ICS 35. xxx
CCS Lxx

团　　体　　标　　准

T/ISC XXX—XXXX

数据跨境合规流通体系建设指南

xxxx—xxxx

在提交反馈意见时，请将您知道的相关专利与支持性文件一并附上。

（征求意见稿）

2025-07-13

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中 国 互 联 网 协 会　　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。

本文件由联通数据智能有限公司提出。

本文件由中国互联网协会归口。

本文件起草单位：联通数据智能有限公司、×××、×××、×××。

本文件主要起草人：×××、×××、×××。

本文件为首次发布。

——

数据跨境合规体系建设指南

1 范围

本文件明确规定了数据跨境合规服务体系的各项要求，涵盖数据治理、技术体系、场景运营、监管要求以及数据流通生态等方面。

本文件适用于所有开展数据跨境活动的组织，包括但不限于企业、机构等，旨在为数据跨境流动提供系统化、规范化的合规体系框架，促进数据要素跨境安全有序流通。

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 35273—2020 信息安全技术 个人信息安全规范

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

3 术语和定义

GB/T AAAAA—AAAA界定的以及下列术语和定义适用于本文件。为了便于使用，以下重复列出了GB/T AAAAA—AAAA中的某些术语和定义。

3.1

跨境数据评估 cross-border data transmission assessment

将境内收集或产生的数据通过网络传输方式提供给境外机构的一次性或连续性活动。

3.2

数据分类分级

将境内收集或产生的数据通过网络传输方式提供给境外机构的一次性或连续性活动。

3.3

个人信息

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，不包括匿名化处理后的信息。

3.4

数据流通 Data circulation

数据脱离了原有使用场景，变更了使用目的，从数据产生端转移至其他数据应用端的过程，是优化数据资源配置、释放数据价值的重要环节。

3.5

数据安全能力 Data security capability

组织在组织建设、制度流程、技术工具以及人员能力等方面对数据的安全保障。

3.6

数据脱敏 Data desensitization

通过一系列数据处理方法对原始数据进行处理以屏蔽敏感数据的一种数据保护方法。

3.7

合规 Compliance

对数据安全所适用的法律法规的符合程度。

4 数据跨境合规体系

围绕数据 “治理 - 技术 - 场景 - 监管 - 生态” 五位一体的架构，开展数据合规服务体系建设。通过整合数据治理策略、技术保障措施、场景化运营方案、监管要求落实以及生态各方协同，建立完善的数据跨境流通合规服务能力，为数据价值的安全、高效、可持续释放提供坚实保障。

5 数据治理合规

聚焦数据治理合规，围绕数据治理、数据生命周期、数据流通流转，明确各环节数据治理要求，确保数据全流程的保密性、完整性和可用性。

5.1 数据治理

5.1.1 合规管理体系

a）规定数据流通的具体要求，明确数据流通的目标、遵循的行动原则、完成的明确任务、实行的工作方式、采取的一般步骤和具体措施；

b）整理数据流通制度内容，包括数据合规政策、数据合规管理办法和数据合规管理细则等，确保数据流通活动能够遵循规则和流程；

c）宣传数据流通制度，对操作数据流通的人员进行培训和宣传，提高他们的合规意识和技能，确保数据流通活动得以合规进行；

d）设计合适的流程和技术措施，确保数据流通过程中的数据安全性和隐私保护，同时防范数据泄露和其他不当行为的发生；、

e）确定数据流通的控制点和监督机制，对数据流通的过程和结果进行监控和管理，及时发现问题并采取措施加以解决；

f）建立责任追究机制，对数据流通中的违规行为进行查处和惩戒，保证数据流通的合规性和稳定性。

5.1.2 数据分类分级

a）根据数据的敏感程度和重要性对数据进行分类分级管理，明确不同类别和级别的数据保护要求。

b）基于法律法规以及业务需求确定组织内部的数据分类分级方法,对生成或收集的数据进行分类分级标识。

5.1.3 风险评估

a）建立数据使用过程的风险评估机制，保护国家秘密、商业秘密和个人隐私，防止数据资源被用于不正当目的；

b）宜对数据使用行为开展定期评估，确保数据处理行为符合双方约定要求，对审计发现超出双方约定的行为及时停止接入。

c）宜通过第三方服务机构对数据流通后的使用条件、约束机制等合规要求进行评估；

d）应定期开展风险评估报告，确保数据流通在终止之前都处于安全合规的状态；

5.2 数据生命周期

5.2.1 数据采集

a）在数据采集前，明确采集目的和范围，确保采集行为合法合规，并获得数据主体的有效授权。

b）对于从客户端采集的数据，应当遵循最小必要原则，并获得用户授权同意。涉及采集敏感信息时，必须要有合理业务场景，且需单独明示收集使用规则并获得用户授权同意。

c）对于网络爬虫获取的数据，须经法务评估以确保符合网络及数据安全、著作权、不正当竞争等法律要求，遵守相关自律公约，禁止通过攻防对抗方式爬取数据。

d）对于采购而来的商业数据，业务方责任人须确保数据采集来源、渠道的合法性，采集目的及流程的正当性，并通过采购合同协议等明确采集数据的目的和用途，并保留相关记录，确保符合相关法律法规要求。

e）采用标准化的数据采集工具和方法，保证采集数据的质量和一致性。

f）对采集到的数据进行初步的清洗和校验，去除无效或错误数据，并做好采集过程记录，包括采集时间、采集人员、数据来源等信息，为后续的数据管理提供基础资料。

5.2.2 数据存储

a）采用加密存储、异地备份等安全措施，确保数据存储的保密性和可靠性。

b）建立数据存储管理制度，明确数据存储期限、存储位置变更、存储介质管理等要求。

c）定期对存储数据进行检查和维护，防止数据丢失、损坏或泄露。

d）对存储系统进行安全防护，如设置访问控制、入侵检测等，保障数据存储环境的安全。

e）应制定数据备份及恢复策略，定期进行数据备份，建立介质存取、验证和转储管理制度，并按介质特性对备份数据进行每年不少于 2 次的定期恢复的有效性验证。

5.2.3 数据处理

a）建立完整的数据合规管理体系，包括对数据来源、访问授权、分类分级控制、数据访问监控等方面进行管理，实现组织内部对数据生命周期的全面管理，确保数据合规性；

b）对流通过程中的数据进行识别，包括个人信息、重要数据和其他数据，并形成数据保护目录。该目录应及时更新，确保对新的数据进行及时识别和保护，并记录数据的分类、分级和敏感程度等信息；

c）组织应按照国家标准、协议规定和业务运营需要对所流通的数据进行分类分级管理。

d）制定数据管理的利益相关者清单，围绕利益相关者的需求，对其数据访问和控制权限进行授权和管理。在数据访问过程中，对用户的身份进行认证识别，并记录和监控其行为，确保数据的安全和隐私；

e）组织应对所流通的数据项进行合规检测，包含数据数量、数据字段属性等，并形成记录。合规检测结果应能根据《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》、《国家健康医疗大数据标准、安全和服务管理办法》的要求，识别敏感数据，对有安全风险的数据项进行排查；

f）对个人属性数据中可唯一识别到个人的信息进行去标识化处理，以保障个人隐私。常用的去标识化方法有屏蔽、抑制、假名化、泛化、加密、数据合成等技术，应根据实际情况选择合适的方法；

g）组织应开展数据流通风险评估，确保流通涉及的健康医疗数据处理和服务符合数据安全和隐私保护要求；风险评估报告应包括处理数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等；

h）对流通数据的合规性进行证明，应通过数据安全管理的主管部门或第三方机构出具的合规检测报告或合规评估报告

5.2.4 数据传输

a）严格遵循最小必要原则，仅向授权人员和机构提供必要的数据

b）对数据使用和共享行为进行记录和审计，确保数据使用的合规性和可追溯性

c）在与外部机构进行数据共享时，签订数据共享协议，明确数据使用范围、保密责任等条款，并对共享数据进行脱敏处理，降低数据泄露风险。

d）数据提供方、接收方双方主体之间按应确保数据安全性，通过校验技术或密码技术保证数据在传输过程中的保密性、完整性；

e）保障数据传输安全性，应将数据在传输过程中进行加密处理，宜采用国家密码局推荐的国密算法加密；

f）在不适合公开原始数据的数据流通场景中，应采用多方安全计算、联邦学习和可信执行环境等隐私计算技术，实现原始数据不出域，数据可用不可见的目标；

g）对于非离线传输链路，如专线、互联网线路和 VPN 等，应采用 TLS、IPSEC、SASL+SSL 等安全传输协议，以保障传输链路的安全性，防止入侵攻击；

h）对于离线传输方式，应确保存储介质的安全性，并将数据加密和密钥分开存储。应记录数据导入导出和介质交接情况，以确保数据的安全传输

5.2.5 数据销毁

a）制定数据销毁处置规范，明确数据销毁的条件、方式和流程。

b）当数据达到存储期限、失去使用价值或因其他原因需要销毁时，采用安全可靠的销毁技术，如数据擦除、物理粉碎等，确保数据无法被恢复。

c）数据销毁前，进行备份和审批确认；销毁过程中，做好记录，包括销毁时间、销毁方式、参与人员等信息。

d）销毁后，及时更新数据资产目录，注销相关数据权限，防止数据被非法使用。

e）应确保所销毁数据被完全清除且不被恢复，同时还应对销毁活动进行记录和留存；

5.3 数据流通流转

5.3.1 传输审批

a）建立数据跨境传输分级审批制度，根据数据敏感程度和重要性划分审批等级。

b）普通数据由部门负责人审批，重要数据需经数据治理委员会审核，敏感数据需报监管部门备案。

c）审批过程中需对传输必要性、合法性、接收方资质等进行严格审查，确保数据跨境传输

5.3.2 数据审计

a）建立针对数据流通的审计制度，对数据的使用活动进行审计，并确定必要的审计控制范围和需要审计的数据；

b）建立数据流通日志系统，保证审计日志的完整性，记录数据流通过程中的访问者、程序、时间、地点和场景等信息，确保重点审计数据的访问和操作合规性，并记录安全事件；

c）发布审计报告，向高级管理人员、数据管理专员以及其他利益相关者报告组织内的数据安全状态；

6 技术体系合规

阐述跨境数据流通技术体系合规，涵盖基础环境、智算模型、安全防护等技术领域，要求组织在物理、网络、系统环境以及人工智能算法等方面符合安全要求，构建权责明晰、规则透明、全程可溯的流通环境，建立健全安全技术防护体系。

6.1 基础环境合规

a）组织应确保数据中心的物理安全和环境安全，采取防火、防盗、防雷、防潮等措施，保护数据中心的安全。

b）组织应建立网络安全防护体系，采取防火墙、入侵检测、加密等技术措施，保护网络安全。

c）组织应确保数据跨境活动所涉及的系统环境符合国家相关标准和要求，包括操作系统、数据库、应用系统等方面。

d）组织应建立系统环境管理制度，规范系统环境的运维和管理，对系统环境进行定期检查和维护，确保系统环境的安全和稳定。

6.2 智算模型合规

a）组织应确保数据跨境活动所涉及的智算模型符合国家有关规定和标准要求。

b）组织应建立算法安全评估机制，对智算模型的算法进行安全评估，确保算法的公平性、透明度和可解释性。

c）加强对算法的监测和管理，及时发现和处理算法歧视、偏见等问题。

d）组织应确保智算模型训练数据的安全性和合规性，对训练数据进行严格的审核和管理，确保训练数据不包含敏感信息和违法信息。

e）在使用外部数据进行模型训练时，应取得数据所有者的同意，并签订数据使用协议。

6.3 安全防护合规

组织应建立健全数据安全防护体系，采取技术和管理措施，保护数据的安全性和完整性。

6.3.1 数据加密

a）组织应根据数据的敏感程度和重要性，对数据进行加密处理，确保数据在存储和传输过程中的安全性。

b）采用符合国家密码管理规定的加密算法和加密产品，确保加密的安全性和可靠性。

6.3.2 访问控制

a）组织应建立访问控制机制，对数据的访问进行严格的权限管理，确保只有授权人员才能访问数据。

b）采用身份认证、授权管理等技术措施，确保访问控制的有效性。

6.3.3 数据脱敏

a）组织在进行数据共享、传输等活动时，应对敏感数据进行脱敏处理，确保数据的安全性。

b）采用符合国家有关规定和标准要求的数据脱敏技术和方法，确保脱敏的有效性和可靠性。

7 场景运营合规

规范场景运营合规，从行业要求、业务流程、权责管理三方面入手，开展运营时应采取措施确保数据流通交易符合行业、自身业务合规要求，明晰权责，保障数据要素流通运营的合规。

7.1 行业要求合规

a）组织应确保数据跨境活动符合所在行业的特殊要求和规定。

b）组织应了解所在行业的数据安全要求和规定，按照行业要求和规定采取相应的安全保护措施，确保数据的安全性。

c）加强与行业主管部门的沟通和交流，及时了解行业最新的政策法规和标准要求。

d）组织应遵守所在行业的跨境业务规范和规定，按照行业规范和规定开展跨境业务活动。

7.2 业务流程合规

a）组织应确保数据跨境活动所涉及的业务流程符合国家有关规定和标准要求。

b）组织在设计跨境业务流程时，应充分考虑数据跨境合规的要求，确保业务流程合法合规。

c）建立跨境业务流程审批机制，对跨境业务流程进行严格的审批，确保业务流程符合国家有关规定和标准要求。

d）组织应制定跨境业务操作规范，明确跨境业务操作的流程、标准和要求。

e）加强对跨境业务操作人员的培训和管理，确保操作人员熟悉业务流程和操作规范，严格按照规定进行操作。

7.3 权责管理合规

a）数据处理者应按照数据控制者的要求处理数据，确保数据处理活动符合法律法规和相关监管要求。

b）建立数据处理安全管理制度，明确数据处理的流程、标准和要求，加强对数据处理活动的管理和监督。

c）建立数据主体投诉处理机制，及时处理数据主体的投诉和建议，维护数据主体的合法权益。

8 监管要求合规

严格恪守监管合规要求，全面遵循国家法律法规、行业规范及企业安全制度；系统开展跨境合规评估，规范完成标准合同备案，确保跨境数据传输符合监管要求。

8.1 监管合规

a）组织应及时了解国家有关数据跨境监管的政策法规和标准要求,按照政策法规和标准要求开展数据跨境活动。

b）建立监管政策跟踪机制，及时跟踪监管政策的变化，调整数据跨境合规策略。

c）发生数据安全事件时，应立即采取相应的补救和防范措施。涉及个人信息的，及时以电话、短信、邮件或者信函等方式告知个人信息主体，同时对可能危害国家安全、公共安全、经济安全和社会稳定的按相关要求向有关主管部门报告；

d）组织应及时了解国家有关数据跨境监管的政策法规和标准要求,按照政策法规和标准要求开展数据跨境活动。

e）组织应按照监管部门的要求，及时报送数据跨境活动的相关信息，接受监管部门的监督检查。

f）面对主管部门审查时，数据流通提供方、数据接收方应迅速响应，依据法律规定、监管要求和内部合规体系要求，应配合查处与整改工作。

8.2 合规评估

a）组织在进行数据出境活动前，应按照国家有关规定进行数据出境安全评估，评估数据出境的必要性、安全性和对个人信息权益的影响。

b）组织应建立合规评估机制，明确合规评估的目的、范围、方法和流程,并定期开展合规评估工作。

c）根据评估结果，采取相应的安全保护措施，确保数据出境活动符合国家有关规定。

8.3 标准合同

开展数据流通活动时，应通过合同来规范，双方需制定数据流通协议，明确数据获取流程、权利、义务及服务质量要求，确保数据流通符合法律法规，并维护数据安全和隐私。协议主要内容应包含：

a）组织应按照国家网信部门制定的标准合同文本，与境外接收方签订个人信息出境标准合同。

b）在签订标准合同前，应对境外接收方的数据安全保护能力进行评估，确保境外接收方能够按照标准合同的要求保护个人信息的安全。

c）合同应明确双方权利和义务，并根据利益相关者的需求对数据获取流程、服务质量、法律法规等方面进行详细说明；

d）应包括数据传输、处理、存储、使用、删除、追溯等环节的具体规定，以确保数据的安全、可靠、可信、隐私保护等方面得到保障；

e）应符合相关法规和规定，并在签署前进行合规审查，确保双方遵守相关法规和规定，避免出现违法行为和法律纠纷

f）组织应按照标准合同的约定，履行自己的义务，确保个人信息出境活动符合标准合同的要求。

g）建立标准合同履行监督机制，对标准合同的履行情况进行监督检查，及时发现和处理标准合同履行中的问题。

9 数据生态合规

对数据提供方、接收方、合作方提出合规要求，明确各方在的权利义务，构建多方协作的合规生态，营造安全、有序的数据跨境环境，实现数据价值的合理利用与生态共赢。

9.1 数据提供方

a）组织确定数据合规工作要求，制定数据合规计划并督促落实；

b）组织开展数据合规影响分析和风险评估，督促整改合规风险；

c）依法向有关部门报告数据流通过程中出现的风险评估和安全事件处置情况。

d）数据提供方应确保数据来源合法合规，不得提供非法获取的数据。

9.2 数据接收方

a）在不适合公开原始数据的数据流通场景中，优先采用多方安全计算、联邦学习和可信执行环境等隐私计算技术，以确保数据流通共享的规范性和安全性，应保障原始数据不出域，实现数据可用不可见的目标；

b）数据接收方存储数据时，应按要求采取安全措施并以合同进行约定。

c）数据接收方应按照与数据提供方约定的用途和方式使用数据，不得超出约定的范围使用数据。

d）数据接收方应采取必要的安全保护措施，保护所接收的数据的安全性和完整性，防止数据泄露、篡改等安全事件的发生。

9.3 数据合作方

a）对合作方进行严格管理，确保其具备相应的数据保护能力和合规资质。

b）在与合作方签订合作协议时，要明确双方在数据保护、安全责任等方面的权利和义务。

c）定期对合作方进行评估和审计，检查其是否按照协议要求进行数据管理和保护。

d）如果发现合作方存在违规行为，要及时终止合作，并采取相应的法律措施。

e）要求合作方提供数据安全认证证书、定期提交数据安全报告等，以确保合作方的合规性。

f）数据合作方应共同建立数据安全管理机制，加强对合作过程中数据的安全保护，防止数据泄露、篡改等安全事件的发生。

g）数据合作方在开展数据合作活动时，应按照合作协议的约定进行数据共享，不得超出约定的范围共享数据。

参 考 文 献

[1] GB/T 35273—2020 信息安全技术 个人信息安全规范
[2] GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型