ICS 03.060
CCS A 11

团 体 标 准

T/CEATEC XXX—2025

金融领域数据全生命周期权责界定要求

Requirements for defining rights and responsibilities in the full life cycle of financial data

（征求意见稿）

2025-X-XX 发布 2025-X-XX 实施

中国欧洲经济技术合作协会 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。

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。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件主要起草单位：。

本文件主要起草人：。

本文件为首次编制。

引言

随着金融数字化转型加速，数据已成为金融业的核心资产，其安全有序流通对行业发展至关重要。然而，当前金融领域与相关行业普遍面临数据孤岛林立、权责边界模糊、流转过程监管缺失等挑战，导致数据共享难、监管难、价值释放难。本文件基于现行法律法规与行业实践，系统界定数据全生命周期中各参与方的权利与责任，为构建可信数据共享生态、促进数据要素合法合规流通提供基础保障。

金融领域数据全生命周期权责界定要求

1 范围

本文件规定了金融领域数据生命周期权责界定的权责界定原则、数据全生命周期阶段划分、各阶段权责界定要求、数据安全与隐私保护、保障与监督机制。

本文件适用于商业银行、保险机构、证券公司、金融科技企业、第三方征信机构及金融基础设施运营机构等，在中华人民共和国境内从事金融业务的数据控制者与数据处理者在金融数据管理中的权责划分，也可供金融领域监管部门、行业协会参考使用。

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 37988 信息安全技术 数据安全能力成熟度模型

JR/T 0171 个人金融信息保护技术规范

JR/T 0197 金融数据安全 数据安全分级指南

JR/T 0223 金融数据安全 数据生命周期安全规范

3 术语和定义

JR/T 0171、JR/T 0223界定的以及下列术语和定义适用于本文件。

3.1

数据全生命周期 data full life cycle

数据从采集、生成到销毁的整个演进过程，通常包括数据的采集、传输、存储、使用、加工、共享、披露、归档和销毁等阶段。

3.2

数据控制者 data controller

有权决定数据处理目的、方式等的组织或个人，在金融领域，通常指金融机构本身。

3.3

数据处理者 data processor

受数据控制者委托，代表其处理数据的组织或个人。

3.4

数据主体 data subject

个人信息所标识或关联到的自然人。

3.5

重要数据 important data

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、经济运行、社会稳定、公共健康和安全的数据。

4 权责界定原则

4.1 依法合规原则

数据权责的界定应以国家法律法规、监管要求及行业标准为根本依据。所有数据处理活动均应在法律框架内进行，确保权责来源的合法性与正当性。

4.2 权责对等原则

数据权责的配置应遵循权利与责任相对等的原则。任何参与方在行使数据管理、使用、收益等权利时，应承担与之对应的数据安全、隐私保护、合规管理等责任，防止有权利无责任或有责任无权利的情况。

4.3 主体责任原则

应明确数据控制者是数据安全与合规的首要责任主体，对数据处理活动承担最终责任。数据处理者应根据数据控制者的委托和授权范围，承担相应的执行与安全保障责任。

4.4 最小必要原则

数据权责的配置应围绕实现特定的业务目的或处理目的，确保数据访问、使用和管理的权限范围是实现该目的所必需的、最小化的，以降低数据滥用与泄露风险。

4.5 安全可控原则

权责的行使应以保障数据安全为前提。应通过技术手段与管理措施，确保数据在处理过程中的保密性、完整性和可用性，并对数据操作行为进行记录、监控与审计，实现全过程可控、可追溯。

4.6 动态调整原则

数据权责并非一成不变，应建立动态调整机制。当业务场景、法律法规、技术环境或数据本身的安全级别发生变化时，应及时评估并调整相应的权责分配，确保其持续有效与适宜。

5 数据全生命周期阶段划分

5.1 数据采集与生成

数据被创建或从数据主体处、其他合法来源获取的阶段。此阶段是数据生命周期的起点，重点关注数据的合法性、准确性、最小必要性以及数据主体的知情同意。

5.2 数据传输与存储

数据在不同实体、系统或地理位置之间移动，以及被持久化保存的阶段。此阶段重点关注数据传输过程中的机密性与完整性，以及存储期间的持久安全性与访问可控性。

5.3 数据使用与加工

数据被查询、访问、计算、分析、挖掘、可视化以及通过算法模型进行加工处理的阶段。此阶段重点关注数据的使用目的合规性、处理过程的规范性，以及通过脱敏、匿名化等技术在利用中保护数据安全。

5.4 数据共享与披露

数据被提供给数据控制者之外的外部第三方（如合作机构、监管机构、公众等）的阶段。此阶段是数据流转和价值释放的关键环节，重点关注共享的合法性、安全性评估、数据主体的授权同意以及对接收方的约束与监督。

5.5 数据归档

数据在完成其主要业务价值后，从生产系统转移至独立的、成本更低的存储环境长期保存，以备法律法规或审计查询之需的阶段。此阶段重点关注归档数据的完整性、不可篡改性以及适度的可用性。

5.6 数据销毁

数据被永久性地、不可恢复地删除或清除，使其不再具有任何使用价值的最终阶段。此阶段重点关注销毁操作的彻底性、安全性与可验证性，是数据生命周期的终点。

6 各阶段权责界定要求

6.1 总则

数据控制者是数据安全与隐私保护的核心责任主体，应对其主导的数据处理活动承担全面管理责任。数据处理者须严格依据合同约定、法律法规及数据控制者的明确授权，在指定范围内开展处理活动，并承担相应的执行与安全保护责任。数据主体依法享有其个人数据的相关权利，并承担提供真实信息的义务，数据全生命周期权责追溯示意图见附录 A。

6.2 数据采集与生成阶段

6.2.1 数据控制者权责

应包括以下内容：

a) 权利：应依法依规向数据主体或合法来源采集业务所必需的数据；

b) 责任：

——确保数据采集的合法性与正当性，原则上应获得数据主体的明确授权（法律、行政法规另有规定的除外）；

——履行全面的告知义务，清晰、明确地向数据主体说明采集目的、方式、数据范围、使用规则及权利救济途径；

——应遵循最小必要原则，仅限于采集实现特定目的所必需的数据，不得过度采集；

——建立数据质量核验机制，确保所采集数据的准确性、完整性。

6.2.2 数据处理者权责

应包括以下内容：

a) 权利：依据数据控制者的明确指令与授权，执行数据采集任务；

b) 责任：

——严格遵循数据控制者设定的采集规范与流程，不得擅自变更；

——采取必要的技术与管理措施，保障数据在采集过程中的安全，防止泄露与被窃取。

6.2.3 数据主体权责

应包括以下内容：

a）权利：享有知情权、同意权（法律、行政法规规定的例外情形除外）及拒绝权；

b）责任：有义务向数据控制者提供真实、准确、完整的个人信息。

6.3 数据传输与存储阶段

6.3.1 数据控制者权责

应包括以下内容：

a）权利：依法依规在组织内部及与可信合作方之间传输数据，并自主决定或选择安全的数据存储方案与位置；

b）责任：

——对敏感数据（如个人金融信息、重要数据）在传输过程中必须采用加密等安全增强措施；

——根据数据分类分级结果，对存储中的数据实施与之匹配的保护策略，包括但不限于加密、脱敏、严格的访问控制等；

——依据业务、法规及合规要求，明确并执行各类数据的存储期限。

6.3.2 数据处理者权责

应包括以下内容：

a）权利：依据合同约定及数据控制者的授权，执行数据传输与存储操作；

b）责任：

——严格执行数据控制者制定的数据传输与存储安全策略；

——未经数据控制者额外授权，不得私自将数据传输至约定范围之外或转移存储位置。

6.4 数据使用与加工阶段

6.4.1 数据控制者权责

应包括以下内容：

a）权利：在获得授权的范围内，为实现声明的业务目的、提升服务质量、进行风险控制等而使用和加工数据；

b）责任：

——确保数据的使用与加工活动严格限定在采集时所声明的目的范围内，确保目的的一致性；

——开展数据挖掘、建模分析等深度加工活动时，不得损害数据主体的合法权益，严禁用于任何非法目的；

——建立完善的内部数据使用授权、审批与监控机制；

——在开发、测试、培训等非生产环境中，必须对真实数据实施有效的脱敏或匿名化处理。

6.4.2 数据处理者权责

应包括以下内容：

a）权利：依据数据控制者的明确委托与授权，进行数据加工与分析；

b）责任：

——严格遵守授权范围，不得以任何形式超范围使用数据；

——确保所使用的加工逻辑、算法模型的透明性与公平性，采取措施避免产生不合理的歧视性结果。

6.5 数据共享、披露与转让阶段

6.5.1 数据控制者权责

应包括以下内容：

a）权利：在符合法律法规强制性规定及获得数据主体单独同意的前提下，向第三方共享、披露或转让数据；

b）责任：

——事前对数据接收方的数据保护能力进行充分的安全风险评估；

——通过具有法律约束力的合同、协议等形式，明确约定双方的数据保护责任与义务，并对接收方的后续数据处理活动进行必要监督；

——向数据主体清晰告知共享/披露的目的、涉及的数据类型、接收方的身份与风险，并就此获得其单独同意（法律、行政法规规定的例外情形除外）；

——所有对外信息披露行为必须依法依规进行。

6.5.2 数据处理者权责

应包括以下内容：

a）权利：未经数据控制者的明确书面指令，无权自行决定或实施任何形式的数据共享与披露；

b）责任：应数据控制者要求，积极协助其完成对数据接收方的安全评估与合规性审查工作。

6.5.3 数据接收方权责

应包括以下内容：

a）权利：依据与数据控制者签订的合同约定，访问和使用所接收的共享数据；

b）责任：

——承担与数据控制者同等水平的数据保护义务；

——严格将数据使用范围限定于合同约定的用途；

——在约定的保存期限届满或合同关系终止后，必须依法依约及时、安全地销毁或返还全部相关数据。

6.6 数据归档与销毁阶段

6.6.1 数据控制者权责

应包括以下内容：

a）权利：自主决定数据的归档策略、保存周期及销毁时机；

b）责任：

——制定并执行明确的数据归档与销毁管理制度；

——对因法定或约定事由不再需要，且已达到保存期限的数据，应采取物理或逻辑上不可恢复的方式予以安全销毁；

——对处于归档状态的数据，应实施与生产数据相同等级的安全保护措施。

6.6.2 数据处理者权责

应包括以下内容：

a）权利：依据数据控制者的书面指令，执行数据归档与销毁的具体操作；

b）责任：

——确保数据销毁操作的彻底性、完整性和不可逆性；

——在完成销毁后，应及时向数据控制者提供可验证的销毁执行证明。

7 数据安全与隐私保护

7.1 总体目标

数据控制者与数据处理者应建立与金融数据敏感性相匹配的安全防护体系，确保数据处理全过程中的数据保密性、完整性与可用性，有效保护数据主体个人信息权益，防范数据泄露、篡改、滥用与丢失风险，维护金融秩序稳定和社会公众信任，数据安全能力成熟度应符合 GB/T 37988 的规定。

7.2 基本原则

应满足以下要求：

a）预防为主原则：采取主动、前瞻性的技术和管理措施，实现安全风险早发现、早预警、早处置；

b）目的明确原则：数据处理活动必须具有明确、特定的合法目的，且不得超出目的范围；

c）权限最小化原则：数据访问权限应基于业务必要性的最小范围进行分配和管理；

d）安全嵌入设计原则：在系统设计阶段即同步规划安全与隐私保护措施。

7.3 全生命周期安全要求

7.3.1 采集与生成阶段

应满足以下要求：

a）应建立数据采集安全规范，对采集渠道、接口和终端环境实施安全认证与加固；

b）直接采集个人信息时，应通过隐私政策明确告知采集目的、方式及权利保障措施。

7.3.2 传输与存储阶段

应满足以下要求：

a）传输个人金融信息及重要数据时，必须采用符合行业要求的加密通道与加密算法；

b）对存储的敏感数据实施分类加密保护，核心数据应使用可靠的加密技术手段；

c）建立分级访问控制机制，严格实施身份认证、权限分离和操作审计。

7.3.3 使用与加工阶段

应满足以下要求：

a）开发测试环境严禁使用未脱敏的生产数据，确需使用时须经有效去标识化处理；

b）对大数据分析、机器学习等数据加工操作建立审批与审计追踪机制；

c）部署数据防泄漏措施，监控异常数据访问与批量导出行为。

7.3.4 共享与披露阶段

应满足以下要求：

a）建立数据共享安全评估机制，对共享数据的类型、规模及风险进行评估；

b）通过合同协议明确数据接收方的安全保护责任与义务；

c）共享个人信息时，应采用数据脱敏、聚合等技术降低识别风险。

7.3.5 归档与销毁阶段

应满足以下要求：

a）对归档数据实施与生产系统相当的安全防护等级，安全防护等级应符合 JR/T 0197 的规定；

b）建立数据销毁管理制度，采用不可恢复的技术手段确保数据彻底删除。

7.4 合规与监管要求

应满足以下要求：

a）所有数据安全与隐私保护活动应符合《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》《中国人民银行金融消费者权益保护实施办法》及金融行业监管规定；

b）数据控制者与处理者应依法配合监管部门开展的安全检查、风险评估与应急处置工作。

8 保障与监督机制

为确保本标准所界定的各项权责能在实践中得到有效落实，数据控制者与数据处理者必须建立系统化的保障与监督体系，实现事前预防、事中监控与事后问责的有机结合。

8.1 组织架构与制度建设

8.1.1 责任主体明确

数据控制者应建立自上而下、权责清晰的数据安全管理组织架构，明确决策层、管理层与执行层的职责，并设立专职数据保护负责人（DPO）或指定相应团队。

8.1.2 制度体系完善

制定覆盖数据全生命周期的管理制度、操作规程与应急预案，确保各项数据处理活动有章可循。制度应明确违规行为的认定标准与问责流程。

8.2 数据分类分级与安全技术保障

8.2.1 基础管理

应依据 JR/T 0197 等标准，对数据进行分类分级，并以此作为实施差异化安全策略的基础。

8.2.2 技术措施

应采用与数据安全级别相匹配的技术手段，包括但不限于密码技术、访问控制、数据脱敏、安全审计、防泄漏等，为数据安全提供可靠的技术保障。

8.3 监测、审计与报告

8.3.1 持续监测

应建立数据全生命周期安全监测机制，对关键数据处理活动进行实时记录与异常行为分析。

8.3.2 定期审计

应定期（至少每年一次）或在新业务上线、发生重大变更时，开展内部数据安全审计与合规性评估，检查权责落实情况。

8.3.3 报告机制

应建立畅通的内外部报告渠道。发生数据安全事件时，应依法依规及时向监管机构和受影响的数据主体报告。

8.4 监督、问责与持续改进

8.4.1 履职监督

数据控制者应建立对自身及数据处理者履职情况的监督机制，确保其承担的责任得到履行。

8.4.2 问责机制

应建立并严格执行问责制度。对违反数据安全政策、操作规程及本标准要求的内部人员或数据处理者，依据情节严重程度采取通报、限期整改、终止合作乃至追究法律责任的处罚措施。

8.4.3 改进机制

应基于监测结果、审计发现及安全事件，定期复盘和评估保障与监督体系的有效性，并实施持续改进。

8.5 应急响应与处置

8.5.1 预案与演练

应制定详尽的数据安全事件应急预案，并定期（如每三个月）组织演练，确保其有效性。

8.5.2 快速处置

在发生数据安全事件时，应立即启动应急预案，采取措施控制并消除风险影响，最大限度降低损失。

附 录 A

（资料性）

数据全生命周期权责追溯示意图

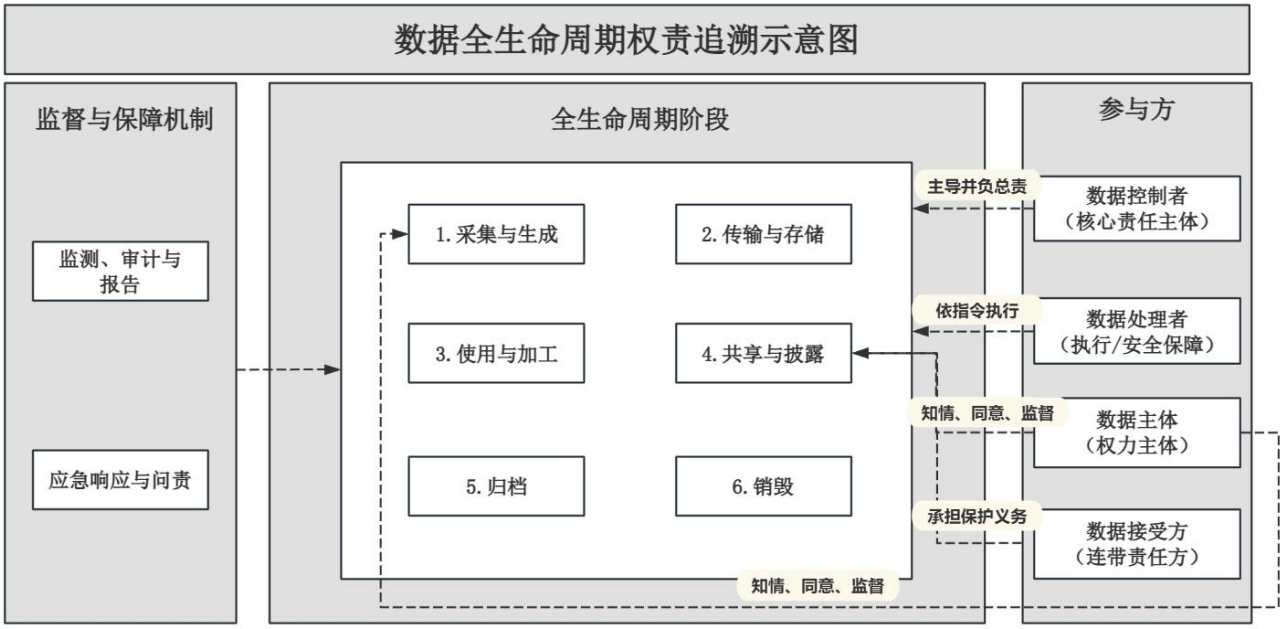

图 A.1 数据全生命周期权责追溯示意图

参考文献

[1] 中华人民共和国网络安全法（中华人民共和国主席令〔2016〕第五十三号）
[2] 中华人民共和国数据安全法（中华人民共和国主席令〔2021〕第八十四号）
[3] 中华人民共和国个人信息保护法（中华人民共和国主席令〔2021〕第九十一号）
[4] 中国人民银行金融消费者权益保护实施办法（中国人民银行令〔2020〕第 5 号）