ICS 35.240.99
CCS L 60

团　　体　　标　　准

T/ISC 0100—2026

数据跨境合规流通体系建设指南

Cross-border data compliance circulation System Construction Guidance

（发布稿）

2026－03－04 发布　　2026－03－04 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、浙江大学、中国联合网络通信集团有限公司、杭州市余杭区数据资源管理局、杭州市余杭大数据经营有限公司、中国联通国际有限公司、中国信息通信研究院、中国交通建设集团有限公司、中国中化集团有限公司、泰康保险集团股份有限公司、清雁科技（北京）有限公司、华清未央（北京）科技有限公司。

本文件主要起草人：林海、李冰、刘洋、罗梦、冯博、王嘉童、李浩宇、孙艺、周映、泮科伟、秦彬、武云易、鲍全贵、周锦鸿、刘光辉、马宝军、黄文波、裴宏祥、孙浩文、马涛、戚琳、刘学忠、孙继波、陶蓉、王岩、何洋、张英伟、何召阳、赵宁、刘建国、戚清海、赵大奇、党铮铮、陈骞莹、王超、王笑晨。

本文件为首次发布。

——

数据跨境合规流通体系建设指南

1 范围

本文件描述了数据跨境合规流通体系框架，明确涵盖数据管理、技术体系、场景运营、监管要求以及数据流通生态等方面，为组织合规有序开展数据跨境流通提供指引。

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，旨在为组织开展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 36073—2018 数据管理能力成熟度评估模型

GB/T 37988—2019 信息安全技术 数据安全能力成熟度模型

GB/T 45652—2025 网络安全技术 生成式人工智能预训练和优化训练数据安全规范

3 术语和定义

GB/T 35273、GB/T 36073、GB/T 37988、GB/T 43697、GB/T 45652界定的以及下列术语和定义适用于本文件。

3.1

数据出境安全评估 data cross-border transfer security assessment

指将在中国境内收集或产生的数据通过网络等方式向境外机构提供（包括一次性或持续性传输）前，对其合法性、正当性、必要性以及安全风险所进行的系统性评估。

3.2

数据战略 data strategy

组织开展数据工作的愿景、目的、目标和原则。

[来源：GB/T 36073—2018，3.4]

3.3

数据分类分级 data classification and grading

根据数据在经济社会发展中的重要程度、一旦遭到篡改、破坏、泄露或者非法获取/使用可能对国家安全、公共利益或个人/组织合法权益造成的危害程度，对数据进行类别划分和等级确定的管理活动。

[来源：GB/T 43697—2024，3.1，有修改]

3.4

个人信息 personal information

以电子或者其他方式记录的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特定自然人活动情况的各种信息。

注：不包括匿名化处理后的信息。

[来源：GB/T 35273—2020，3.1，有修改]

3.5

训练数据 training data

用于生成式人工智能训练的数据。

[来源：GB/T 45652—2025，3.6，有修改]

3.6

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。

3.7

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。

3.8

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。

[来源：GB/T 37988—2019，3.12]

3.9

合规 compliance

对数据安全所适用的法律法规的符合程度。

[来源：GB/T 37988—2019，3.16]

3.10

数据提供方 data provider

指在数据流通活动中，主动提供原始数据、衍生数据或数据服务的一方。其通常对所提供数据拥有合法的控制权或处理权，并承担数据来源合法性、内容合规性及初始安全保护的责任。

3.11

数据接收方 data recipient

指在数据流通活动中，从数据提供方获取数据并进行后续处理（如存储、分析、建模、再分发等）的一方。其对所接收数据的安全保障和合规使用负直接责任。

3.12

数据合作方 data collaborator

指在多方协同的数据处理活动中，与数据提供方或接收方共同参与数据处理、共享控制权或承担联合责任的一方。其角色可能兼具提供与接收属性，具体责任需根据实际分工确定。

4 数据跨境合规体系框架

组织开展数据跨境合规流通体系建设以数据管理、技术保障、场景运营、监管遵从及生态协同五大维度为基本框架，通过系统整合管理策略、技术措施、运营方案、监管要求与各方协作，旨在构建完善的合规服务能力，确保数据跨境流通的安全、高效与可持续，保障数据价值依法有序释放。

5 数据管理合规

5.1 数据战略与治理

组织宜建立与业务需求相匹配的数据战略、治理策略以及权责清晰的数据治理架构，具体要求包括：

a）组织宜建立与业务战略协同的数据战略，明确愿景、目标与原则。制定并发布数据跨境实施路线图，定期评估战略执行成效与业务价值，确保资源配置与战略方向一致。

b）组织宜建立权责清晰的数据治理架构，并制定分层次的数据管理制度体系（政策、办法、细则）。制度应有效宣贯与执行，建立跨部门沟通、协商与问责机制。

5.2 数据质量与标准

组织宜制定标准化质量管理体系，统一数据标准，涵盖业务术语、数据元、主数据与参考数据等。建立覆盖全生存周期的数据质量需求、检查、分析与提升的闭环管理流程。

5.3 数据安全管理

组织宜制定覆盖数据全生命周期的安全策略与管理制度。实施数据分类分级、访问控制、安全监控与审计，依照国家数据跨境要求，定期开展跨境数据安全风险自评估，建立跨境数据负面清单和备案机制，确保跨境数据安全合规流通。

5.4 数据生命周期应用管理

组织宜规范数据分析、开放共享与服务流程机制，确保数据应用合法合规。对数据从需求、设计、运维到退役的全生存周期各阶段实施标准化与可控化管理。

6 技术体系合规

6.1 基础环境合规

基础环境包括了承载跨境业务数据的数据中心机房、信息系统等，组织需采取措施确保基础环境符合业务连续性、网络安全等级保护的基本要求。包括但不限于：

a）组织宜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。

b）组织宜确保数据承载环境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。

c）组织宜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，包括但不限于操作系统、数据库、应用软件等方面。

d）组织宜建立网络安全防护体系，根据国家网络安全等级保护制度，采取防火墙、入侵检测、加密等技术措施，保护网络系统安全。

6.2 智算模型合规

为促进智算模型在数据跨境活动中的可信应用，组织应建立涵盖模型管理、算法评估与数据合规的系列要求，包括但不限于：

a）组织宜确保在数据跨境活动中所采用的智算模型符合国家有关规定和标准要求。

b）组织宜建立模型算法安全评估机制，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）组织宜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

组织宜建立健全数据跨境安全技术防护体系，参考数据要素流通安全和个人信息保护的有关国家、行业标准要求保护数据。

6.3.1 数据加密

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。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

组织宜建立访问控制机制，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。宜采用身份认证、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，宜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

7.1 行业要求合规

组织应主动识别并融入行业特殊监管框架，通过了解行业要求、对接主管部门、遵守业务规范，构建行业层面的合规保障。具体要求包括：

a）组织宜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

组织应将合规要求系统性地融入数据跨境业务流程的全过程，包括流程设计、审批控制、操作规范与人员管理，确保业务操作合法合规。具体要求包括：

a）组织宜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，宜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）组织宜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

组织应确保数据处理者遵循既定要求合规处理数据，并建立涵盖安全管理与主体权利响应的配套制度。具体要求包括：

a）数据处理者应按照数据处理要求处理数据，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

8.1 监管合规

组织宜建立数据全周期的主动合规管理机制，通过持续跟踪监管要求、有效应对安全事件并积极配合监管，以确保数据跨境活动始终符合国家法规与政策。具体要求包括：

a）组织宜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）组织宜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

组织在数据出境前，应依法开展前置性专项安全评估，建立评估机制，并根据评估结果实施风险管控措施。具体要求包括：

a）组织在进行数据出境活动前，宜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）组织宜建立合规评估机制，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 合同管理

开展数据流通活动时，宜通过合同来规范，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）组织宜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，宜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）宜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）组织宜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 数据跨境合作生态合规

9.1 数据提供方合规要求

为履行数据提供方的法定义务与主体责任，组织应建立健全内部合规管理体系，并确保所提供数据的合法合规性，具体包括但不限于以下要求：

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）组织开展跨境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跨境流通过程中出现的风险评估和安全事件处置情况。

d）数据提供方宜确保数据来源合法合规，不得提供非法获取的数据。

9.2 数据接收方合规要求

为确保数据接收方在数据流通与跨境场景中履行全面的合规义务，防范数据安全与法律风险，组织应要求数据接收方承诺并践行以下要求，其责任不以所在司法辖区的规定为转移：

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，宜按要求采取安全措施并以合同进行约定。

c）数据接收方宜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。

e）数据接收方宜建立数据主体权利响应机制，包括但不限于访问、更正、删除（被遗忘）等权利。在接收到数据提供方转交的数据主体删除请求后，宜及时对相关个人信息进行删除或匿名化处理，并向数据提供方反馈处理结果。

f）数据接收方在合作协议或标准合同中明确其履行数据主体删除义务的责任与流程，确保在跨境数据传输场景下，数据主体的“被遗忘权”得以实现。

g）数据接收方应承诺遵守中华人民共和国关于数据出境安全、个人信息保护等相关法律法规及监管要求，无论其所在司法辖区是否存在冲突性规定。数据接收方有义务配合数据提供方及中华人民共和国主管部门的监督、评估、审计与调查，并采取必要措施防止数据被滥用、恶意使用或用于损害中国国家安全、公共利益及个人合法权益的目的。

h）若数据接收方违反双方约定或中华人民共和国相关法律法规，数据提供方有权暂停或终止数据跨境传输，并要求接收方承担相应责任。

9.3 数据合作方合规要求

为有效管理数据合作风险，确保合作全过程的数据安全与合规，组织宜对数据合作方实施以下管理要求：

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）数据合作方可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，宜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] 国家数据基础设施建设指引
[2] GB/T 39477—2020 信息安全技术 政务信息共享 数据安全技术要求
[3] GB/T 40094.4—2021 电子商务数据交易 第4部分：隐私保护规范
[4] GB/T 43697—2024 数据安全技术 数据分类分级规则
[5] GB/T 45577—2025 数据安全技术 数据安全风险评估方法
[6] GB/T 46068—2025 数据安全技术 个人信息跨境处理活动安全认证要求
[7] TC 609-6-2025-01 可信数据空间 技术架构