跨境数据交易合规评估指引

Guidelines for Compliance Assessment of Cross-border Data Transactions

免责声明

重要提示：本文件仅为一般性信息指南，不构成任何法律或其他专业意见。

本《跨境数据交易合规评估指引》（以下简称“本文件”）由深圳数据交易所牵头，与起草单位、起草人共同编写，旨在为跨境数据交易相关方提供一套具有可操作性的评估标准。

本文件的内容基于截至 2026 年 2 月 9 日所掌握的公开信息和对相关法律法规的理解。本文件的编写方和撰稿人已努力确保本文件所载信息的准确性、完整性和及时性。然而，数据隐私和合规领域的法律法规复杂多变，且可能存在解释上的差异。因此，本文件可能无法涵盖所有相关细节，也无法及时反映所有最新的法律发展、监管要求或实践变化等。

本文件不构成、亦不应被视为任何形式的法律、会计、投资或其他专业意见。本文件中的信息不能取代针对特定情况的专业税务、会计、法律或其他相关专业意见。在做出任何与数据合规相关的具体决策或采取任何相关行动之前，读者应当咨询具备相关资质的专业顾问，并向其提供与特定情况相关的所有事实。社会主体在具体业务中应以法律法规和国家监管部门的正式规定为准。

本文件的编写方和撰稿人对本文件所含信息的完整性、准确性或及时性不作任何明示或暗示的保证，包括但不限于对本文件的功能、适销性和特定用途适用性的保证。对于本文件中的任何错误和疏漏，以及任何人因信赖本文件之全部或任一部分内容而采取或未

采取的任何措施或因此而产生的任何后果，本文件的编写方和撰稿人不承担任何责任。

本文件的使用受以下条款约束:

1.本文件仅供信息参考，不得用于任何商业目的。

2.在引用或传播本文件的任何内容时，请务必注明出处，并明确其公益合作性质。

3.本文件的编写方保留随时修改、更新或撤回本文件的权利，恕不另行通知。

4.通过访问、阅读或使用本文件，即表示您已阅读、理解并同意本免责声明的所有条款。

编委会

指导单位

深圳市互联网信息办公室

深圳市政务服务和数据管理局

主编

王青兰 深圳数据交易所合规部总经理

副主编

陈一芊 深圳数据交易所数据合规经理

王　艺 北京市环球（深圳）律师事务所合伙人

起草单位

深圳数据交易所有限公司、深圳市福田区司法局、深圳市福田区政务服务和数据管理局、公安部第三研究所、深圳市标准技术研究院、中国联合网络通信有限公司智能城市研究院、中兴通讯股份有限公司、深圳市优必选科技股份有限公司、深圳 TCL 新技术有限公司

起草人

王青兰、陈一芊、王艺、张颖、李晓明、胡婧卓、胡敏喆、南红玉、龙军、戴佳兵、刘晋名、姚迁、王鹏、梅傲婷、王永霞、付子牛、钟晓瑜、谭丽

目次

一、 范围 6
二、 规范性引用文件 6
三、 术语和定义 6
四、 跨境数据交易模式 10
五、 评估原则 11
六、 评估框架 11
七、 主体合规评估 12
八、 标的合规评估 19
九、 流通合规评估 27
十、 评估方法 35
附录 A 38
附录 B 43

跨境数据交易合规评估指引

一、范围

本文件规定了跨境数据交易合规评估的评估原则、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方法。

本文件适用于跨境数据交易的交易主体、数据交易机构、数据第三方专业服务机构等跨境数据交易相关方对跨境数据交易进行评估，也适用于主管部门和监督管理部门对跨境数据交易活动进行监督、管理和评估。

二、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 25069—2022　信息安全技术　术语

GB/T 35273—2020　信息安全技术　个人信息安全规范

DB4403/T 564—2024　数据交易合规评估规范

三、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。

（一） 跨境数据 cross-border data

指交易主体将在中国境内运营中收集和产生的数据（以下简称“境内数据”）由中国内地提供至其他国家或者地区，包括由中国内地提供至中国香港特别行政区、中国澳门特别行政区，由中国大陆提供至中国台湾地区，交易主体将在境外运营中收集和产生的数据（以下简称“境外数据”）由境外提供至中国境内。

注：跨境数据主要包括以下几种情形：（1）交易主体直接向境外通过电子、人工转移的方式传输在中国境内运营中收集、产生的数据；（2）境外的机构、组织或者个人可以直接查询、调取、下载、导出存储在境内的数据；（3）以向境内自然人提供产品或者服务为目的或为了分析、评估境内自然人的行为，由境外主体直接收集的中国境内的数据。

（二） 交易主体 subject of the transaction

跨境数据交易活动中的数据卖方、数据买方和数据商。分为中国境内交易主体（以下简称“境内交易主体”）和中国境外交易主体（以下简简称“境外交易主体”）。

注 1：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。

注 2：境内交易主体是指注册于中国境内，并以其名义进行数

据处理，作为数据控制者的法人或非法人组织。

注 3：境外交易主体是指注册于中国境外，并以其名义进行数据处理，作为数据控制者的法人或非法人组织。

（三） 跨境数据交易 cross-border data transaction

指数据卖方或数据商与数据买方以特定形态的跨境数据作为交易标的，在中国境内或境外进行的以货币或其他等价物作为对价的交易行为。

（四） 数据主体 subject of the data

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

（五） 跨境数据产品 cross－border data product

指用于交易的跨境数据的原始数据和数据主体对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值，形成的衍生数据产品。

注：跨境数据产品包括但不限于数据集、数据分析报告、数据可视化产品、数据指数、API 数据、加密数据等。

（六） 交易标的 object of the transaction

数据卖方或数据商与数据买方交易的对象。

注：本文件中交易标的主要是指跨境数据产品。

（七） 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。

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。

（八） 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。

（九） 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。

（十） 公共数据 public data

是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的数据。

（十一） 数据第三方专业服务机构 professional third-party data service provider

是指为促进数据交易活动合规高效开展，提供数据集成、质量评价、数据经纪、合规认证、安全审计、数据公证、数据保险、数据托管、资产评估、争议调解、风险评估、人才培训、咨询服务等第三方服务的专业化组织。

四、跨境数据交易模式

根据跨境数据产品的数据源及交易主体的来源不同，跨境数据交易可以分为以下六种模式：

表 1 跨境数据交易模式

模式	跨境数据产品的数据源	数据卖方 / 数据商	数据买方
I	境内数据	境内交易主体	境外交易主体
II		境外交易主体	境外交易主体
III		境外交易主体	境内交易主体
IV	境外数据	境内交易主体	境外交易主体
V		境外交易主体	境外交易主体
VI		境外交易主体	境内交易主体

注 1：境内数据和境外数据在两个境内主体之间交易，因流通不涉及跨境，不属于本文件定义的跨境数据交易行为。

注 2：本文件的合规评估要求仅适用于表 1 跨境数据交易模式 I、II、III和VI。境内主体将境外数据引入境内数据后再销售给境外主体的，适用本文件的相关规定。模式 IV 和 V 的数据源均为境外数据，不涉及境内数据出境，并且跨境数据产品最终在境外使用或

处理，不适用中国相关法律法规的规定，故二者均不纳入本文件跨境数据交易模式的独立评估范畴。

五、评估原则

（一）合法原则

跨境数据交易合规评估依法合规开展，遵守所有适用的法律法规要求，确保评估人员不违反法律法规。

（二）客观公正原则

跨境数据交易合规评估真实和准确地反映跨境数据交易活动现状，确保评估意见仅建立在评估证据的基础上。

（三）保密原则

评估人员遵守保密义务，审慎使用并保护在评估过程获得的信息。

六、评估框架

根据相关法律法规的规定，结合跨境数据交易过程，首先针对交易主体的相关情况进行评估，再针对交易标的的相关情况进行评估，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。每个环节均从合法、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，评估框架见图 1。

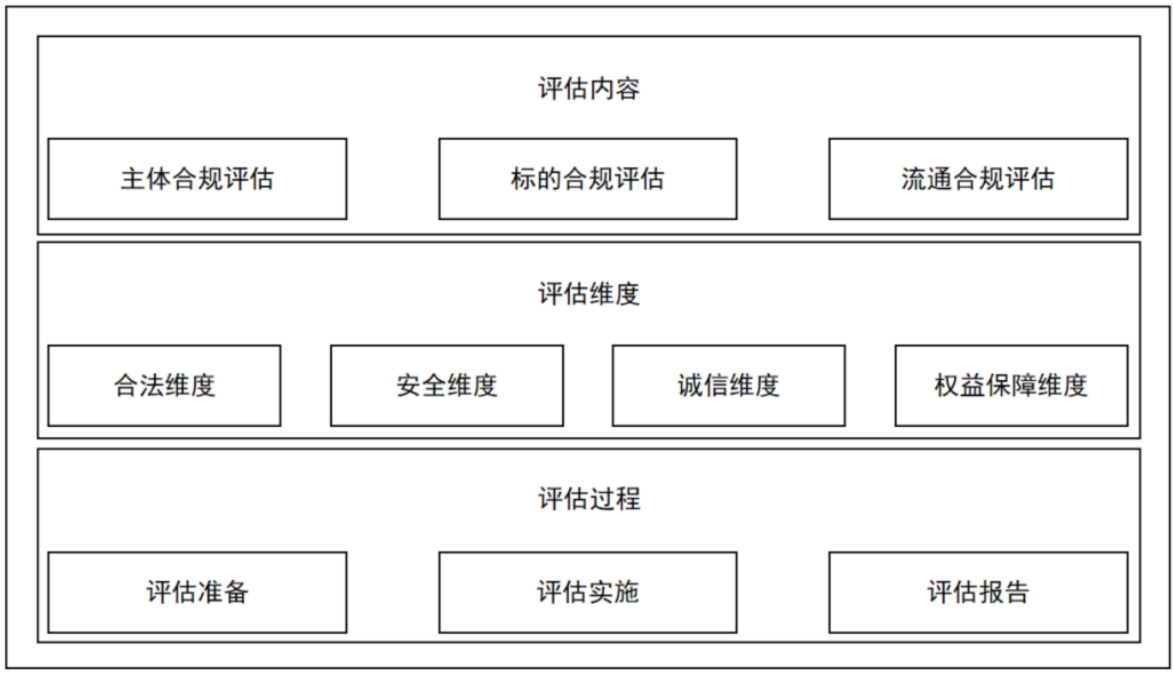


图 1　跨境数据交易合规评估参考框架图

七、主体合规评估

（一）合法维度评估

1. 对交易主体的评估内容包括:

a）境内交易主体依法取得的营业执照或相关登记证书合法有效，境外交易主体提供同等类型合法证照。

b）境内交易主体的经营业务若根据法律、行政法规规定须经批准或须获取特定行业资质的，已依法经过批准或获取特定行业资质，且在有效期内。

c）交易主体不存在开展我国法律法规禁止的数据交易的情形。

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。

（二）安全维度评估

境内交易主体根据交易的数据类型分为境内一般数据交易主体、境内涉重要数据交易主体、境内涉个人信息交易主体，适用不同数据类型的安全评估要求。

表 2　主体合规要求清单

分类	安全要求
境内一般数据交易主体	DB4403 / T 564—2024（数据交易合规评估规范）第 7.2.2 条、本文件第七条第（二）款第 1 项
境内涉个人信息交易主体	DB4403 / T 564—2024（数据交易合规评估规范）第 7.2.2 条、本文件第七条第（二）款第 1 项、第（七）条第（二）款第 2 项
境内涉重要数据交易主体	DB4403 / T 564—2024（数据交易合规评估规范）第 7.2.2 条、本文件第七条第（二）款第 1 项、第七条第（二）款第 2 项、第七条第（二）款第 3 项
境外交易主体	本文件第七条第（二）款第 4 项

1. 境内一般数据交易主体

对境内一般数据交易主体的评估内容包括:

a）根据本单位的业务特性、企业规模等相关因素匹配满足相对应的 DB4403 / T 564—2024 第 7.2.2 条安全维度评估要求的“A 级标准”;

b）具有专门负责数据跨境安全的负责人、组织，明确负责数据出境传输安全工作的团队及其工作职责;

c）制定跨境数据安全相关的制度，包括但不限于数据分类分级保护制度、数据跨境技术保护制度、数据跨境访问权限控制机制、数据跨境合规审查制度、数据跨境安全审计;

d）建立数据跨境交易业务合规保障机制，包括但不限于数据跨境合规风险监测预警机制、数据跨境应急预案、数据跨境监管响应机制;

e）在跨境数据分类分级的基础上，根据业务出境的场景，制定出境数据加密传输方案及出境传输通道的加密方案;

f）根据跨境交易的数据接口及数据类型，梳理出跨境交易的数据交易通道（接口、应用、邮件、数据集、FTP 等），形成出境通道清单;

g）交易主体若作为关键信息基础设施的运营者，在进行跨境数据交易向境外提供个人信息或者重要数据前已向国家网信部门进行申报并通过数据出境安全评估。

2. 境内涉个人信息交易主体

对境内涉个人信息交易主体的评估内容包括:

a）满足本文件第七条第（二）款第 1 项境内一般数据交易主体的安全合规要求;

b）明确指定负责个人信息出境的备份与恢复工作的部门或个人及其工作职责;

c）制定出境个人信息备份与恢复的制度和操作规程;

d）每年定期对出境的个人信息进行备份，并对备份数据完整性和可用性进行验证;

e）制定数据分类分级保护制度，并对个人信息进行标签标记;

f）梳理出跨境交易的个人信息交易通道（接口、应用、邮件、

数据集、FTP等），并通过数据标签识别出跨境交易的个人信息资产；

g）根据法律法规要求定期对出境的个人信息数量进行监测和统计，并制定预警阈值，在临近申报条件的预警值前进行预警，根据业务、场景的发展情况，选择适用的数据出境合规路径；

h）根据法律法规要求定期对个人信息跨境交易的通道（接口、应用、邮件、数据集、FTP等）的所有日志进行备份，确保日志的完整性，并对日志进行分析，日志记录传输的个人信息数量与备份的个人信息数量一致；

i）原则上个人信息出境的个人信息备份与个人信息跨境交易通道日志分别保存三年，法律另有规定除外；

j）建立个人信息跨境交易数据台账清单，确保因跨境交易而备份的个人信息按时删除、销毁；

k）对个人信息删除、销毁过程全程记录，并对数据删除、销毁效果进行评估；

l）跨境交易的个人信息数量满足法律法规相应要求的，采取适用的数据出境合规路径、履行对应的手续后，方可进行跨境交易；

m）关键信息基础设施的运营者交易个人信息，向国家网信部门进行申报，经过审批部门批准后方可进行跨境交易；

n）交易过程中如果接收到境外主体提供的境外个人信息，按照所在国家／地区的法律法规要求、安全保护要求进行安全处理；

o）明确出境接收方的安全责任，在出境数据共享过程中，对

接收方的出境数据安全防护能力（作为整体）进行评估。

3. 境内涉重要数据交易主体

对境内涉重要数据交易主体的评估内容包括:

a）满足本文件第七条第（二）款第 1 项境内一般数据交易主体的安全合规要求;

b）已向国家网信部门申报并通过数据出境安全评估;

c）根据国家和行业主管监管部门有关重要数据识别的规定以及重要数据识别规则国家标准的要求，制定并定期更新本组织的重要数据识别制度;

d）落实本组织的重要数据识别制度，对本组织处理的重要数据进行分级，并识别需跨境交易的重要数据，制定重要数据清单管理程序，明确清单的编制、审核、维护、更新等要求;

e）制定重要数据跨境交易的安全评估制度，明确评估要点、评估流程、跨境交易的审批流程等;

f）制定跨境交易的重要数据备份与恢复的制度和操作规程;

g）根据法律法规要求每年定期对跨境交易的重要数据进行备份，并对备份数据完整性和可用性进行验证;

h）数据安全负责人对重要数据跨境交易的数据传输过程中安全保护技术和管理措施的有效性进行评估，对跨境交易进行审批，并将评估和审批记录留存 3 年以上;

i）重要数据跨境交易，重要数据处理者已与数据接收方签订合同等法律文件，约定处理重要数据的目的、范围、处理方式、安

全保护义务等，并约定对接收方履行安全保护义务的情况进行监督；

j）数据安全负责人对接收方数据处理环境安全情况、数据安全防护能力、履行数据保护责任和义务的能力（或聘请数据第三方专业服务机构）进行评估，数据安全负责人对评估结果进行审批，并将评估和审批记录留存3年以上；

k）对重要数据跨境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，建立对数据交易过程进行追溯的能力；

l）主管部门或执法部门核验向境外提供重要数据的类型、范围时，以明文、可读方式予以展示；

m）采取技术和管理措施，在跨境交易的既定目的、范围、方式和数据类型、规模等事项之内进行数据跨境传输，不超出跨境交易前向国家申报数据出境安全评估时明确的事项等向境外提供重要数据；

n）主管部门认定不应出境的，停止数据出境，并采取有效措施对已出境数据的安全予以补救；

o）非经主管部门批准，不向外国司法或者执法机构提供存储于中国境内的重要数据。

4. 境外跨境交易主体

对境外交易主体的评估内容包括：

a）在享有数据权益的同时，已履行相关义务，确保数据交易安全合规；

b）满足其所在的国家／地区数据安全保护政策法规要求，网络安全环境达到中国境内数据安全、网络安全保护水平;

c）涉及个人信息跨境交易时，同时满足其所在国家／地区数据保护法律要求的数据处理合规义务，包括个人信息保护负责人和个人信息保护机构设置、个人信息跨境处理规则公示等;

d）涉及重要数据跨境交易时，提供不低于境内涉重要数据交易主体的数据安全保护能力，包括组织机构、技术与工具、人员能力等方面;

e）涉及重要数据跨境交易时，提供数据接收方名称、联系方式、接收数据的类型、数量及目的，重要数据在境外的存储地点、存储期限、适用范围和方式等;

f）涉及重要数据、个人信息跨境交易时，提供数据销毁机制，超过约定期限后对接收的重要数据进行销毁;

g）定期进行合规性评估，确保业务操作符合国内的法律要求和技术要求;

h）宜遵循国际影响力较大的数据隐私保护标准，如GDPR（欧盟通用数据保护条例）、HIPAA（美国健康保险流通与责任法案）等，确保个人数据处理的透明度、合法性和安全性;

i）宜通过ISO 27001信息安全管理体系的认证;

j）宜通过IS0 27701 隐私信息管理体系的认证。

（三）诚信维度评估

对交易主体的评估内容包括:

1. 满足DB4403／T 564—2024第7.3条“A级标准”对交易主体诚信维度的要求；

2. 双方确保在跨境数据交易过程中，不得违反所在国家或地区的出口管制、贸易限制、新闻舆论监督的相关规定，不得从事任何非法的数据转移或共享活动；

3. 发布的数据处理规则（如隐私政策、个人信息处理规则等）包含跨境数据处理相关规定；

4. 诚实守信，恪守承诺，全面及时履行合同约定及相关承诺。

（四）权益保障维度评估

对交易主体的评估内容包括：

1. 满足DB4403／T 564—2024第7.4条“A级标准”对交易主体权益保障维度的要求；

2. 交易主体之间通过法律文件约定数据安全保护义务的补救措施、违约责任和争议解决方式；

3. 交易主体在其官网、产品说明等公开途径公示了开展应急处置的要求和个人信息主体维护其个人信息权益的途径和方式。

八、标的合规评估

（一）合法维度评估

1. 来源合法

（1）境内数据来源合法

交易标的数据来源于境内或为境内数据卖方自行生产的数据的，需评估是否满足DB4403／T 564—2024第8.1.2条对数据来源

合法的要求。

（2）境外数据来源合法

1）对于交易标的数据来源于境外，在中国境内加工处理后再进行跨境交易的，评估内容包括:

a）交易标的为从公开渠道获取的数据的，能够证明获取方式与过程的合法性，确保数据的收集符合数据来源国家/地区及中国的法律法规;

b）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，能够证明采购或授权的合法性、真实性、完整性和有效性，确保第三方数据提供者提供交易标的遵循其所在国家/地区的法律法规;

c）交易标的涉及收集境外主体个人信息的，已根据适用的域外法律法规规定进行收集，确保该等收集已具备合法性基础，包括收集的范围、方式、目的等符合有关规定，数据主体已给予明确的同意或数据收集已取得其他合法性基础的;

d）交易标的获取过程、手段不存在违反我国法律法规强制性规定或者危害我国国家安全、公共安全或侵犯第三方合法权益的情形，且不含有以欺诈、诱骗、误导等方式或从非法、违规渠道获取的数据;

e）数据传输至中国境内的行为，已根据适用的域外法律法规规定，办理数据跨境的有关手续或满足其他域外国家或地区对数据跨境的要求;

f）数据传输至中国境内的行为，不违反数据来源国家/地区或其他司法管辖区适用的法律法规规定，包括但不限于反不正当竞争、反垄断、贸易管制和制裁、网络安全审查等方面的法律法规规定。

2）对于交易标的数据来源于境外，在中国境外加工处理后再跨境传输至中国境内进行交易的，评估内容包括:

a）数据的收集过程已根据适用的数据来源国家/地区法律法规规定，办理数据跨境的有关手续或满足其他域外国家或地区对数据跨境的要求，如数据主体同意或跨境数据传输的法律基础;

b）交易标的涉及收集境外主体个人信息的，已根据适用的数据来源国家/地区法律法规规定进行收集，确保该等收集已具备合法性基础，包括收集的范围、方式、目的等符合有关规定，数据主体已给予明确的同意或数据收集已取得其他合法性基础的;

c）所收集的数据不违反中国、数据来源国家/地区或其他司法管辖区适用的域外法律法规规定，包括但不限于反不正当竞争、反垄断、贸易管制和制裁、网络安全审查等方面的法律法规规定。在内容上不得包含涉政、涉恐等中国法律法规所禁止的内容。

2. 处理合法

（1）仅处理境内数据

交易标的形成仅涉及境内数据或境内数据卖方自行生产的数据的处理的，需评估是否满足 DB4403／T 564—2024 第 8.1.3 条对数据处理合法的要求。

（2）仅处理境外数据

交易标的形成仅涉及境内交易主体对境外数据处理，不涉及引入境内数据的，数据处理活动的评估内容包括:

a）处理活动遵循数据来源国家/地区或其他司法管辖区适用的法律法规，尤其是针对特定类型数据的规定（如敏感数据）；

b）若处理的境外数据包含境外个人信息，处理活动遵循数据来源国家/地区或其他司法管辖区个人信息保护相关的法律法规规定;

c）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、目的等限制，并履行法律法规规定的数据处理强制性义务，遵循数据处理的合规要求。

（3）引入境内数据

交易标的的形成系境内交易主体对境外数据的处理，且涉及引入境内数据的，数据处理活动的评估内容包括:

a）涉及对境内个人信息的引入的，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，不通过误导、欺诈、胁迫等方式处理个人信息;

b）涉及对境内个人信息的引入的，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）引入境内个人信息已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）保存个人信息期限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，但法律法规另有规定的除外；

e）交易主体委托处理个人信息的，已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，已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）交易标的涉及处理境内敏感个人信息、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，交易主体已开展个人信息保护影响评估并履行相应的合规义务；

h）涉及对境内公共数据的引入的，遵循公共数据开发利用相关法律法规、公共数据授权协议对公共数据处理的限制；

i）涉及对重要数据的引入的，在根据法律法规要求进行数据安全风险评估的过程中，已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；

j）涉及引入工业和信息化领域、能源领域重要数据等按照适

用法律法规的规定需要将本单位重要数据目录向本地区行业监管部门备案或报送的，已按照适用法律法规的规定完成备案或报送，备案或报送内容发生重大变化的，在发生变化的三个月内履行变更备案手续;

k）中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行。

3. 内容合法

对交易标的的内容评估包括:

（1）满足 DB4403／T 564—2024 第 8.1.4 条对数据内容合法的要求;

（2）不含有国家法律法规规定或者国家网信部门及其他有关主管部门认定的禁止交易或禁止出境的数据;

（3）含有国家法律法规规定或者国家网信部门及其他有关主管部门规定的限制或附条件出境的数据类型，但符合相应的条件;

（4）不含有以下数据:

a）其跨境可能危害国家安全或公共利益的数据;

b）其跨境可能违反与第三方约定或向第三方作出的承诺的数据;

c）其跨境可能侵犯第三方知识产权、商业秘密、个人隐私等合法权益的数据;

d）未依法公开、开放的公共数据;

e）未依法获得授权的个人信息或在不借助其他数据的情况下可以识别特定自然人的数据。

（二）安全维度评估

交易标的根据数据收集和产生的位置可以分为境内交易标的和境外交易标的。

1. 境内交易标的安全维度

对境内交易标的的评估内容包括:

a）满足DB4403／T 564—2024安全维度第8.2.2条“A级标准”下的通用要求以及对应数据类别的安全要求;

b）交易标的所在的存储区域与其他区域之间已采取可靠的技术隔离手段;

c）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;

d）根据交易标的数据来源所在国家或地区的法律法规要求匹配对应的安全管理和技术措施，保障交易标的安全;

e）已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，而且评估结果为无中高危风险;

f）涉及脱敏后的重要数据交易，数据卖方已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;

g）涉及公共数据交易的情况，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数据加工处

理，隐私计算平台已通过权威机构的安全检测，并获得相关证书。

2. 境外交易标的安全维度

对境外交易标的的评估内容包括:

a）满足本文件第八条第（二）款第 1 项“境内交易标的安全维度”的要求;

b）存储交易标的已采取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;

c）根据数据交易标的所在国家/地区的数据安全相关政策和监管环境对数据交易标的采取针对性的数据安全保障措施。

（三）诚信维度评估

对交易标的的评估内容包括:

a）满足 DB4403／T 564—2024 第 8.3 条的要求;

b）交易主体在交易标的推广和营销过程中不应使用夸大、虚假或误导性的宣传语，确保所有宣传材料准确反映交易标的质量、预设使用场景;

c）交易主体确保交易标的数据来源清晰、权属关系明确，确保数据跨境传输记录可溯源、传输过程可审查，且内容完整、规范。

（四）权益保障维度评估

对交易标的的评估内容包括:

a）满足 DB4403／T 564—2024 第 8.4 条的要求;

b）交易标的涉及处理不同国家/地区个人信息且具备相应告知条件的，以清晰、易懂（如设置多语言模式）等显著的方式告知

相关主体权益，并设置便捷的权益主张渠道;

c）告知内容包括权益告知、权益请求响应、权益异常处理等机制，以清晰的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，确保个人信息权益维护的渠道通畅。

九、流通合规评估

（一）合法维度评估

1. 通用要求

对流通对象的评估内容包括:

a）数据买方的主体资质满足其所在国家或地区的法律法规的规定;

b）数据买方已提供所属行业、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）交易主体已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；或取得个人信息保护相关认证。

d）数据买方按照交易申报（如需）的使用目的、场景和方式，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;

e）交易标的在跨境交易流通程序方面，交易主体已向有关部

门申请许可、履行备案、申报或办理其他行政手续并取得有关部门的批准；法律法规规定免予申报数据出境安全评估、个人信息出境标准合同备案、个人信息保护认证，且不属于需要申报网络安全审查及完成其他适用的许可、备案、申报流程的情形除外。

注 1：例如人类遗传资源数据跨境交易，需满足《中华人民共和国人类遗传资源管理条例》和《人类遗传资源管理条例实施细则》对人类遗传资源数据出境相关规定。

2. 不同跨境数据交易模式的评估内容

本文件的合规评估要求仅适用于本文件表 1 跨境数据交易模式I、II、III和VI。境内主体将境外数据引入境内数据后再销售境外主体的，适用本文件的相关规定。

（1）跨境数据交易模式I

跨境数据交易模式I是指跨境数据产品数据源为境内数据，数据卖方／数据商位于境内，数据买方位于境外。

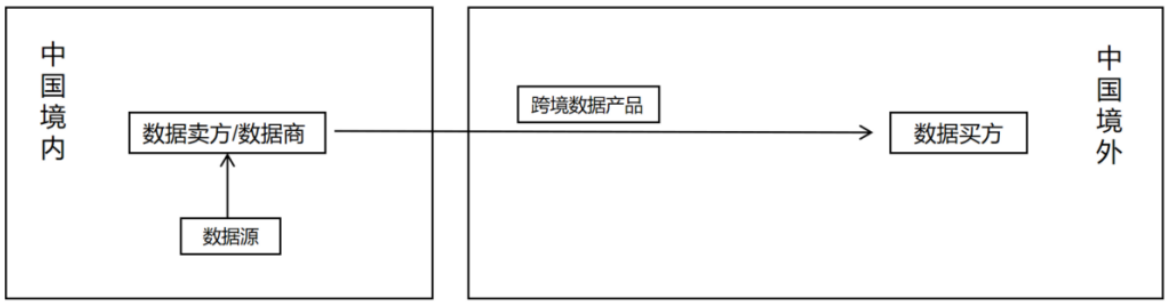


图 2　跨境数据交易模式I

对跨境数据交易模式I的流通合法性评估内容包括：

a）满足本文件第九条第（一）款第 1 项的要求；

b）跨境数据产品若涉及个人信息，数据卖方已告知个人信息

主体数据买方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向数据买方提供敏感个人信息的，已向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外;

c）跨境数据产品的形成以基于个人同意处理个人信息作为合法性基础，且跨境数据产品仍包含个人信息，已在释明数据跨境交易及其影响的前提下，取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，已取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，已取得书面同意;

d）跨境数据产品若涉及重要数据，数据卖方已向国家网信部门申报并通过数据出境安全评估;

e）关键信息基础设施运营者以外的数据处理者，自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息，向国家网信部门申报并通过数据出境安全评估，但法律法规另有规定的从其规定。

（2）跨境数据交易模式II

跨境数据交易模式II是指跨境数据产品数据源为境内数据，数据卖方／数据商及数据买方均位于境外。

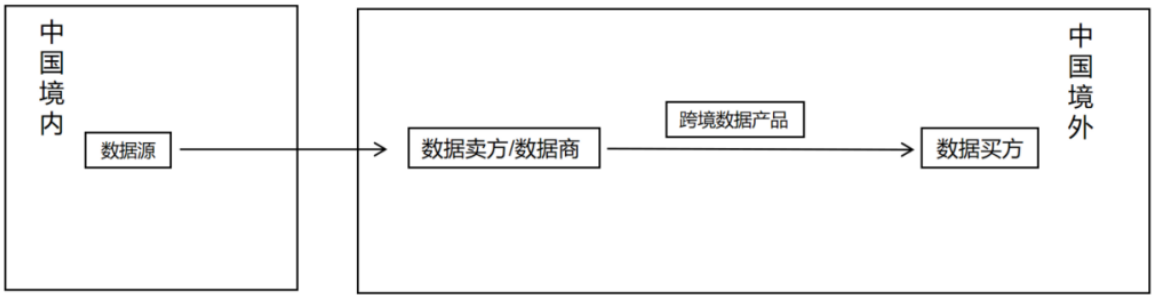


图 3　跨境数据交易模式II

对跨境数据交易模式II的流通合法性评估内容包括:

a）满足本文件第九条第（一）款第 1 项的要求;

b）跨境数据产品若涉及个人信息，数据卖方已告知个人信息主体数据买方的名称或者姓名、联系方式、处理目的、处理方式、个人信息种类、保存期限以及行使个人信息主体权利的方式和程序等事项。向数据买方提供敏感个人信息的，已向个人信息主体告知提供敏感个人信息的必要性以及对个人权益的影响。但是法律、行政法规规定不需要告知的除外;

c）跨境数据产品的形成以基于个人同意处理个人信息作为合法性基础的，已取得个人信息主体的单独同意。涉及不满十四周岁未成年人个人信息的，已取得未成年人的父母或者其他监护人的单独同意。法律、行政法规规定应当取得书面同意的，已取得书面同意;

d）跨境数据产品若涉及重要数据，数据卖方已向国家网信部门申报并通过数据出境安全评估;

e）数据卖方在中国设立代表处或指定代理人来处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等

报送中国履行个人信息保护职责的部门；若数据买方以向境内自然人提供产品或者服务，或以分析、评估境内自然人的行为为目的，同样适用该条要求。

（3）跨境数据交易模式III

跨境数据交易模式III是指跨境数据产品数据源为境内数据，数据卖方／数据商位于境外，数据买方位于境内。

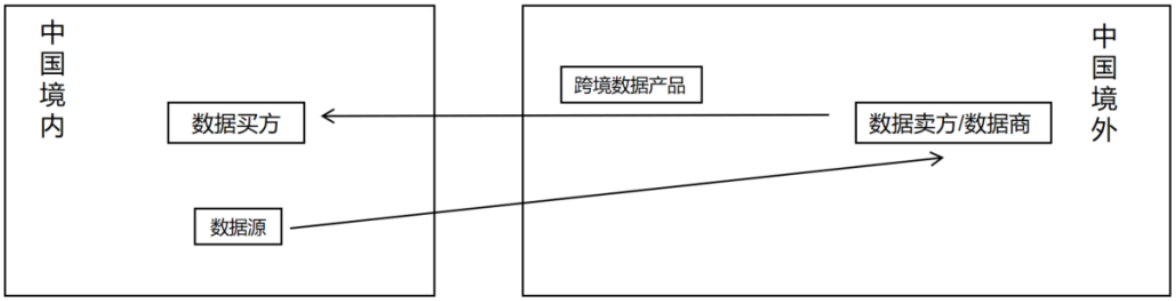


图 4　跨境数据交易模式III

对跨境数据交易模式III的流通合法性评估内容包括：

a）满足本文件第九条第（一）款第 1 项的要求；

b）数据卖方在中国设立代表处或指定代理人来处理个人信息保护相关事务，并将有关机构的名称或者代表的姓名、联系方式等报送中国履行个人信息保护职责的部门。

（4）跨境数据交易模式VI

跨境数据交易模式VI是指跨境数据产品数据源为境外数据，数据卖方／数据商位于境外，数据买方位于境内。

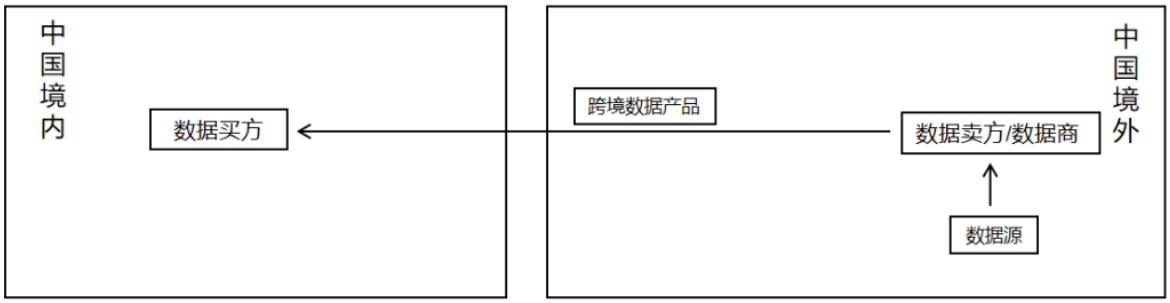


图 5　跨境数据交易模式VI

对跨境数据交易模式VI的流通合法性评估内容包括:

a）满足本文件第九条第（一）款第 1 项的要求;

b）跨境数据产品如果涉及境外的个人信息，则必须遵守境外相关法律法规的规定，如 GDPR，包括但不限于明确告知数据主体其数据如何被收集和使用、获取有效同意等;

c）如果涉及个人信息的跨境传输，需要遵守境外法律法规的规定，如签署数据跨境传输协议等;

d）若境外数据相关法律法规要求必须进行本地化存储，则已对跨境数据产品进行本地化部署;

e）跨境数据产品最终将在中国境内使用或处理，则需要符合中国相关法律法规的规定，不得向中国境内传输法律禁止的跨境数据产品。

（二）安全维度评估

跨境数据交易在流通方面的安全维度从境内交易主体和境外交易主体两个方面进行评估。

1. 境内交易主体的流通安全要求

对境内交易主体的流通安全评估内容包括:

a）满足 DB4403／T 564—2024 第 8.2.2 条、第 9.2.2 条“A 级标准”下通用要求以及对应数据类别安全要求;

b）交易主体在交易流通前进行身份验证，验证方式采用口令、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使用密码技术来实现;

c）交易主体作为数据卖方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，而且评估结果为无中高危风险;

d）交易主体作为数据卖方交易重要数据的，已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;

e）交易主体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、滥用等恶意行为能及时阻断并告警;

f）交易主体开展接口调用日志记录及监控审计，评估加密算法和协议安全漏洞。必要时引入第三方渗透测试等方式评估验证安全性;

g）交易主体在交易结束后，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。

2. 境外交易主体的流通安全要求

对境外交易主体的流通安全评估内容包括:

a）对出境传输通道两端主体进行身份鉴别;

b）使用行业最佳实践或不低于通行惯例的加密传输算法和协议，例如 TLS 1.3;

c）遵守我国关于数据流通与交易管理的法律法规，尊重社会公德、商业道德，服从监督管理;

d）能自动识别并阻拦我国法律法规禁止进口或接收的数据（如涉及中国禁止进口限制进口技术目录的技术数据）;

e）采取必要措施，做到交易过程可控制、风险可防范、责任可追溯、合规性可监督;

f）建立二级供应商选择策略和管理制度，根据产品／服务重要程度对二级供应商，特别是数据再出境的境外第三方开展安全调查，防范因政治、外交、贸易等非技术因素导致产品／服务供应中断的风险;

g）分别与二级供应商签订安全保密协议和安全责任书，明确安全和保密义务与责任。

9.3　诚信维度评估

对跨境数据交易流通的评估内容为满足 DB4403／T 564—2024 第 9.3 条对流通合规的诚信维度的要求。

9.4　权益保障维度评估

对跨境数据交易流通的评估内容包括:

a）满足 DB4403／T 564—2024 第 9.4 条的要求;

b）数据交易主体已签署具有法律约束力的文件，明确数据跨

境目的、方式、范围、数据保存地点、期限，境外交易主体违反数据安全保护义务的补救措施、违约责任和争议解决方式，数据安全事件的应急处置要求和保障个人维护其个人信息权益的途径和方式；

c）境内交易主体建立针对数据买方的监督审核机制，以确保境外交易主体按照交易合同约定的目的、范围及期限使用交易标的；

d）交易主体履行数据安全保护义务，采取技术措施和其他必要措施，保障数据出境安全。发生或者可能发生数据安全事件的，采取补救措施，及时向省级以上网信部门和其他有关主管部门报告。

十、评估方法

（一）评估准备

1. 评估团队组建

交易主体或其委托的第三方法律服务机构按照不同的跨境数据交易需求，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。

2. 评估方案

（1）评估团队按照不同的跨境数据交易需求，制定评估方案和评估计划。

（2）评估团队按照本文件第六、七、八条的要求及参照本文件附录 A 建议文档进行评估资料收集，并做好资料分类及内容标

记。

（3）交易主体对拟进行数据交易的申请资料进行确认，保证资料的完整性、正确性、一致性等符合相关法律要求。

（二）评估实施

1. 评估实施的工作流程如下:

（1）主体合规评估：评估团队依据本文件第六条的要求对主体合规进行评估，并记录评估结果和评估问题;

（2）标的合规评估：评估团队依据本文件第七条的要求对标的合规进行评估，并记录评估结果和评估问题;

（3）流通合规评估：评估团队依据本文件第八条的要求对流通合规进行评估，并记录评估结果和评估问题;

（4）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;

（5）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。

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

（三）评估报告

1. 评估报告编制

评估团队整理评估过程记录、评估底稿文件及评估结果，基于分析结果，撰写评估报告，报告中包含评估过程、主要发现、结论、

改进建议等内容。

2. 结果沟通与反馈

评估团队签署评估报告并发送至交易主体，收集反馈意见。

3. 跟踪与改进

交易主体根据评估结果和反馈，制定改进措施或调整策略，设定跟踪机制以监督改进措施的实施情况和效果。

4. 存档与复审

第三方法律服务机构对本次评估活动的全部材料进行归档封存。

附　录　A

跨境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下表 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、负责人工作履历、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）跨境交易的数据交易通道清单（包括个人信息传输通道和重要数据传输通道）； f）出境数据加密传输方案及出境传输通道的加密方案； g）数据跨境合规风险监测平台、平台日志分析报告； h）网信部门对于数据出境（个人信息 / 重要数据）的审核结果； i）境外数据接收方的数据安全防护能力的评估报告； j）个人信息、重要数据跨境交易的数据传输过程中安全保护技术和管理措施的评估报告； k）IS0 27001 信息安全管理体系、ISO 27701 隐私信息安全管理体系认证证书等。
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，若涉及处理不同法域的个人信息，还需提交不同法域对应的隐私政策等文本）； 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；

评估维度	建议文档
	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下表 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）适用时，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）境外交易标的在存储过程中的完整性、保密性、安全保障措施的证明材料。
诚信维度	a）交易标的的描述说明、适用范围、计费方式等信息、服务样例； b）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。
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（示例，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，包括交易标的的服务类型、涉及数据类型、敏感程度（是否属于重要数据、敏感个人信息）等； 6）流通费用描述，包括计费方式、标准、税率等。 b）交易标的合同文本（包括个人信息出境标准合同、数据传输协议等）。 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，已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）提供用于跨境数据交易标的流通的资质、行政许可、备案证明文件（如备案通知、安全评估通知、个人信息保护认证以及境外的数据跨境合规证明等）。
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、数据出境风险自评估报告； 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； g）跨境数据交易传输的加密传输算法和协议证明； h）数据跨境传输监控管理平台以及过滤策略证明； i）境外数据交易主体的二级供应商选择策略和管理制度； J）与二级供应商签订安全保密协议和安全责任书。
诚信维度	a）承诺函； b）交易标的说明文本； c）交易标的合同文本； 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（若涉及处理不同法域的个人信息，还需提交不同法域对应的隐私政策等文本）； b）数据主体权利请求响应方式、流程、管理政策； c）建立投诉、举报机制，设置便捷的投诉、举报入口，公布处理流程和反馈时限，及时受理、处理公众投诉举报证明等； d）建立辟谣机制，保存利用深度合成服务制作、复制、发布、传播虚假信息有关记录证明等。

附　录　B

特殊场景下的跨境数据交易合规要求

B.1　概述

本资料性附录依据相关法律法规及特定行业对数据跨境传输的规定，针对跨境数据交易的特殊情形提供列举说明。这些特殊情形包括但不限于以下几类，且每种情形及行业均需遵循相应的数据跨境传输要求。

B.2　医疗应用场景

包含但不限于以下行为：

a）反映群体健康生理状况、族群特征、遗传信息等的基础数据，如人口普查资料、人类遗传资源信息、基因测序原始数据属于重要数据。

b）在临床试验、远程诊疗服务、国际联合研究、国际医疗保险等医疗应用行业的出境场景中，若出境的数据属于重要数据的范畴，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

c）在临床试验、远程诊疗服务、国际联合研究、国际医疗保险等医疗应用行业的出境场景中，若出境的临床试验数据、患者健康数据包含敏感个人信息，自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息，已通过所在地省级网信部门向国家网信部门申报数据出境安

全评估。但出境数据如果属于相关自由贸易试验区就医疗领域数据出台的负面清单范围内数据，则应按照相关自由贸易试验区就负面清单制定的管理规定进行数据出境。d）利用我国人类遗传资源开展国际合作科学研究，或者因其他特殊情况确需将我国人类遗传资源材料运送、邮寄、携带出境的，符合下列条件，并取得国务院科学技术行政部门出具的人类遗传资源材料出境证明：

1）对我国公众健康、国家安全和社会公共利益没有危害；

2）具有法人资格；

3）有明确的境外合作方和合理的出境用途；

4）人类遗传资源材料采集合法或者来自合法的保藏单位；

5）通过伦理审查。

注 1：利用我国人类遗传资源开展国际合作科学研究，需要将我国人类遗传资源材料运送、邮寄、携带出境的，可以单独提出申请，也可以在开展国际合作科学研究申请中列明出境计划一并提出申请，由国务院科学技术行政部门合并审批。

注 2：将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用的，已向国务院科学技术行政部门备案并提交信息备份。

B.3　汽车应用场景

包含但不限于以下行为：

a）汽车行业中，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能危害国家安全、公共利益或者个人、组织合法权益

的数据，属于汽车行业重要数据，包括:

1）军事管理区、国防科工单位以及县级以上党政机关等重要敏感区域的地理信息、人员流量、车辆流量等数据;

2）车辆流量、物流等反映经济运行情况的数据;

3）汽车充电网的运行数据;

4）包含人脸信息、车牌信息等的车外视频、图像数据;

5）涉及个人信息主体超过 10 万人的个人信息;

6）国家网信部门和国务院发展改革、工业和信息化、公安、交通运输等有关部门确定的其他可能危害国家安全、公共利益或者个人、组织合法权益的数据，包括但不限于根据《汽车数据出境安全指引（2026 版）》中各场景判定规则判定为重要数据的汽车数据。

b）汽车数据处理者在跨国车辆诊断和维修、车联网和智能网联汽车数据共享、全球供应链管理、跨国合作研发等场景中向境外提供数据，若出境的数据属于重要数据的范畴，依法在境内存储，因业务需要确需向境外提供的，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

c）汽车数据处理者向境外提供重要数据，不得超出出境安全评估时明确的目的、范围、方式和数据种类、规模等。国家网信部门会同国务院有关部门以抽查等方式核验前款规定事项，汽车数据处理者予以配合，并以可读等便利方式予以展示。

d）向境外提供重要数据的汽车数据处理者，在每年十二月十

五日前向省、自治区、直辖市网信部门和有关部门报送以下年度汽车数据安全管理情况:

1）汽车数据安全管理负责人、用户权益事务联系人的姓名和联系方式;

2）处理汽车数据的种类、规模、目的和必要性;

3）汽车数据的安全防护和管理措施，包括保存地点、期限等;

4）向境内第三方提供汽车数据情况;

5）汽车数据安全事件和处置情况;

6）汽车数据相关的用户投诉和处理情况;

7）出境汽车数据接收者的基本情况;

8）出境汽车数据的种类、规模、目的和必要性;

9）汽车数据在境外的保存地点、期限、范围和方式;

10）涉及向境外提供汽车数据的用户投诉和处理情况;

11）国家网信部门会同国务院工业和信息化、公安、交通运输等有关部门明确的其他汽车数据安全管理情况。

e）汽车数据处理者在跨国车辆诊断和维修、车联网和智能网联汽车数据共享、全球供应链管理、跨国合作研发等场景中向境外提供数据，自当年1月1日起累计向境外提供100万人以上个人信息（不含敏感个人信息）或者1万人以上敏感个人信息，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。但出境数据如果属于相关自由贸易试验区就汽车领域数据出台的负面清单范围内数据，则应按照相关自由贸易试验区就负面清单制定的管

理规定进行数据出境。

f）有下列情形之一的，汽车数据处理者免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息出境认证（下列各项所称向境外提供的个人信息，不包括重要数据）：

1）在境外收集和产生的汽车数据传输至境内处理后向境外提供，处理过程中没有引入境内个人信息或者重要数据的；

2）为订立、履行个人作为一方当事人的合同，如跨境购车、跨境寄递、跨境支付、跨境注册账户等，确需向境外提供个人信息的；

3）按照依法制定的劳动规章制度和依法签订的集体合同实施跨境人力资源管理，确需向境外提供员工个人信息的；

4）紧急情况下为保护自然人的生命健康和财产安全，确需向境外提供个人信息的；

5）关键信息基础设施运营者以外的汽车数据处理者自当年1月1日起累计向境外提供不满10万人个人信息（不含敏感个人信息）的；

6）自由贸易试验区内登记注册的汽车数据处理者符合自由贸易试验区有关要求，向境外提供负面清单外的数据的；

7）因修补安全漏洞需要，汽车数据处理者按照《网络产品安全漏洞管理规定》有关要求，已向工业和信息化部报告的安全漏洞数据；

8）因处置安全事件需要，汽车数据处理者按照行业网络安全、

数据安全事件相关应急预案，已向工业和信息化部及相关行业监管部门报告的汽车产品、车联网平台及相关系统的安全事件数据；

9）因消除汽车产品缺陷、实施召回需要，汽车数据处理者按照《缺陷汽车产品召回管理条例》已向国家市场监督管理总局备案的 OTA 升级软件包对应的源代码。

g）落实《汽车数据出境安全指引（2026 版）》中规定的管理、防护技术、日志、应急处置等方面的汽车数据出境安全保护要求。

B.4　金融应用场景

包含但不限于以下行为：

a）通常主要用于金融行业大型或特大型机构、金融交易过程中重要核心节点类机构中的关键业务，一般针对特定人员公开，且仅为必须知悉的对象访问或使用，属于金融行业的重要数据；

b）金融机构向境外提供数据的，若出境的数据属于重要数据的范畴，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

c）若金融机构属于关键信息基础设施运营者的范畴，或自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息的，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。但出境数据如果属于相关自由贸易试验区就金融领域数据出台的负面清单范围内数据，或属于金融行业主管部门就金融行业数据出境制定的特别规定所附清单范围内数据，则应按照相关自由贸易试验区就负面清单制定

的管理规定，或相关行业主管部门就数据出境制定的特别规定进行数据出境。

d）在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息，在境内存储、处理和分析。因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，具体要求如下：

1）符合国家法律法规及行业主管部门有关规定；

2）获得个人金融信息主体明示同意；

3）依据国家、行业有关部门制定的办法与标准开展个人金融信息出境安全评估，确保境外机构数据安全保护能力达到国家、行业有关部门与金融业机构的安全要求；

4）与境外机构通过签订协议、现场核查等方式，明确并监督境外机构有效履行个人金融信息保密、数据删除销毁、案件协查等职责义务。

e）境外证券监督管理机构不得在中华人民共和国境内直接进行调查取证等活动。未经国务院证券监督管理机构和国务院有关主管部门同意，任何单位和个人不得擅自向境外提供与证券业务活动有关的文件和资料。

B.5　人工智能应用场景

包含但不限于以下行为：

a）若出境数据中涉及人工智能的训练数据，确保训练数据来源的合法合规，不使用非法的、未经授权的、可能侵犯他人包括知

识产权、人格权或者其他合法权利的数据对人工智能进行训练，并确保训练数据来源的可追溯，处理个人信息至少具备一个合法性基础。

b）面向境外提供人工智能产品或服务的企业，或国内企业通过境外生成式人工智能模型堆砌数据，增加至一定量级时可能构成重要数据，审查训练数据中是否包含重要数据，若存在重要数据，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。

c）面向境外提供服务的我国人工智能产品服务提供者，或在国内提供服务的境外人工智能产品服务提供者，需精准识别人工智能与用户交互过程中收集的个人信息，若自当年 1 月 1 日起累计向境外提供 100 万人以上个人信息（不含敏感个人信息）或者 1 万人以上敏感个人信息的，已通过所在地省级网信部门向国家网信部门申报数据出境安全评估。但出境数据如果属于相关自由贸易试验区就人工智能领域数据出台的负面清单范围内数据，则应按照相关自由贸易试验区就负面清单制定的管理规定进行数据出境。

d）面向境外提供服务的我国人工智能产品服务提供者，或在国内提供服务的境外人工智能产品服务提供者，明确其提供的人工智能服务的机制机理，确保人工智能服务的应用场景合法正当，并在面向用户提供生成文本、图片、音频、视频等内容时，对生成内容或生成内容的界面进行明确标识。

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 564—2024 数据交易合规评估规范

[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] 中华人民共和国公司法.第十三届全国人民代表大会常务委员会第六次会议第四次修正.2018 年 10 月 26 日

[15] 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

[16] 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

[17] 中华人民共和国对外贸易法.中华人民共和国主席令第 128 号.2022 年 12 月 30 日

[18] 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

[19] 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

[20] 网络数据安全管理条例.国务院令第 790 号.2024 年 9 月 24 日

[21] 中华人民共和国技术进出口管理条例. 国务院令第 732 号. 2020 年 11 月 29 日

[22] 征信业管理条例.国务院令第 631 号.2013 年 1 月 21 日

[23] 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

[24] 广东省公共数据管理办法.粤府令第 290 号.2021 年 10 月 25 日

[25] 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

[26] 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

[27] 个人信息出境认证办法.国家互联网信息办公室、国家市场监督管理总局令第 20 号.2026 年 1 月 1 日

[28] 网络安全审查办法.国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国工业和信息化部、中华人民共和国公安部、中华人民共和国国家安全部、中华人民共和国财政部、中华人民共和国商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、中国证券监督管理委员会、国家保密局、国家密码管理局令第 8 号.2022 年 2 月 15 日

[29] 个人信息保护合规审计管理办法.国家互联网信息办公室令第 18 号.2025 年 5 月 1 日

[30] 国家网络安全事件报告管理办法.国家互联网信息办公室 2025 年 9 月 11 日发布.2025 年 11 月 1 日

[31] 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

[32]汽车数据出境安全指引（2026 版）.工信部联网安〔2026〕27 号.2026 年 1 月 30 日