或其委托的第三方法律服务机构按照不同的数据交易需求，组建包含评估组长、管理评估员、技术评估员、质量控制员等角色的评估团队；
b) 方案制定：评估团队按照不同的数据交易需求，制定评估方案和评估计划；
c) 文档收集：评估团队按照本文件第 7、8、9 章的要求进行文档收集，并做好文档分类及内容标记；
d) 申请确认：交易主体对拟进行数据交易的申请文档进行确认，保证文档的完整性、正确性、一致性等符合相关法律要求。

10.2 评估实施

评估实施工作包括：

a) 主体合规评估：评估团队依据本文件第 7 章的要求对主体合规进行评估，并记录评估结果和评估问题；
b) 标的合规评估：评估团队依据本文件第 8 章的要求对标的合规进行评估，并记录评估结果和评估问题；
c) 流通合规评估：评估团队依据本文件第 9 章的要求对流通合规进行评估，并记录评估结果和评估问题；
d) 评估问题反馈：评估团队对评估过程中发现的问题进行汇总分析并反馈给交易主体；
e) 问题整改确认：交易主体对问题进行整改后，评估团队对问题整改情况进行确认并将确认结果反馈给交易主体；
f) 评估结论出具：评估团队根据整改确认后的情况，尽职审慎对主体、标的、流通的合规性出具正式的法律意见，明确评估等级，是否可安全交易、在特定条件下可交易或不予交易的结论，并提示交易的安全合规风险。

注：对安全合规评估的部分，委托第三方技术评估机构进行评估出具评估意见，供交易主体或其委托的第三方法律服务机构援引。

10.3 评估报告

评估报告包括：

a) 评估报告的编制：评估团队整理评估过程记录、评估底稿文件及评估结果，并基于前述材料编制评估报告；
b) 评估报告的出具：评估团队签署评估报告并发送至交易主体；
c) 评估材料的归档：评估团队及交易主体分别对评估活动的全部材料进行归档，如通过数据交易场所进行交易，数据交易场所应同步归档。

附 录 A
（资料性）
数据交易合规评估建议文档

A.1 主体合规评估建议文档

主体合规评估的建议文档见表A.1。

表 A.1 主体合规评估建议文档

评估维度	建议文档
合法维度	a)主体营业信息，包括主体名称、性质、注册资金、营业范围及统一社会信用代码； b)主体经营相关的资质证书及行政许可证书、执照，包括合法有效的经营执照，交易主体所获得的与数据合规/数据交易相关的行业认证、数据安全能力认证、备案证明、证书等材料（例如数据安全管理能力认证、数据安全能力成熟度认证、合规管理体系认证等）。
安全维度	a)数据安全管理体系文档，包含数据安全总体方针、策略、程序文件、管理制度、相关记录表单等，如数据安全管理制度、数据安全关键岗位组织架构图、招聘流程、负责人背景资料、数据操作人员招聘流程、日常管理操作规程、数据安全事件应急响应制度、数据销毁安全管理制度、个人信息合规审计制度、个人信息合规审计报告、重要数据安全风险评估报告等； b)数据分类分级管理制度文件、数据资产清单，清单的编制、审核、维护、更新的记录等； c)对相关供应链上下游数据处理活动供应链服务商的数据安全风险评估报告及评估过程和评估结果材料； d)数据合规监测预警平台材料、数据资产地图等平台工具； e)支撑数据基本安全保护措施，如网络、系统、终端、数据库及数据库或平台组件、云平台（若有）安全管理策略、程序文件。
诚信维度	a)承诺函，如不存在违法标的承诺、无违法违规承诺函、不存在舆情事件承诺函等； b)近三年相关的行政处罚、被诉和被仲裁案件的信息等（如有）； c)同时参考其他维度提供的信息。
权益维度	a)数据主体权利的告知（例如个人信息保护政策/隐私政策、隐私通知的相关章节等）； b)数据主体权利请求响应流程、管理政策或相关内部发文（如有）； c)数据主体权利请求处理和响应表单、记录（示例，如有）； d)与合作方的合作协议、数据过程记录； e)第三方管理机制，包括对数据交易领域内的第三方合作方管理的文件及机制说明，对第三方管理审查的记录等； f)数据相关的知识产权权属证明、数据相关的知识产权约定的协议（如有）。

A.2 标的合规评估建议文档

标的合规评估建议文档见表 A.2。

表A.2 标的合规评估建议文档

评估维度	建议文档
合法维度	a)交易标的类信息，包括交易标的形态、技术方案、操作指引及限制约束等信息； b)数据类信息，包括数据敏感程度、数据主体类型、数据分级分类及风险分析、数据所属行业、数据表结构与定义及元数据、数据规模及条目等信息； c)数据来源证明文件，包括第三方处采购或获取运营授权数据的采购协议、授权文本、合法意见，数据具有独立来源，数据来源合法书面承诺等； d)数据处理相关证明文件，包括个人信息保护影响评估报告、数据存储制度、数据出境情况、数据出境安全评估通知书、个人信息出境备案证明文件、第三方法律服务机构出具的法律意见书等； e)数据内容相关文本，包括数据卖方内容合法承诺、第三方法律服务机构出具的法律意见等。
安全维度	a)数据安全传输、存储的安全技术措施介绍； b)公共数据安全要求检测认证报告； c)算法模型的备案证明、算法模型的保护措施； d)隐私计算平台安全保护措施、隐私计算平台安全合规认证证书； e)相关安全认证，如等保测评报告、密评报告、个人信息保护影响评估报告、数据安全风险评估报告、个人信息合规审计报告、ISO认证材料等； f)数据处理活动（包括：数据收集、数据存储、数据传输、数据使用和加工、数据提供、数据公开、数据删除）的技术实现方案及安全防护方案； g)数据脱敏管理制度、数据脱敏审计记录、数据重识别风险评估报告； h)渗透测试、漏洞扫描报告； i)支撑数据基本安全保护措施，如网络、系统、终端、数据库及数据库或平台组件、云平台（若有）安全管理策略、程序文件。
诚信维度	承诺函，如不存在违法标的承诺、无违法违规承诺函、不存在舆情事件承诺函等。
权益维度	a)数据主体权利保障相关文本，如个人信息保护政策/隐私政策、隐私通知、个人权益保障机制、违法不良信息举报机制文本等； b)数据主体权利请求响应流程、管理政策或相关内部发文（如有）； c)数据主体权利请求处理和响应表单、记录（如有）； d)与合作方的合作协议、数据处理过程记录； e)第三方管理机制，包括对数据交易领域内的第三方合作方管理的文件及机制说明，对第三方管理审查的记录等； f)数据相关的知识产权权属证明、数据相关的知识产权约定的协议（如有）。

A.3 流通合规评估建议文档

流通合规评估建议文档见表 A.3。

表 A.3 流通合规评估建议文档

评估维度	建议文档
合法维度	a)交易标的描述说明文档，宜包括如下信息： 1)流通形态描述，包括线上/线下/托管交付的方式描述及具体交付逻辑等； 2)流通场景描述，包括流通目的、流通场景、是否涉及跨境等； 3)流通性质描述，包括出售、授权许可或其他等； 4)流通限制描述，包括使用目的限制、使用期限限制、使用地域限制、转让限制信息等； 5)流通内容描述，包括数据规模、数据范围、数据种类、数据精度、敏感程度（是否属于重要数据、敏感个人信息）、更新频率、涉及的数据主体等； 6)流通费用描述，包括计费方式、标准、税率等。 b)交易标的流通合同文本； c)交易标的流通及使用的授权证明材料，涉及个人信息的，提供数据标的流通已取得个人合法有效授权的证明，如授权同意书、签署（同意）记录、签署（同意）流程、电子签名、时间戳（日志）记录等；已对个人信息进行匿名化处理的，应提供匿名化处理的证明文件，如处理后台截图、日志等；涉及公共数据的，提供授权流通的证明文件； d)提供用于交易标的流通的资质、行政许可、备案证明文件。
安全维度	a)数据交易安全风险评估、个人信息保护影响评估报告、数据安全风险评估报告、去标识化评价报告； b)数据传输通道保密性、完整性、不可否认性技术防护措施； c)数据交易日志及保存日志证明材料等； d)数据交易审计记录、隐私计算方式说明材料、隐私计算方式安全认证证书材料； e)数据监控工具介绍材料、数据监控审计日志记录； f)数据清除技术措施介绍、数据清除日志记录。
诚信维度	a)承诺函； b)交易标的说明文本； c)交易标的流通合同文本； d)交易标的交付验收清单、支付凭证、发票等流通交付过程资料； e)交易标的流通相关记录、资料，例如个人信息保护影响评估报告、流通日志记录、审计报告； f)交易标的历史交易合同、发票、交易标的价值评估报告。
权益维度	a)数据主体权利的告知，如个人信息保护政策/隐私政策、隐私通知的相关章节、界面截图等； b)数据主体权利请求响应方式、流程、管理政策； c)交易标的流通合同文本，如数据处理协议、个人信息出境标准合同。

参 考 文 献

[1] GB/T 22239—2019 信息安全技术 网络安全等级保护基本要求
[2] GB/T 33770.6—2021 信息技术服务 外包 第6部分：服务需求方通用要求
[3] GB/T 35273—2020 信息安全技术 个人信息安全规范
[4] GB/T 35295—2017 信息技术 大数据 术语
[5] GB/T 37932—2019 信息安全技术 数据交易服务安全要求
[6] GB/T 39204—2022 信息安全技术 关键信息基础设施安全保护要求
[7] GB/T 39335—2020 信息安全技术 个人信息安全影响评估指南
[8] GB/T 41479—2022 信息安全技术 网络数据处理安全要求
[9] GB/T 42460—2023 信息安全技术 个人信息去标识化效果评估指南
[10] GB/T 43697—2024 数据安全技术 数据分类分级规则
[11] DB4403/T 271—2022 公共数据安全要求
[12] DB4403/T 439—2024 公共数据安全评估方法
[13] 中华人民共和国民法典.第十三届全国人民代表大会第三次会议通过.2020年5月28日
[14] 中华人民共和国网络安全法.第十二届全国人民代表大会常务委员会第二十四次会议通过.2016年11月7日
[15] 中华人民共和国出口管制法.中华人民共和国第十三届全国人民代表大会常务委员会第二十二次会议通过.2020年10月17日
[16] 中华人民共和国数据安全法.第十三届全国人民代表大会常务委员会第二十九次会议通过.2021年6月10日
[17] 中华人民共和国个人信息保护法.第十三届全国人民代表大会常务委员会第三十次会议通过.2021年8月20日
[18] 中华人民共和国公司法.第十四届全国人民代表大会常务委员会第七次会议第二次修订.2023年12月29日
[19] 中华人民共和国保守国家秘密法.第十四届全国人民代表大会常务委员会第八次会议第二次修订.2024年2月27日
[20] 征信业管理条例.国务院令第631号.2013年1月21日
[21] 网络数据安全管理条例.国务院令第790号.2024年9月24日
[22] 网络信息内容生态治理规定.国家互联网信息办公室令第5号.2019年12月15日
[23] 广东省公共数据管理办法.粤府令第290号.2021年10月18日
[24] 数据出境安全评估办法.国家互联网信息办公室令第11号.2022年7月7日
[25] 个人信息出境标准合同办法.国家互联网信息办公室令第13号.2023年2月22日
[26] 促进和规范数据跨境流动规定.国家互联网信息办公室令第16号.2024年3月22日
[27] 深圳经济特区数据条例.深圳市第七届人民代表大会常务委员会第二次会议通过.2021年6月29日
[28] 国家统计局.关于印发《统计上大中小微型企业划分办法（2017）》的通知：国统字〔2017〕213号
[29] 工业和信息化部.关于印发《工业和信息化领域数据安全管理办法（试行）》的通知：工信部网安〔2022〕166号.2022年12月8日

［30］ 深圳市发展和改革委员会.关于印发《深圳市数据交易管理暂行办法》的通知：深发改规〔2023〕3号.2023年2月21日

［31］ 深圳市发展和改革委员会.关于印发《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》的通知：深发改规〔2023〕4号.2023年2月24日