ICS
CCS 点击此处添加 CCS 号
登记号：

T/ACCEM

团　　体　　标　　准

T/ACCEM XXXXX—XXXX

数据资产全流程合规与监管规则建设指南

Guide to the Construction of Full-process Compliance and Regulatory Rules for Data Asset Management

（征求意见稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

中国商业企业管理协会　发布

目　　次

前言 III
引言 IV
1 范围 5
2 规范性引用文件 5
3 术语和定义 5
4 总则 5
4.1 合法合规原则 5
4.2 数据最小化原则 5
4.3 透明性原则 5
4.4 安全可控原则 6
4.5 责任明确原则 6
5 分级分类授权使用规范 6
5.1 分级标准 6
5.2 分类标准 6
5.3 授权使用规范 6
6 数据资产全流程合规要求 7
6.1 数据资产的收集与存储 7
6.2 数据资产的加工 7
6.3 数据资产的传输和使用 7
6.4 数据资产的运营和交易 7
6.5 数据资产的销毁 7
7 数据资产全流程监管要求 7
7.1 监管机构与职责 8
7.2 监管方式 8
7.3 监管的评估与改进 8
参考文献 9

前　　言

本文件按照GB/T 1.1-2020《标准化工作导则 第一部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由xxxxxxx提出。

本文件由中国商业企业管理协会归口。

本文件起草单位：xxxxxxxxx。

本文件主要起草人：xxxxxx。

引　言

数据作为新时代的关键生产要素，正日益成为推动经济社会发展与转型的核心力量。在数字化、网络化、智能化的浪潮中，数据不仅深化了我们对世界的认知，更开辟了前所未有的价值创造空间，对社会治理、公共服务及科学研究等领域产生了深远影响。

然而，随着数据应用的日益广泛与深入，数据资产的管理与监管问题亦逐渐浮出水面，成为亟待解决的重要议题。当前的数据管理与监管体系尚未能全面适应数据作为新型生产要素的特质，对于数据从采集、处理、分析到共享、保护等全生命周期的合规性要求，尚缺乏一套系统性、规范性的指导框架。此现状不仅可能导致数据资源的低效利用与不当滥用，还可能对个人隐私权益、国家安全利益以及社会稳定大局构成潜在的严重威胁。

基于此，构建一套科学严谨、全面系统且具备高度可操作性的《数据资产全流程合规与监管规则体系》，已成为当务之急。本团体标准旨在填补当前数据管理与监管领域的制度空白，为政府机构、社会组织以及科研机构等多元主体提供一套兼具指导性与实践性的规范框架。该体系将全面覆盖数据的采集源头至最终应用场景，明确各阶段应遵循的合规原则、操作流程、技术标准及监管要求，旨在促进数据资产管理的规范化、标准化与法治化进程。

我们期待能够进一步提升社会各界对数据资产管理重要性的认识水平，推动形成政府主导、多元主体协同参与的监管治理格局。同时，我们也坚信，本团体标准将成为推动数据合规高效利用、强化数据安全保护、充分释放数据价值的重要工具，为构建更加智慧、更加和谐的数字社会与智慧国家奠定坚实的基础。

数据资产全流程合规与监管规则体系

1 范围

本文件旨在明确数据资产从产生到销毁的全生命周期内的合规与监管要求，涵盖数据的采集、处理、分析、存储、共享、使用、运营、交易及销毁等关键环节。

本文件建议适用于所有开展数据处理活动的组织和个人。这包括但不限于政府机构、教育机构、非营利组织，以及数字经济、金融科技、互联网等的各类企业和机构。

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。

DB33/T 1329-2023 数据资产确认工作指南

3 术语和定义

DB33/T 1329-2023 界定的以及下列术语和定义适用于本文件。

3.1

数据资产 data assets

组织过去的交易或事项形成的，由组织合法拥有或控制的，为组织带来经济价值的数据资源。

[来源：DB33/T 1329-2023,3.2]

3.2

数据处理 data processing

包括数据的收集、存储、使用、加工、传输、提供、公开、删除等活动。

3.3

数据处理者 data processor

是指在数据处理活动中自主决定处理目的和处理方式的个人或者组织。

4 总则

4.1 合法合规原则

合法合规原则要求所有数据资产的收集、存储、处理、传输、使用和披露都必须严格遵守国家法律法规、行业规范及国际标准，确保数据活动的合法性。

4.2 数据最小化原则

数据最小化原则要求在数据收集、处理和使用过程中，仅收集实现特定目的所必需的最少量数据，减少不必要的个人数据收集和存储，降低数据泄露风险。

4.3 透明性原则

透明性原则要求数据处理者向数据主体清晰、准确地披露数据的收集、使用、共享和保护情况，确保数据主体对其个人数据的控制权和知情权。

4.4 安全可控原则

安全可控原则要求通过技术手段和管理措施，确保数据资产在存储、处理、传输过程中的保密性、完整性和可用性，防止数据泄露、篡改和丢失。

4.5 责任明确原则

责任明确原则要求数据活动的各个参与方（包括数据控制者、数据处理者、数据主体等）对其在数据处理中的角色和责任有清晰的认识，并承担相应的法律责任。

5 分级分类授权使用规范

5.1 分级标准

数据的分级标准旨在根据数据的重要性、敏感性等因素，将数据划分为不同的安全等级，以便采取相应的保护措施。分级标准通常包括以下四个等级：

a)公开级：指可以无条件向公众开放的数据，这些数据通常不涉及个人隐私、商业秘密或国家安全等敏感信息。

b)内部使用级：指仅供数据处理者内部人员使用的数据，这些数据可能包含一定的业务敏感信息，但不足以构成重大风险。

c)敏感级：指涉及个人隐私、商业秘密或可能对国家安全造成一定影响的数据，需要采取额外的保护措施，限制访问权限。

d)高度敏感级：指涉及核心商业秘密、个人隐私中的敏感信息（如健康记录、财务信息）或国家安全关键数据，需要最高级别的安全保护和严格的访问控制。

5.2 分类标准

数据的分类标准则根据数据的性质、用途和来源等因素，将数据划分为不同的类别，以便进行更有效地管理和利用。分级标准通常包括以下五类：

a)个人信息类：包括姓名、身份证号、联系方式、住址等能够直接或间接识别个人的数据。

b)业务运营类：涉及企业日常运营的数据，如销售记录、库存情况、财务报表等。

c)技术研发类：包括研发过程中的实验数据、技术文档、专利信息等。

d)市场客户类：关于市场趋势、竞争对手分析、客户反馈等数据。

e)合规监管类：涉及法律法规要求保留的数据，如税务记录、合规报告等。

5.3 授权使用规范

针对不同等级和类别的数据，应制定详细的授权使用规范，确保数据的合法、合规使用。这些规范通常包括以下五个方面：

a)访问权限管理：根据数据的分级分类结果，为不同用户或角色分配相应的访问权限。对于敏感和高度敏感级数据，应实施严格的访问控制，如多因素认证、访问审计等。

b)数据使用审批：对于敏感数据的使用，应建立审批流程，确保数据的使用目的、方式和范围符合法律法规和企业政策要求。

c)数据共享与传输：在数据共享和传输过程中，应遵守相关法律法规和行业规范，采取必要的安全措施，如加密传输、签订保密协议等。

d)数据备份与恢复：定期备份重要数据，并建立数据恢复机制，以应对可能的数据丢失或损坏风险。

e)数据安全培训：定期对员工进行数据安全培训，增强员工的数据安全意识，确保数据的合规使用。

6 数据资产全流程合规要求

6.1 数据资产的收集与存储

数据资产的收集需遵循以下要求：

a)需确保数据收集活动基于明确的法律基础，如用户同意、合同必要、公共利益等。

b)公开数据收集的目的、范围、方式及可能的数据使用场景，保障数据主体的知情权。

c)仅收集实现特定目的所必需的最少量数据，避免过度收集与业务无关的个人信息或敏感数据。

d)确保收集的数据准确、完整、及时，并采取措施防止数据错误或遗漏。

数据资产的存储需遵循以下要求：

a)定期对存储的数据进行校验和更新，保持数据的有效性。

b)采用加密技术、访问控制、备份恢复等措施保护数据免受未经授权的访问、泄露、篡改或丢失。

c)遵循数据分类分级原则，对不同级别的数据实施不同的安全保护措施。

6.2 数据资产的加工

数据资产的加工需遵循以下要求：

a)数据加工应严格限于收集时声明的目的，不得擅自改变数据用途。

b)若需进行超出原目的的数据处理，需重新获取数据主体的同意或依据新的法律基础。

c)对非必要保留个人身份的数据进行匿名化处理，降低数据可识别性。

d)在可能的情况下，采用去标识化技术，确保数据无法直接关联到具体个人，同时保留数据分析价值。

e)确保使用的算法模型透明，能够解释输出结果，避免算法偏见和歧视。

f)定期对算法进行审计和评估，确保其符合公平、公正、无歧视的原则。

6.3 数据资产的传输和使用

数据资产的传输和使用需遵循以下要求：

a)采用加密技术保障数据传输过程中的安全性，防止数据在传输过程中被窃取或篡改。

b)严格限制数据传输的通道和方式，确保数据传输的合法性和必要性。

c)实施严格的访问权限管理，确保只有授权人员能够访问和使用数据。

d)记录数据访问日志，便于追踪和审计数据使用情况。

e)与第三方共享、委托处理数据时，应签订书面协议，明确数据安全责任、使用范围、保密义务等。

f)定期对第三方进行数据安全管理评估，确保其符合相关法律法规和内部政策要求。

6.4 数据资产的运营和交易

数据资产的运营和交易需遵循以下要求：

a)在数据运营过程中，持续监控数据质量，确保数据的准确性、完整性和时效性。

b)对数据质量问题进行及时纠正，防止因数据错误导致的决策失误或法律风险。

c)数据交易应遵循相关法律法规，确保数据来源合法、交易过程透明、交易双方权益得到保障。

d)禁止交易涉及个人隐私、国家安全等敏感数据。

e)数据交易应签订书面合同，明确交易双方的权利、义务、违约责任等。

f)合同中应包含数据保护条款，确保数据在交易过程中的安全性和保密性。

6.5 数据资产的销毁

数据资产的销毁需遵循以下要求：

a)明确数据销毁的条件和触发机制，如数据生命周期结束、业务需求变化、法律法规要求等。

b)确保数据销毁活动符合相关法律法规和内部政策要求。

c)采用物理销毁或逻辑销毁方式，确保数据无法被恢复。

d)销毁过程应记录并可追溯，以便审计和验证。

e)设立独立的监督机构或岗位，负责监督数据销毁活动的执行情况和效果。

f)定期对数据销毁活动进行验证，确保数据销毁的彻底性和合规性。

7 数据资产全流程监管要求

7.1 监管机构与职责

监管机构可细分为多类，具体包括数据保护监管机构、行业监管机构、审计与监督机构、标准化与技术监管机构以及法律与司法机构。

a)数据保护监管机构负责制定并执行数据保护相关法律法规，监管数据处理活动的合法性，妥善应对数据泄露事件，并切实保护个人隐私权益。此类机构包括国家数据局、信息安全管理局等。

b)行业监管机构则依据行业特性，制定数据管理与使用的具体规范，并监督行业内数据资产的使用状况，确保其实践符合行业标准和最佳做法。例如，银保监会负责金融监管，国家卫生健康委员会负责医疗监管，工业和信息化部负责信息技术监管等。

c)审计与监督机构负责定期对数据进行审计，核查数据处理的合规性，评估数据资产的安全风险，并提出相应的改进建议。这类机构包括审计署、内部审计部门以及第三方审计公司等。

d)标准化与技术监管机构负责制定数据资产管理的技术标准、规范和指南，推动技术创新与应用，并确保数据资产的技术合规性。国家标准化管理委员会以及国家市场监督管理总局下属的相关技术机构等便属于此类。

e)法律与司法机构则负责处理与数据资产相关的法律纠纷，提供法律解释和指导，确保数据资产的法律权益得到充分保护。法院、检察院以及律师协会等机构均属于此范畴。

7.2 监管方式

对数据资产全流程监管的监管方式如下：

a)对数据资产的处理、存储、传输等环节进行定期检查，确保符合法律法规和行业标准。

b)建立数据资产风险评估机制，识别潜在风险点，及时发布预警信息，采取预防措施。

c)对数据资产处理活动进行合规性审查，确保数据处理活动的合法性和正当性。

d)开展数据资产管理相关的教育和培训活动，提高数据管理人员和员工的合规意识和技能水平。

e)鼓励公众参与数据资产管理的监督，建立举报机制，保护举报人的合法权益。

7.3 监管的评估与改进

在数据资产监管的评估和改进方面，建议：

a)定期对监管效果进行评估，包括监管活动的有效性、合规性、风险控制等方面。

b)根据评估结果和问题反馈，制定改进措施，包括完善法律法规、优化监管流程、提升技术水平等。

c)建立持续改进机制，定期对监管体系进行更新和优化，以适应数据资产管理的新需求和新挑战。

d)加强各监管机构之间的沟通与协作，形成合力，共同推动数据资产管理的合规与监管工作。

参 考 文 献

[1] T/CITIF 001-2024 数据合规审计指南

[2] T/CITIF 001-2022 数据合规管理体系 要求

[3] 中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见（2022年12月2日）

[4] 完善数据全流程合规治理与监管体系，构筑数据高效安全流通屏障（2022年12月20日）